UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ-2020)

XVII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2020 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Часть 1

Санкт-Петербург

2020

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РЕГИОНАЛЬНАЯ ИНФОРМАТИКА (РИ-2020)

XVII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 28-30 октября 2020 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Часть 1

Санкт-Петербург

2020

УДК (002:681):338.98

Р32

Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября
Р32 2020 г.: Материалы конференции. Часть 1. \ СПОИСУ. – СПб, 2020. – 393 с.
ISBN 978-5-907223-85-1

В первую часть сборника вошли материалы докладов, охватывающих широкий круг направлений: Государственная политика информатизации. Цифровая экономика; Теоретические проблемы информатики и информатизации; Телекоммуникационные сети и технологии; Информационная безопасность; Правовые проблемы информатизации; Информационно-психологическая безопасность; Информационные технологии в экономике; Информационные технологии в управлении техническими системами; Информационные технологии в производстве; Информационные технологии в критических инфраструктурах; Информационные технологии на транспорте. Предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций Санкт-Петербурга и других регионов, специализирующихся в области информатизации, связи и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

Публикуется в авторской редакции

Подписано в печать 20.10.2020. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 45,7. Тираж 400 экз. Заказ № 1560
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-907223-85-1

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
ORGANIZATION DES NATIONS UNIES POUR L'EDUCATION, LA SCIENCE ET LA CULTURE

РИ-2020
РЕГИОНАЛЬНАЯ ИНФОРМАТИКА

REGIONAL INFORMATICS (RI-2020)

XVII ST. PETERSBURG INTERNATONAL CONFERENCE

St. Petersburg, October 28-30, 2020

PROCEEDINGS OF THE CONFERENCE

Part 1

St. Petersburg

2020

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

- Правительство Санкт-Петербурга
- Законодательное Собрание Санкт-Петербурга
- Правительство Ленинградской области
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
- Министерство науки и высшего образования Российской Федерации
- Российская академия образования
- Отделение нанотехнологий и информационных технологий Российской академии наук
- Санкт-Петербургский национальный исследовательский университет информационных
- Санкт-Петербургский институт информатики и автоматизации Российской академии наук[1]
- Санкт-Петербургская территориальная группа Российского национального комитета по автоматическому управлению
- Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ

- Российский фонд фундаментальных исследований
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н. Г. Кузнецова»
- Российский государственный гидрометеорологический университет
- Санкт-Петербургский государственный морской технический университет
- Санкт-Петербургский политехнический университет Петра Великого (национальный исследовательский университет)
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет промышленных технологий и дизайна
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский научный центр Российской академии наук
- Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
- Санкт-Петербургский университет МВД России
- Санкт-Петербургский институт экономики и бизнеса
- Группа компаний «Марвел»
- АО «Институт инфотелекоммуникаций»
- АО «Концерн «НПО «Аврора»
- АО «Научно-исследовательский институт программных средств»
- АО «Научно-производственное объединение «Импульс»
- АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- АО «НИИ «Масштаб»
- АО «Центр компьютерных разработок»
- ЗАО «Институт телекоммуникаций»
- ООО «АСБ»
- ООО «Геонавигатор»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- ПАО «ИНТЕЛТЕХ»
- Партнерство для развития информационного общества на Северо-Западе России
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии инженерных наук им. А.М. Прохорова
- Санкт-Петербургское отделение Академии информатизации образования
- Санкт-Петербургское отделение Международной академии информатизации

[1] В связи с реорганизацией в форме присоединения в 2020 году на базе Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) образован Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН); СПИИРАН является структурным подразделением СПб ФИЦ РАН.

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ

Беглов Александр Дмитриевич	Губернатор Санкт-Петербурга
Макаров Вячеслав Серафимович	Председатель Законодательного собрания Санкт-Петербурга
Дрозденко Александр Юрьевич	Губернатор Ленинградской области
Фальков Валерий Николаевич	Министр науки и высшего образования Российской Федерации
Шадаев Максут Игоревич	Министр цифрового развития, связи и массовых коммуникаций Российской Федерации
Аверьянов Юрий Тимофеевич	Первый заместитель Секретаря Совета Безопасности Российской Федерации

ПРЕЗИДИУМ КОНФЕРЕНЦИИ

Советов Борис Яковлевич	Председатель Программного комитета, сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования
Юсупов Рафаэль Мидхатович	Председатель Организационного комитета, научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук, член-корреспондент Российской академии наук
Васильев Владимир Николаевич	Ректор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, член-корреспондент Российской академии образования, член-корреспондент Российской академии наук
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета промышленных технологий и дизайна, вице-президент Российского союза ректоров, председатель Совета ректоров вузов Санкт-Петербурга и Ленинградской области
Ильин Николай Иванович	Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России
Казарин Станислав Валерьевич	Председатель Комитета по информатизации и связи Санкт-Петербурга
Красников Геннадий Яковлевич	Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук, академик Российской академии наук
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Панкевич Виктор Николаевич	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе
Пешехонов Владимир Григорьевич	Генеральный директор ГНЦ «Центральный научно-исследовательский институт «Электроприбор», академик Российской академии наук
Ронжин Андрей Леонидович	Директор Санкт-Петербургского Федерального исследовательского центра Российской академии наук
Степура Сергей Николаевич	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Шерстюк Владислав Петрович	Президент Национальной ассоциации международной информационной безопасности

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук, член-корреспондент Российской академии наук

Заместитель председателя Организационного Комитета

Казарин Станислав Валерьевич	Председатель Комитета по информатизации и связи Санкт-Петербурга

Члены Организационного Комитета

Алексеев Анатолий Владимирович	Исполнительный директор Института автоматизации процессов борьбы за живучесть корабля, судна, профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Антохина Юлия Анатольевна	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Басков Вячеслав Дмитриевич	Генеральный директор ООО «НеоБИТ»
Белый Олег Викторович	Директор по науке Санкт-Петербургского научного центра Российской академии наук
Блажис Анатолий Константинович	Директор АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора»
Богданов Владимир Николаевич	Директор АО «ЦентрИнформ», лауреат Государственной премии Российской Федерации в области науки и техники
Борисов Николай Валентинович	Заведующий кафедрой Санкт-Петербургского государственного университета
Гаценко Олег Юрьевич	Генеральный директор АО «Научно-исследовательский институт программных средств»
Гирдин Сергей Алексеевич	Президент Группы компаний «Марвел»
Григорьев Владимир Александрович	Генеральный директор ООО «Лаборатория инфокоммуникационных сетей», президент Санкт-Петербургского отделения Академии инженерных наук им. А.М. Прохорова»
Даричев Петр Геннадьевич	Руководитель приоритетного проекта «Умный город» Департамента экономического развития города Севастополя
Жданов Сергей Николаевич	Заместитель генерального директора АО ВТБ Девелопмент
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Руководитель отделения «Кибербезопасность» института передовых производственных технологий, профессор Санкт-Петербургского политехнического университета Петра Великого (национального исследовательского университета)
Игумнов Владимир Вячеславович	Советник генерального директора АО «Научно-производственное объединение «Импульс»
Идрисов Рустам Фидайович	Директор Центра исследований проблем безопасности Российской академии наук
Ипатов Олег Сергеевич	Директор Института дополнительного образования Санкт-Петербургского политехнического университета Петра Великого (национального исследовательского университета)

Карпов Александр Вадимович	Заместитель начальника ВУНЦ ВМФ «Военно-морская академия имени Адмирала Флота Советского Союза Н. Г. Кузнецова» по учебной и научной работе
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Кефели Игорь Федорович	Директор Центра геополитической экспертизы Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Корниенко Анатолий Адамович	Заведующий кафедрой Петербургского государственного университета путей сообщения Императора Александра I
Крупцов Сергей Владимирович	Первый заместитель генерального директора АО «Центр компьютерных разработок»
Кузичкин Александр Васильевич	Заместитель генерального директора по информационным технологиям АО «НИИ телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Кулешов Игорь Александрович	Заместитель генерального директора по научной работе ПАО "ИНТЕЛТЕХ"
Куприянов Михаил Степанович	Первый проректор, заведующий кафедрой вычислительной техники Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Кучерявый Михаил Михайлович	Советник генерального директора АО «Корпорация Московский институт теплотехники» Государственной корпорации «Роскосмос», Государственный советник Российской Федерации 1 класса
Марков Вячеслав Сергеевич	Ученый секретарь Объединенного научного совета Санкт-Петербургского научного центра Российской академии наук
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Михайлов Николай Семенович	Начальник управления информационных технологий и телекоммуникаций АО «Равенство», технический директор Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Михайлова Анна Сергеевна	Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью
Михеев Валерий Леонидович	Ректор Российского государственного гидрометеорологического университета
Молдовян Александр Андреевич	Заведующий лабораторией Санкт-Петербургского института информатики и автоматизации Российской академии наук
Николашин Юрий Львович	Генеральный директор ПАО "ИНТЕЛТЕХ", генеральный конструктор системы управления ВМФ
Никулин Евгений Николаевич	Ректор Санкт-Петербургского института экономики и бизнеса
Ныркov Анатолий Павлович	Профессор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Оводенко Анатолий Аркадьевич	Президент Санкт-Петербургского государственного университета аэрокосмического приборостроения
Овчаренко Андрей Вячеславович	Директор СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Пролетарский Андрей Викторович	Декан Московского государственного технического университета им. Н.Э. Баумана, председатель Федерального УМО по УГСН 09.00.00 «Информатика и вычислительная техника»
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»

Силла Евгений Петрович	Ученый секретарь Санкт-Петербургского института информатики и автоматизации Российской академии наук
Смирнов Павел Игоревич	Генеральный директор АО «НИИ «Масштаб»
Солодянников Александр Владимирович	Генеральный директор ООО «АСБ»
Стрельцов Анатолий Александрович	Заведующий отделом Института проблем информационной безопасности Московского государственного университета им. М.В. Ломоносова, действительный государственный советник Российской Федерации 3 класса
Строганов Дмитрий Викторович	Проректор по международной деятельности Пущинского государственного естественно-научного института, председатель Учебно-методического совета по направлению 09.00.02 «Информационные системы и технологии»
Тихомиров Сергей Григорьевич	Генеральный директор АО «Кодекс»
Туричин Глеб Андреевич	Ректор Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Советник генерального директора АО «Научно-производственное объединение «Импульс»
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Федерального исследовательского центра «Информатика и управление» Российской академии наук
Шелудько Виктор Николаевич	Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Шерстюк Юрий Михайлович	Генеральный директор АО «Институт инфотелекоммуникаций»
Шилов Константин Юрьевич	Генеральный директор АО «Концерн «НПО «Аврора»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Программного Комитета

Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования

Заместитель председателя Программного Комитета

Тумарев Владимир Михайлович	Первый заместитель председателя Комитета по информатизации и связи Санкт-Петербурга

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА – РУКОВОДИТЕЛИ И СЕКРЕТАРИ СЕКЦИЙ

Абрамов Максим Викторович	Руководитель лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, доцент кафедры информатики Санкт-Петербургского государственного университета, канд. техн. наук
Алексеев Анатолий Владимирович	Исполнительный директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, д-р техн. наук, профессор
Афанасьев Александр Васильевич	Полковник полиции, начальник научно-исследовательского отдела Санкт-Петербургского университета МВД России, канд. юр. наук, доцент
Баранова Евгения Васильевна	Профессор кафедры цифрового образования института информационных технологий и технологического образования Российского государственного Российского государственного педагогического университета им. А.И. Герцена, д-р пед. наук, профессор

Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора», д-р техн. наук, профессор
Богданов Виталий Олегович	Программист Санкт-Петербургского института информатики и автоматизации Российской академии наук
Браницкий Александр Александрович	Старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Бузников Анатолий Алексеевич	Заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), заслуженный деятель науки Российской Федерации, д-р техн. наук, профессор
Верзун Наталья Аркадьевна	Доцент кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Воробьев Андрей Игоревич	Доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доцент
Воробьев Владимир Иванович	Профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, профессор
Гончаров Вадим Владимирович	Менеджер ООО «Монтаж Электросистем», Жигадло Валентин Эдуардович, заместитель генерального директора ЗАО «Институт телекоммуникаций», д-р техн. наук, доцент
Горенбургов Михаил Абрамович	Главный научный сотрудник отдела формирования финансовой политики северных регионов Федерального исследовательского центра «Кольский научны центр Российской академии наук», д-р экон. наук, профессор
Горохов Владимир Леонидович	Профессор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, д-р техн. наук, профессор
Горяинов Виктор Сергеевич	Ассистент кафедры фотоники Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Денисова Дарья Михайловна	Научный сотрудник лаборатории биомедицинской информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук
Ефремов Артём Александрович	Заведующий кафедрой системного анализа и управления Санкт-Петербургского политехнического университета Петра Великого (национального исследовательского университета), канд. физ.-мат. наук, доцент
Жвалевский Олег Валерьевич	Научный сотрудник лаборатории биомедицинской информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, д-р техн. наук, доцент
Жуланова Дарья Николаевна	Ассистент кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Зайцева Александра Алексеевна	Ученый секретарь Санкт-Петербургского Федерального исследовательского центра Российской академии наук, канд. техн. наук
Захаров Валерий Вячеславович	Младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук
Захаров Юрий Никитич	Первый заместитель директора Санкт-Петербургского информационно-аналитического центра, канд. техн. наук, профессор
Звонов Денис Валерьевич	Первый заместитель генерального директора АО «Научно-производственное объединение «Импульс», канд. техн. наук

Зикратов Игорь Алексеевич	Декан факультета информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, д-р техн. наук, профессор
Ивлева Людмила Евгеньевна	Инженер кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова
Игумнов Владимир Вячеславович	Советник генерального директора АО «Научно-производственное объединение «Импульс», канд. техн. наук
Искандеров Юрий Марсович	Заведующий лабораторией информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, профессор
Истомин Евгений Петрович,	Директор Института геоинформационных систем и технологий, заведующий кафедрой прикладной информатики Российского государственного гидрометеорологического университета, д-р техн. наук, проф.
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доцент
Кефели Игорь Федорович	Директор Центра геополитической экспертизы Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, заслуженный работник высшей школы Российской Федерации, д-р филос. наук, профессор
Козлов Владимир Николаевич	Профессор Высшей школы киберфизических систем и управления Санкт-Петербургского политехнического университета Петра Великого (национального исследовательского университета), д-р техн. наук, профессор
Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, д-р техн. наук, профессор
Коршунов Игорь Львович	Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Котенко Игорь Витальевич	Заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, профессор
Кулешов Сергей Викторович	Главный научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук
Лаптев Владимир Валентинович	Первый проректор Российского государственного педагогического университета им. А.И. Герцена, академик Российской академии образования, заслуженный деятель науки Российской Федерации, д-р пед. наук, канд. физ.-мат. наук, профессор
Ласкин Михаил Борисович	Старший научный сотрудник лаборатории информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. физ.-мат. наук, доцент
Литвинов Владислав Леонидович	Доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, канд. техн. наук, доцент
Локнов Алексей Игоревич	Майор полиции, старший преподаватель кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, канд. техн. наук
Лытаев Сергей Александрович	Главный научный сотрудник лаборатории прикладной информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р. мед. наук

Мельник Галина Сергеевна	Профессор кафедры цифровых медиакоммуникаций Высшей школы журналистики и массовых коммуникаций Санкт-Петербургского государственного университета, д-р полит. наук, профессор
Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, канд. экон. наук
Михайленко Евгений Иванович	Ведущий специалист АО «Научно-производственное объединение «Импульс»
Михайличенко Николай Валерьевич	Преподаватель Военной академии связи им. Маршала Советского Союза С.М. Буденного, канд. техн. наук
Мороз Николай Васильевич	Заместитель директора ООО «Геонавигатор»
Мусатенко Роман Иванович	Руководитель Центра ранговой партнерской сертификации НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», старший научный сотрудник ВУНЦ ВМФ «ВМА»
Ныркoв Анатолий Павлович	Профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, профессор
Паращук Игорь Борисович	Профессор кафедры Военной академии связи им. Маршала Советского Союза С.М. Буденного, д-р техн. наук, профессор, засл. изобретатель Российской Федерации
Плебанек Ольга Васильевна	Заведующая. кафедрой социально-гуманитарных дисциплин Университета при МПА ЕврАзЭС, д-р филос. наук, доцент
Попов Николай Николаевич	Доцент кафедры информационных технологий и систем безопасности Института информационных систем и геотехнологий Российского государственного гидрометеорологического университета, канд. техн. наук, доцент
Примакин Алексей Иванович	Полковник полиции, начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, д-р техн. наук, профессор
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор», канд. техн. наук, профессор
Рудницкий Сергей Борисович	Ведущий научный сотрудник лаборатории прикладной информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д.т.н.
Саенко Игорь Борисович	Ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р техн. наук, профессор
Свешникова Наталья Олеговна	Доцент кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, канд. психол. наук, доцент
Симонова Ирина Викторовна	Профессор кафедры цифрового образования института информационных технологий и технологического образования Российского государственного педагогического университета им. А.И. Герцена, д-р пед. наук, профессор
Смирнова Полина Владиславовна	Аналитик отдела мониторинговых исследований Центра технологий электронного правительства Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Советов Борис Яковлевич	Сопредседатель Научного совета по информатизации Санкт-Петербурга, заслуженный профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), академик Российской академии образования, засл. деятель науки и техники Российской Федерации, д-р техн. наук, профессор
Согонов Сергей Александрович	Заведующий кафедрой судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, канд. техни. наук, доцент

Соколов Борис Владимирович	Главный научный сотрудник – руководитель лаборатории информационных технологий в системном анализе и моделировании Санкт-Петербургского института информатики и автоматизации Российской академии наук, заслуженный деятель науки России, д-р техн. наук, профессор
Соколов Сергей Сергеевич	Проректор по образовательной деятельности, заведующий кафедрой комплексного обеспечения компьютерной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, доцент
Тарашнина Светлана Ивановна	Начальник отдела моделирования и прогнозирования Санкт-Петербургского информационно-аналитического центра, канд. физ.-мат. наук, доцент
Татарникова Татьяна Михайловна	Директор Института информационных систем и геотехнологий, заведующая кафедрой информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, д-р техн. наук, профессор
Тишков Артем Валерьевич	Заведующий кафедрой физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. акад. И.П. Павлова, канд. физ.-мат. наук, доцент
Токарев Владимир Семенович	Главный специалист, секретарь Научно-технического совета Санкт-Петербургского информационно-аналитического центра, канд. техн. наук, доцент
Тулупьев Александр Львович	Профессор кафедры информатики Санкт-Петербургского государственного университета, главный научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, д-р физ.-мат. наук, профессор
Тумалева Елена Андреевна	Доцент кафедры цифрового образования института информационных технологий и технологического образования Российского государственного педагогического университета им. А.И. Герцена, канд. пед. наук, доцент
Тюрин Иван Сергеевич	Аспирант Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Советник генерального директора АО «НПО «Импульс», канд. техн. наук
Фаткиева Роза Равильевна	Старший научный сотрудник лаборатории информационно-вычислительных систем Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук, доцент
Федорченко Людмила Николаевна	Старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, канд. техн. наук
Хлобыстова Анастасия Олеговна	Младший научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук
Цехановский Владислав Владимирович	Заведующий кафедрой информационных систем, профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доцент
Чугунов Андрей Владимирович	Директор Центра технологий электронного правительства Института дизайна и урбанистики Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, канд. полит. наук, доцент
Шакин Дмитрий Николаевич	Заместитель руководителя Управления ФСТЭК России по Северо-Западному федеральному округу, канд. воен. наук, доцент

Юсупов Рафаэль Мидхатович	Научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук, член-корреспондент Российской академии наук, заслуженный деятель науки и техники Российской Федерации, д-р техн. наук, профессор
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. психол. наук

Ученый секретарь Конференции

Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ИНФОРМАТИЗАЦИИ. ЦИФРОВАЯ ЭКОНОМИКА

УДК 316.422.4

ДАННЫЕ ЭЛЕКТРОННОГО УЧАСТИЯ КАК КОСВЕННЫЙ ИСТОЧНИК ИНФОРМАЦИИ О ХАРАКТЕРИСТИКАХ ГОРОДСКОЙ СРЕДЫ

Антонов Александр Сергеевич, Кудинов Сергей Александрович
Университет ИТМО
Биржевая линия, В.О., 14, Санкт-Петербург, 199034, Россия
e-mails: asantonov@itmo.ru, sergei.kudinov@itmo.ru

Аннотация. В ходе исследования сформулирована методика анализа качества городской среды с помощью данных электронного участия. Выявлены два основных фактора, влияющих на территориальное и категориальное распределение проблем городской среды: неравномерное распределение активности пользователей и локальная активность горожан по отправлению сообщений на портал городских проблем. Также были разработаны способы учета данных факторов.

Ключевые слова: электронное участие; электронные обращения; гражданское общество; гражданская активность; качество городской среды.

E-PARTICIPATION DATA AS AN INDIRECT SOURCE OF INFORMATION ON CHARACTERISTICS OF URBAN ENVIRONMENT

Antonov Aleksandr, Kudinov Sergey
ITMO University
14 Birzhevaya line, Vasilievsky Island, St. Petersburg, 199034, Russia
e-mails: asantonov@itmo.ru, sergei.kudinov@itmo.ru

Abstract. A method of analyzing the quality of urban environment with help of e-participation data is developed in this study. We have identified two main factors, which have an impact on spatial and categorial distribution of problems of urban environment. These are, firstly, the unequal distribution of user activity and, secondly, local activity of citizens, who send reports on urban problems to e-participation portals. We have also designed ways of accounting these factors.

Keywords: electronic participation, electronic appeal, civil society, civic activity, quality of urban environment, participation inequality.

В процессе развития систем электронного взаимодействия граждан и государства начали формироваться порталы и приложения, позволяющие сообщать о тех или иных проблемах с городским благоустройством в государственные органы не традиционным образом, в виде письма или личного посещения органа власти, а электронным. Подобные системы на данный момент существуют как за рубежом, так и в российских городах. В том числе два портала были созданы в Санкт-Петербурге («Наш Санкт-Петербург» [1], «Красивый Петербург» [2]).

Появление подобных инструментов облегчило и ускорило процесс подачи заявления [3], благодаря чему участие граждан в городском благоустройстве стало более активным. В свою очередь, с популяризацией подобных систем объем сообщений резко вырос. С учётом существующего объема данных о городских проблемах стало возможно рассматривать такой источник в качестве исходных данных для косвенной оценки качества городской среды. Тем не менее, данные электронного участия имеют свои особенности, которые необходимо учитывать в исследованиях.

Использованию сообщений с порталов электронного участия для анализа различных социальных и экономических характеристик городской среды посвящен ряд исследований. В частности, это работы Константина Контокосты и других авторов [4, 5] университета Нью-Йорка, проводящих исследования городов при помощи разнообразных данных, в том числе, сообщений американского сервиса «311» [6], использующегося во многих городах США. В этих работах раскрываются особенности данных электронного участия, включающие в себя их пространственно-временной характер, различия в популярности различных типов проблем в разных городских районах, а также неравномерная активность горожан по сообщению о городских проблемах и способы ее выявления. Также следует выделить исследования О'Брайена [7, 8], работающего по направлению эконометрии и социальной теории «разбитых окон». Он анализирует роль пользователей порталов электронного участия в надзоре за порядком на окружающей их территории.

Можно установить две основных теории об изучении характеристик городской среды с помощью инструментов электронного участия. Во-первых, неоднородное распределение сообщений о городских проблемах может служить

индикатором состояния городской среды. Во-вторых, при применении этих данных необходимо учитывать несколько факторов, в частности, неравномерное распределение активности горожан и ее преимущественно локальный характер.

Целью данного исследования является формулирование методики анализа городской среды, которая бы учитывала возможные субъективные факторы, влияющие на территориальное распределение сообщений, и, в результате, позволяла извлекать из необработанных данных знания о городской среде и пользовательской активности.

В результате изучения зарубежных исследований и анализа базы данных портала «Наш Санкт-Петербург» [9] были выявлены два основных фактора, влияющих на территориальное и категориальное распределение городских проблем.

Первый фактор – это локальная активность пользователей, ограничивающаяся пределами одного или нескольких кварталов. Она является мерой, разделяющей прогнозные объективные данные и субъективную оценку качества городской среды, формируемую пользователями. В ходе работы на основе зарубежного опыта был сформулирован метод определения показателя локальной активности. Он заключается в вычислении отношения частоты, с которой горожане обращаются на портал по определенному виду проблем, к частоте их возникновения, определяемой на основе существующих объективных данных, с учетом социальных и градостроительных характеристик территории. Для апробации в проведенном исследовании в качестве подобного вида проблем были выбраны аварийные отключения горячей воды. Следует отметить, что, в отличие от жителей зарубежных городов, петербуржцы склонны сообщать о существенно меньшем количестве проблем.

Второй фактор – это неравномерное распределение активности пользователей, по причине которого небольшая группа «суперпользователей» создает бóльшую часть сообщений в отдельных кварталах на изучаемой территории. Для учета этого фактора был разработан алгоритм, нивелирующий подобные всплески активности по городским кварталам и группам проблем.

На основе сформированных решений, учитывающих особенности данных электронного участия, была подготовлена методика анализа качества городской среды, предоставляющая ряд показателей дефицита её качества, объединенных в единую интегральную оценку.

Она содержит пять шагов. Сначала, для более качественного отображения состояния элементов городской среды, существующие типы проблем объединяются в тематические группы (например, «Мусор и загрязнения» или «Освещение»). Затем в каждом городском квартале исследуемой территории подсчитывается количество сообщений разных групп. Далее при помощи разработанного алгоритма в каждом квартале нивелируется повышенная активность «суперпользователей». Получившееся число сообщений взвешивается по показателю локальной активности, расчет которого описан ранее. Затем результаты по каждой группе проблем пересчитываются в относительный вид и уравновешиваются, в сумме образуя прогнозную оценку дефицита качества городской среды. В итоге территория с наименьшей оценкой принимается за наиболее благополучную, и наоборот.

Далее методика была апробирована на двух территориях в Санкт-Петербурге с различной морфологией: в Василеостровском районе и в кварталах около станции метро «Комендантский проспект». Наименьшую оценку качества городской среды в 2015-2017 годах получили кварталы около станции метро «Василеостровская», а также на улице Репина. Подобные результаты могут свидетельствовать о повышенной нагрузке на инфраструктуру города около крупного транспортного узла, а также о слабом социальном надзоре со стороны граждан. Тем не менее, при применении методики к более новым данным оценки могут измениться по причине увеличившегося объема создаваемых сообщений, что ведет к более точным результатам.

Далее в исследовании была проведена верификация полученных итогов. Одним из ее вариантов был выбран анализ сообщений о преступлениях, данные о которых были доступны за 2016 год. Выбор такого метода обусловлен рядом зарубежных исследований, связывавших уровень преступности с качеством городской среды. Однако, статистически значимой корреляции между интегральной оценкой качества городской среды и концентрацией сообщений о преступлениях в Санкт-Петербурге обнаружено не было. Таким образом, данный метод верификации требует уточнения альтернативными способами, что является задачей дальнейших исследований, включающих в себя натурные обследования территории с анализом актуальной выгрузки данных о городских проблемах за предшествующий обследованию временной период. Тем не менее, полученные результаты позволяют предположить, что при учете описанных ранее факторов на основе данных электронного участия можно косвенным образом вычислять прогнозный уровень проблем городской среды.

СПИСОК ЛИТЕРАТУРЫ

1. Портал "Наш Санкт-Петербург". - URL: https://gorod.gov.spb.ru/.
2. Портал "Красивый Петербург". - URL: http://красивыйпетербург.рф/about.
3. Chugunov A., Kabanov Y., Misnikov Y. Citizens versus the Government or Citizens with the Government: a Tale of Two e-Participation Portals in One City – a Case Study of St. Petersburg, Russia // Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance. New York. 2017. P. 70-77.
4. Kontokosta C., Hong B., Korsberg K. Equity in 311 Reporting: Understanding Socio-Spatial Differentials in the Propensity to Complain // Bloomberg Data for Good Exchange Conference. New York. 2017.
5. Lingjing W., Qian C., Kontokosta C., Sobolevsky S. Structure of 311 service requests as a signature of urban location // PloS one. 2017. Vol. 12, № 10.
6. NYC311. - URL: https://portal.311.nyc.gov/.
7. O'Brien D.T. Custodians and Custodianship in Urban Neighborhoods: A Methodology Using Reports of Public Issues Received by a City's 311 Hotline // Environment and Behavior. 2015. Vol. 3, № 47. P. 304-327.
8. O'Brien D.T., Sampson R.J., Winship C. Ecometrics in the age of big data: Measuring and assessing "broken windows" using large-scale administrative records // Sociological Methodology. 2015. Vol. 45, № 1. P. 101-147.
9. Kudinov S., Ilina E., Antonov A. Analyzing civic activity in the field of urban improvement and housing maintenance based on e-participation // 6th Int. Conf. EGOSE 2019. Communications in Computer and Information Science (CCIS). Springer, 2020. Vol. 1135. P. 88-102. DOI: 10.1007/978-3-030-39296-3_7

УДК 004.89

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭЛЕКТРОННОЙ ИНВЕНТАРИЗАЦИИ ОБЪЕКТОВ ГОРОДСКОГО ХОЗЯЙСТВА

Беген Петр Николаевич, Наджафи Каджабад Эбрахим
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: begen@itmo.ru, e.najafi@itmo.ru

Аннотация. В ходе исследования выявлены возможности и перспективы применения технологий искусственного интеллекта в процессе инвентаризации объектов городского хозяйства; разработан прототип «умного» классификатора на основе методов машинного обучения, компьютерного зрения, распознавания образов; подготовлен набор данных, размеченный по типам объектов и элементов благоустройства.

Ключевые слова: распознавание образов; компьютерное зрение; машинное обучение; искусственный интеллект; инвентаризация; городское хозяйство; цифровая экономика; умный город.

USING ARTIFICIAL INTELLIGENCE TOOLS IN ELECTRONIC INVENTORY OF URBAN FACILITIES

Begen Petr, Najafi Kajabad Ebrahim
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: begen@itmo.ru, e.najafi@itmo.ru

Abstract. In this course of study we revealed the possibilities and prospects of using artificial intelligence tools in inventory of urban and municipal facilities; developed a prototype of "smart" classifier based on machine learning methods, computer vision, pattern recognition and detection; prepared dataset that is labeled by the types of objects and elements of urban improvement.

Keywords: pattern recognition; computer vision; machine learning; artificial intelligence; inventory; urban management; digital economy; smart city.

Перспективность исследований в области повышения качества жизни населения и качества оказания государственных и муниципальных услуг с применением современных информационно-коммуникационных технологий (сокр. ИКТ) нарастает, что обуславливается принятием на федеральных уровнях программы «Цифровая экономика Российской Федерации», проекта «Формирование комфортной городской среды», проекта «Умный город» и т.п. Основные мировые тенденции предполагают проведение теоретических и экспериментальных исследований в целях выявления перспективных ИКТ-сервисов умного города, функционирующих на основе открытых городских данных; определения подходов к сбору, анализу и подготовке репрезентативных данных [1].

Проект «Умный город» в России реализуется в рамках национального проекта «Жилье и городская среда» и программы «Цифровая экономика Российской Федерации». В основу проекта заложено формирование эффективной системы управления городским хозяйством. Состав городского хозяйства представляет собой сложный комплекс различных подотраслей, тесно связанных между собой и объединенных общей целью удовлетворения потребностей населения в его услугах. Поддерживать такой состав в актуальном состоянии в рамках осуществления деятельности процесса инвентаризации объектов является трудной и рутинной задачей, которая требует ежедневных усилий со стороны сотрудников администрации, управляющих компаний и муниципальных органов. Использование передовых ИКТ-инструментов способно автоматизировать данную деятельность и повысить качество и скорость процесса электронной инвентаризации объектов.

В качестве предмета исследования был выбран процесс инвентаризации объектов городского хозяйства на интернет-портале «Паспортизация объектов благоустройства Санкт-Петербурга» (http://ob.kb.gov.spb.ru), на котором осуществляется учет объектов благоустройства и элементов благоустройства на территории Санкт-Петербурга.

В рамках проведенного исследования совместно с представителями администрации Петроградского района Санкт-Петербурга были выявлены возможности разработки программного решения в целях контроля, оптимизации процессов учета и классификации объектов городского хозяйства, а также упрощения (автоматизации) ввода и обработки данных в системе инвентаризации объектов городского хозяйства.

В качестве основного подхода к решению было предложено разработать «умный» классификатор на основе технологий искусственного интеллекта, в частности методов машинного обучения, компьютерного зрения, распознавания объектов. «Умный» классификатор способен по фотоизображению определить основные объекты (элементы) городского хозяйства (двери, окна, козырьки, перила и т.д.), сгруппировать определенные элементы с указанием зависимостей в порядке вложенности (например, Красногвардейский район → улица Белорусская → дом № 6 → входная группа → дверь → кодовый замок).

Инструментарий технологий искусственного интеллекта использует принципы и подходы, аналогичные человеческому интеллекту, позволяя в автоматическом режиме обрабатывать значительные объемы данных, что обеспечивает более оперативное и релевантное решение задач по управлению государством, экономикой, формированию стратегий качественной жизни населения [2].

В рамках данного исследования и разработки «умного» классификатора в городской системе учета и инвентаризации объектов городского хозяйства использованы современные методы и подходы по использованию технологий искусственного интеллекта, таких как методы машинного обучения, компьютерное зрение, методы распознавания графических образов, статистический анализ данных. Применение данных методов и подходов обусловлено их актуальностью и перспективностью в рамках осуществления в Российской Федерации Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной указом Президента РФ от 10 октября 2019 г. № 490, и в рамках национальной программы «Цифровая экономика Российской Федерации». В документах подчеркивается, что применение новых цифровых технологий, направленных на повышение качества госуправления, является одной из основных и приоритетных задач для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства.

На текущем этапе исследования была разработана первая версия сервиса «умного» классификатора, в которой реализован базовый функционал, позволяющий загрузить или удалить фотоизображение, предоставляющий отдельные методы на основе YOLOv3 [3] по классификации и распознаванию [4] 11 типов объектов (элементов) на фотоизображении. Средняя точность распознавания объектов составляет около 78 %, значение функции потерь данного метода составляет 1.246 %. Методы реализованы на основе принципов REST API, что позволяет произвести интеграцию внешних систем с разработанным сервисом распознавания и классификации объектов, в частности интеграцию с интернет-порталом «Паспортизация объектов благоустройства Санкт-Петербурга».

Перспективами дальнейших исследований является расширение списка распознаваемых типов объектов, дальнейшее осуществление сбора и подготовки репрезентативного и сбалансированного набора обучающих данных. Будут продолжены работы по улучшению точности классификации и распознаванию объектов с применением других классов методов компьютерного зрения (семейство методов класса R-CNN [5]); использованию ансамблей моделей для достижения оптимального уровня критериев «качество-скорость»; проведению испытаний апробации сервиса в реальной среде и анализ полученных результатов.

Работа выполнена при поддержке гранта ПАО Сбербанк – Университет ИТМО в рамках темы № 50454 «Интеллектуальные технологии умного города в задачах обеспечения населения банковскими услугами».

СПИСОК ЛИТЕРАТУРЫ

1. Джабборов Д.Б. Большие данные, плановая экономика и государство // Вопросы политической экономии. 2019. № 4. С.96–101.
2. Косоруков А.А. Технологии искусственного интеллекта в современном государственном управлении // Социодинамика. 2019. № 5. С. 43–58.
3. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement. 2018. URL: https://pjreddie.com/darknet/yolo/ (дата обращения: 18.07.2020).
4. Zhao Z., Zheng P., Xu S., Wu X. Object Detection with Deep Learning: A Review // IEEE Transactions on Neural Networks and Learning Systems. 2019. P. 1–21. DOI: 10.1109/TNNLS.2018.2876865
5. He K., Gkioxari G., Dollár P., Girshick R. Mask R-CNN. 2018. URL: https://arXiv:1703.06870 (дата обращения: 19.07.2020).

УДК 004.9:351.9

ЭЛЕКТРОННЫЕ ПОРТАЛЫ КАК МЕХАНИЗМ СНИЖЕНИЯ СОЦИАЛЬНО-ПОЛИТИЧЕСКОЙ КОНФЛИКТОГЕННОСТИ: ОТНОШЕНИЕ НАСЕЛЕНИЯ К ЭЛЕКТРОННОМУ ВЗАИМОДЕЙСТВИЮ С ВЛАСТЬЮ

Белый Владислав Александрович, Чугунов Андрей Владимирович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: vladislav@itmo.ru chugunov@itmo.ru

Аннотация. В работе приводятся результаты исследования мнения граждан о том, какие направления развития электронных сервисов они считают приоритетными и отражающими насущные потребности жителей Санкт-Петербурга, проведенного Центром технологий электронного правительства Института дизайна и урбанистики Университета ИТМО. Проанализированы наиболее востребованные сервисы, эффективность имеющихся сервисов, изучены параметры учета мнения населения и доверия между субъектами взаимодействия при использовании онлайн-порталов.

Ключевые слова: электронные порталы; e-participation; умный город; конфликтогенность.

ELECTRONIC PORTALS AS A MECHANISM FOR REDUCING SOCIAL AND POLITICAL CONFLICTS POTENTIAL: POPULATION ATTITUDE TO ELECTRONIC INTERACTION WITH GOVERNMENT

Belyi Vladislav, Chugunov Andrei
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: vladislav@itmo.ru chugunov@itmo.ru

Abstract. The paper presents the results of the EGovernment Center of the Institute of Design and Urban Studies of ITMO University survey of citizens' opinions on which areas of development of electronic services they consider to be priorities and reflect the urgent needs of residents of St. Petersburg. The work analyzed the most demanded services, the effectiveness of the available services, studied the parameters of taking into account the opinion of the citizens and parameters of trust between citizens and government in e-participation.

Keywords: electronic portals; e-participation; smart city; conflict potential.

Работа представляет результаты опроса жителей Санкт-Петербурга об использовании каналов взаимодействия с властью и участия в управлении городом. Опрос был проведен в марте 2020 г. в сотрудничестве с системой Многофункциональных центров оказания государственных и муниципальных услуг (МФЦ) Санкт-Петербурга в шести районах города: в Василеостровском, Выборгском, Петроградском, Приморском, Московском, Фрунзенском с использованием метода анкетного опроса граждан, обратившихся за услугами в МФЦ. В опросе приняли участие 564 респондента. Выборка репрезентирует население Санкт-Петербурга по полу и возрасту.

Анкета содержала параметры для оценки доверия к технологиям, используемым для электронного взаимодействия населения с представителями органов власти и для получения государственных и общественных услуг, решения городских проблем и участия в управлении городом, оценки эффективности электронных сервисов, а также содержала параметры для оценки наиболее востребованных сервисов. В докладе представлены некоторые результаты этого исследования.

Сегодня Санкт-Петербург занимает одно из первых мест по уровню цифровизации в России. Жители Санкт-Петербурга активно используют местные порталы взаимодействия с властью, что подтверждается и результатами проведенного исследования. Государственные и муниципальные услуги через интернет «получают часто» около 40% петербуржцев. Ситуации, в ходе которых петербуржцы обращаются к порталам, свидетельствует о приоритете их использования как механизма взаимодействия с властью в заявительном, а не инициативном порядке. Население стремится получить качественные и быстрые услуги, заявить об имеющейся проблеме в сфере ЖКХ и благоустройства, или получить определенную информацию от органов государственной власти, а не проявить гражданскую инициативу. Показательно, что все исследуемые в опросе ситуации участия (кроме ситуации получения электронных услуг) набрали наибольшее чисто ответов «никогда» по отношению к частоте использования Интернета для взаимодействия с властью (см. табл. 1).

При этом современные инфокоммуникационные ресурсы и порталы электронного взаимодействия имеют серьезный потенциал для анализа и учета мнения населения, предотвращения и разрешения конфликтов. В ходе проведенного опроса было установлено, что у более 35% опрошенных есть уверенность в том, что посредством интернет-технологий можно донести позицию общества до власти. Около 21% считают, что Интернет позволяет решать проблемы коррупции в органах государственной власти.

Таким образом, налицо потенциал электронных ресурсов для снижения конфликтогенности в обществе. Открытое взаимодействие и конструктивная борьба за собственные права населения с использованием высокотехнологичных каналов должны быть интересны как для власти, пытающейся замалчивать многие из имеющихся противоречий, так и для населения, которое зачастую не способно отстаивать свои интересы и чья гражданская активность, в основном, проявляется в безвозмездной помощи малоимущим и нуждающимся. [1] Стоит отметить, что зарубежные исследователи отмечают необходимость активной позиции граждан цифрового государства, то есть использования электронных ресурсов не как высокотехнологичных каналов получения цифровых услуг, а как площадки активного взаимодействия и отстаивания собственных прав. В противном случае пассивность населения ставит под угрозу его экономические и гражданские свободы. [2] [3]

В дальнейшей перспективе исследований должно быть уделено внимание аспектам развития электронного участия граждан в условиях продолжающейся цифровизации, смены поколений и при различных сценариях социально-политического развития государства. Необходимо тщательнее проанализировать сервисы, используемые для инициативного взаимодействия с властью, а не просто представляющие собой альтернативу бумажным и очным обращениям.

Работа выполнена при поддержке Российского научного фонда, проект №18-18-00360 «Электронное участие как фактор динамики политического процесса и процесса принятия государственных решений».

СПИСОК ЛИТЕРАТУРЫ

1. Гражданская активность и общественные проблемы – URL: https://www.levada.ru/2020/04/27/grazhdanskaya-aktivnost-i-obshhestvennye-problemy/
2. Evans D., Yen D.C. E-government: An analysis for implementation: Framework for understanding cultural and social impact // Government Information Quarterly. 2005. Vol. 22 (3). P. 354–373. DOI: 10.1016/j.giq.2005.05.007
3. European E-Democracy in Practice. Springer Open, 2020. 359 p. DOI: 10.1007/978-3-030-27184-8.

УДК 303.42

ГИС СОВМЕСТНОГО УЧАСТИЯ В ИССЛЕДОВАНИИ ПОДРОСТКОВОЙ МОБИЛЬНОСТИ

Галактионова Анастасия Алексеевна, Ненько Александра Евгеньевна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: aagalaktionova@itmo.ru, al.nenko@itmo.ru

Аннотация. В докладе рассматривается результаты использования геоинформационной системы совместного участия (ГИССУ) в исследовании подросткового поведения и восприятия городской среды в Санкт-Петербурге.

Ключевые слова: ГИС совместного участия, совместное картирование, подростки, мобильность.

PPGIS IN TEENAGE MOBILITY RESEARCH

Galaktionova Anastasiia, Nenko Aleksandra
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: aagalaktionova@itmo.ru, al.nenko@itmo.ru

Abstract. The paper is dedicated to the Public Participation Geographic Information System (PPGIS) use in teenage behaviour and perception of urban environment in Saint-Petersburg.

Keywords: PPGIS, participatory mapping, teenage, mobility.

Совместное планирование является областью городского планирования, которой уделяется большое внимание за рубежом и, в последние года, в России [1, 2]. Геоинформационные системы (ГИС) совместного участия представляет собой один из перспективных методов совместного планирования, поскольку одно мероприятие вовлекает в среднем 200 человек, что гораздо больше, чем участников публичных слушаний или проектных воркшопов [3-5].

В феврале 2020 году Университет ИТМО заключил соглашения о сотрудничестве с двумя школами Санкт-Петербурга о проведении двух сессий с 210 учениками 7-11 классов с использованием ГИС совместного участия. Возрастная группа была выбрана с учетом знаний по географии. В рамках сессий школьников попросили отметить на картах свои дома, места, куда они ходят почти каждый день, нарисовать ежедневные маршруты на примере одного рабочего дня и отметить места, которые им нравятся или не нравятся. 67% подростков использовали онлайн-приложение Mapsurvay, разработанном в Лаборатории качества жизни Университета ИТМО. 33% подростков использовали распечатанные карты.

В результате проведенных сессий стало понятно, что для подростков не представляет труда использование цифровых или бумажных карт, а также правила использования онлайн-приложения. Основными недостатками со стороны пользователей были прерывистость работы школьного интернета, наличие на школьных компьютерах устаревших браузеров, а также внутренние ошибки приложения, которые приводили к необходимости многократно заполнять карты. Со стороны аналитики собранной информации недостатком стало отсутствие персональной идентификации участников. Легкость и быстрота работы с онлайн-приложением компенсировалась неоднородностью собранной информации. Например, часть участников нарисовала маршруты только до самой дальней точки пути, без уточнения является ли путь «туда» путем «обратно». Соответственно для расчета среднего ежедневного пешеходного пути была сделана выборка из 46 человек, по ним проверена вся информация из геоинформационного слоя «Маршруты» и вручную дополнены данные по длине пути обратно в QGIS и MS Excel. Дополнительные усилия аналитиков принесли любопытные результаты по подростковой мобильности. Оказалось, что планировочная городская структура почти не влияет на длину пешеходного пути, который в среднем составляет 3,9-4,6 км или 7800-9200 шагов. Также анализ плотности пешеходных потоков в QGIS выявил значительно большие сгущения плотности пешеходных потоков в более новом типе планировочной структуры, что противоречит интуитивным ожиданиям проектирующих градостроителей. Таким образом, ГИС совместного участия может быть эффективно использована в планировании транспортно-пешеходного каркаса города.

Работа выполнена при поддержке гранта РФФИ, проект № 20-013-00891 “Эмоциональное восприятие среды как фактор городской устойчивости (resilience)” 2020-2022.

СПИСОК ЛИТЕРАТУРЫ

1. Kahila-Tani M., Kytta M., Geertman S. Does mapping improve public participation? Exploring the pros and cons of using public participation GIS in urban planning practices //Landscape and urban planning. – 2019. – T. 186. – C. 45-55.
2. Федеральный проект «Формирование комфортной городской среды». – URL: http://gorodsreda.ru/federal-projects/gorodskaya-sreda/ (дата обращения: 20.07.2020).
3. Brown G. An empirical evaluation of the spatial accuracy of public participation GIS (PPGIS) data //Applied geography. – 2012. – Vol. 34. – P. 289-294.
4. Brown G., Kyttä M. Key issues and priorities in participatory mapping: Toward integration or increased specialization? //Applied geography. – 2018. – Vol. 95. – P. 1-8.

УДК 004.942:332.154

АНАЛИЗ ПРОСТРАНСТВЕННОГО ИНВЕСТИЦИОННОГО КОНТЕКСТА ПАМЯТНИКОВ КУЛЬТУРНОГО НАСЛЕДИЯ

Дрожжин Андрей Игоревич, Хрульков Александр Александрович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: drozhzhin@itmo.ru, oneonwar@itmo.ru

Аннотация. В ходе исследования изучается вопрос сохранения памятников культурного наследия, возможные пути сохранения таких объектов с учетом не только параметров самого объекта, но и факторов его ближайшего и дальнего окружения. В исследовании использованы методы пространственного анализа для изучения инвестиционной привлекательности таких объектов и вопросов неравномерности распределения финансов в настоящий момент.

Ключевые слова: культурное наследие; инвестиционная привлекательность; контекст памятника.

THE ANALYSIS OF SPATIAL INVESTMENT CONTEXT OF CULTURAL HERITAGE

Drozhzhin Andrei, Khrulkov Alexandr
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: drozhzhin@itmo.ru, oneonwar@itmo.ru

Abstract. The study examines the issue of preserving cultural heritage monuments, possible ways to preserve such objects, taking into account not only the parameters of the object itself, but also the factors of its immediate and distant surroundings. The study used the methods of spatial analysis to study the investment attractiveness of such objects and issues of uneven distribution of finance at the moment.

Keywords: cultural heritage; investment attractiveness; cultural preservation; cultural heritage context.

В данной работе исследуются объекты культурного наследия как объекты недвижимого имущества с исторически связанными с ними территориями, возникшие в результате исторических событий, представляющие собой ценность с точки зрения истории, археологии, архитектуры, градостроительства, искусства, науки и техники, эстетики, социальной культуры и являющиеся свидетельством эпох и цивилизаций, подлинными источниками информации о зарождении и развитии культуры [1]. К сожалению, не все подобные объекты, даже расположенные в культурных центрах, находятся в удовлетворительном или хорошем состоянии. Это связано с отсутствием финансирования. Источников два: государство и частное финансирование. Однако, многие памятники разрушаются, не получая финансирование ни из одного источника. Это связано в основном с тем, что затраты на первичное обследование памятников для решения вопроса их дальнейшего приспособления слишком дорого и не всегда приносит положительный ответ. В таком случае встает вопрос инвестиционной привлекательности такого рода объектов.

Рассмотрим вопрос на примере России. По мнению ряда исследователей [2**Ошибка! Источник ссылки не найден.**], современное российское государство изменило подходы к историко-культурному наследию, доставшемуся ему от предшествующих поколений. Если в советский период объектам истории и культуры придавалось в основном идейно-просветительское значение, то теперь они предстают как важнейший экономический ресурс, фактор формирования национального самосознания народа, образовательного и воспитательного процессов [3]. Иначе говоря, функциональное назначение памятников прошлого сейчас дополняют более весомым статусом, причем, в самых разных аспектах: экономическом, социальном и даже психологическом.

На данный момент охрана культурных объектов в нашей стране (да и не только) далеко не совершенна. Многие памятники уничтожены совсем недавно под разными предлогами. При этом некоторые, стоит признать, воссозданы с около-историческими фасадами. В любом случае в центрах городов из-за высокого спроса на землю, проблема стоит очень остро, несмотря на регулярное присутствие в дискуссиях градозащитников и общества и в СМИ [4, 5, 6]. А вот объекты, располагающиеся за пределами городских центров, с или без статуса значимых объектов, приходят в негодность из-за отсутствия надлежащего ухода. К тому же интерес к ним питают в основном только историки и местные жители. Исходя из всего вышесказанного, встает запрос на адекватное регулирование процессов сохранения наследия и его эксплуатации, с целью реализацией памятниками своей эстетической, исторической и смысловой ценности в полной мере.

Тема актуальна не только в России и, в частности, в Санкт-Петербурге, но и во всем мире, т.к. государства и крупный бизнес чаще всего вкладываются в содержание только знаковых памятников истории. Тема поднимается и популяризируется во многих странах, и существует множество вариантов не только по финансированию реставрации, но и по дальнейшей эксплуатации памятников. Однако многие из них либо имеют существенные минусы, либо имеющиеся предложения не применимы к другим объектам.

В данном исследовании предложен возможный подход, способствующий сохранению объектов культурного наследия с применением возможностей современных ИКТ.

Сохранение объекта культурного наследия предполагает выбор его дальнейшей судьбы (консервация, ремонт, реставрация, приспособление для современного использования). При этом практически все обследования того или иного объекта культурного наследия с целью его сохранения и/или коммерциализации обычно ограничиваются самим объектом, игнорируя его окружение [2-3, 7-9 и пр.]. Тем самым, текущее состояние объекта– это массив значений различных параметров объекта. Между тем, вместе с параметрами самого объекта его окружение ничуть не менее важная часть для определения его будущей судьбы. Таким образом, под контекстом объектов будем понимать характеристики окружающей среды и отношение объекта с другими объектами в определенном радиусе.

По степени влияния на объект контекст можно разделить условно на три группы параметров.

1. Микроконтекст: ближайшее окружение, ансамбль, куда входит объект, объекты досуга, располагающиеся в непосредственной близости. Размеры этого контекста ограничены площадью, улицей, максимум кварталом, где располагается объект.

2. Мезоконтекст: то, как воспринимает объект человек в городской среде (соседние объекты досуга, но уже на некотором расстоянии, жилые массивы, архитектурные панорамы). Его размер может разниться от

всего населенного пункта, в котором располагается или к которому приписан объект, если речь идет о небольших городах и селах, до микрорайона, если речь идет о крупном городе.

3. Макроконтекст: окрестные населенные пункты, рельеф, природа, схожие типологически объекты культурного наследия за пределами города/микрорайона. Размер этого контекста условно можно ограничить расстоянием, преодолеваемым автомобилем за половину светового дня от объекта.

Макроконтекст важен в основном для объектов, располагающихся за пределами крупных городов, тогда как микроконтекст и мезоконтекст важны для всех объектов.

Задача принятия управленческого инвестиционного решения, является важной и актуальной, особенно в связи с растущей цифровизацией и объемом информации, задача упрощения принятия подобных решений, на основании верхнеуровневых данных, доступных в интернете, напрямую связана со скоростью и успешностью принятия решений, как следствие на успех. На текущий момент подобные задачи решаются классическими экономическими методами прогнозирования денежных потоков и методами пространственного анализа, которые в свою очередь являются весьма современным решением, получившим особенное распространение в недавнее время, использующее современные методы пространственного анализа, которые открывают новые возможности в принятия инвестиционных решений [10].

Используя метод пространственного анализа, была создана карта привлекательности объектов культурного наследия Василеостровского района Санкт-Петербурга, в которой учитывался микро- и мезоконтекст. В центре внимания находятся объекты культурного наследия с зоной микроконтекста радиусом в 500 м. Попавшие в эту зону объекты можно разделить на культурное окружение (другие объекты культурного наследия, музеи, примечательные места и пр.), объекты транспортной доступности (остановки общественного транспорта, станции метро), рекреационное окружение (отели, магазины) и зеленые зоны. По первым трем группам отмечается количество, зеленые же зоны рассчитываются как площадь пересечения собственно этой зоны и радиуса микроконтекста.

Дальнейшее направление исследований может быть связано с расширением субъективных моментов в оценке привлекательности объекта, таких как возможные заинтересованные структуры и лица для работы с объектом, социальная оценка значимости сохранения объектов, история самого памятника.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 25 июня 2002 года № 73-ФЗ «Об объектах культурного наследия (памятниках истории и культуры) народов Российской Федерации».
2. Дударенко В.Н., Герасимов Н.М., Генин Л.В., Выдрин И.В. Органы местного самоуправления и сохранение объектов культурного наследия // Муниципалитет: экономика и управление. 2018. №3 (24). С. 11-19. URL: http://municipal.uapa.ru/issue/2018/03/02 (дата обращения: 09.05.2020).
3. Кулемзин А. М. Изучение охраны памятников в современной России // Вестник Кемеровского государственного университета. 2014. № 2. С. 53–58.
4. Лебедева И.В., Романова А.П., Якушенков С.Н. Массмедиа и консюмеризация культуры // Известия Волгоградского гос. пед. университета. 2012. №9. С. 71-74. URL: http://izvestia.vspu.ru/files/publics/73/71-74.pdf (дата обращения: 10.07.2020).
5. Мартышева О.М. Приватизация памятников истории и культуры: уничтожение или спасение? // Вестник ОмГУ. Серия. Право. 2010. №4. URL: https://cyberleninka.ru/article/n/privatizatsiya-pamyatnikov-istorii-i-kultury-unichtozhenie-ili-spasenie (дата обращения: 12.06.2020).
6. Болотова Е.Д. О необходимости установления уголовной ответственности за осквернение памятников истории и культуры // Вестник Московского гос. областного университета. Серия: Юриспруденция. 2020. №1. С. 115-121. DOI: 10.18384/2310-6794-2020-1-115-121. URL: https://vestnik-mgou.ru/Articles/Doc/13670 (дата обращения: 22.06.2020).
7. Крогиус В.Р. Исторические города России как феномен её культурного наследия. Москва: Прогресс-Традиция, 2009. 312 с.
8. Боголюбова Н.М., Николаева Ю.В. Охрана культурного наследия: международный и российский опыт // Вестник СПбГУКИ. 2014. № 4. С. 6-13.
9. Постников Д.А. Проблема использования объектов природного наследия в туристских целях. - Пермь: ПермГУ, 2016. – 235 с.
10. Cliquet G. Geomarketing: Methods and Strategies in Spatial Marketing. John Wiley & Sons, 2013. 327 p.

УДК 004.9

ФОРМИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ ДЛЯ ПРОЕКТИРОВАНИЯ СЕРВИСА ДИСТАНЦИОННОГО МОНИТОРИНГА ПОКАЗАТЕЛЕЙ ЗДОРОВЬЯ

Дьякова Валерия Александровна[1], Кононова Ольга Витальевна[1], Матросова Евгения Викторовна[2]

[1] Университет ИТМО

Биржевая линия, В.О., 14, Санкт-Петербург, 199034, Россия

[2] Санкт-Петербургское государственное бюджетное учреждение здравоохранения МИАЦ

Шкапина ул., 30, Санкт-Петербург, Россия, 198095

e-mails: dyakova.valery@yandex.ru, kononolg@yandex.ru, matrosovaE@spbmiac.ru

Аннотация. В статье представлены предварительные результаты работы по определению функциональных требований для проектируемого сервиса дистанционного мониторинга показателей здоровья в рамках приоритетного проекта Санкт-Петербурга «Электронное здравоохранение» и анализ типовых телемедицинских диагностических устройств.

Ключевые слова: дистанционный мониторинг здоровья, телемониторинг, диагностические устройства, телемедицина.

CREATING FUNCTIONAL REQUIREMENTS FOR DESIGNING A REMOTE HEALTH MONITORING SERVICE

Dyakova Valeriya[1], Kononova Olga[1], Matrosova Evgeniya[2]
[1] ITMO University
14 Birzhevaya line, Vasilievsky Island, St. Petersburg, 199034, Russia
[2] St. Petersburg State Budgetary Healthcare Institution MIAC
30 Shkapina St, St. Petersburg, 198095, Russia
e-mails: dyakova.valery@yandex.ru, kononolg@yandex.ru, matrosovaE@spbmiac.ru

Abstract. The article presents preliminary results of work on defining functional requirements for the projected remote monitoring service of health indicators in the framework of the priority project of St. Petersburg "E-health" and analysis of typical telemedicine diagnostic devices.

Keywords: remote health monitoring, telemonitoring, diagnostic devices, telemedicine.

Проекты цифровизации в сфере здравоохранения нацелены на повышение продолжительности и качества жизни населения, улучшение качества оказания медицинских услуг. Актуальным направлением в электронном здравоохранении в мире уже не первое десятилетие является телемедицина, обеспечивающая мониторинг состояния здоровья и доступность медицинских консультаций в онлайн-формате. Возможности телемедицины получили развитие с ростом доступности интернет и мобильных технологий для населения, повсеместного внедрения технологий машинное обучения, искусственного интеллекта, “умных" устройств и др. [1]. Прогнозируется увеличение спроса на услуги телемедицины, эффекты от удовлетворения которого обладают значительным экономическим потенциалом для системы здравоохранения и развития страховой медицины.

Диспансерное наблюдение больных хроническими неинфекционными заболеваниями с применением дистанционных технологий является одним из направлений телемедицины и зафиксировано, как одна из задач национального проекта в сфере здравоохранения [2].

В рамках приоритетного проекта Санкт-Петербурга «Электронное здравоохранение» планируется реализация электронных медицинских сервисов для пациентов, медицинских работников и руководителей сферы здравоохранения [3], в том числе сервиса дистанционного мониторинга показателей здоровья. Аналитическая работа и проектирование сервисов в Санкт-Петербурге проводится в СПб ГБУЗ МИАЦ.

Сервис дистанционного мониторинга показателей здоровья – это специализированный сервис медицинского назначения для удаленного контроля состояния здоровья пациентов с хроническими неинфекционными заболеваниями, который представляет собой информационную систему, имеющую интерфейсы для дистанционного подключения к ней различных устройств контроля жизненных показателей человека с возможностью беспроводной передачи информации, и обеспечивающую, как обработку и визуализацию полученной информации, так и возможность передачи ее для контроля лечащему врачу или в медицинское учреждение [4]. В первую очередь сервис предназначен для мониторинга показателей, свойственных заболеваниям артериальная гипертензия и сахарный диабет, показатели заболеваемости которыми имеют стабильно высокие значения. Для данных заболеваний был выявлен ряд параметров, которые будут контролироваться при дистанционном мониторинге.

Значения показателей, полученные автоматически с помощью диагностических устройств или внесенные в систему вручную пациентом, будут агрегированы и отображены в табличном и графическом представлениях, которые пациент и врач смогут посмотреть через свои личные кабинеты. В случае отклонения показателей от нормы врач и пациент получат об этом уведомления. В сервисе предусмотрены опросники для пациента, которые он должен будет заполнять по рекомендации врача. В личном кабинете пациент сможет узнать основную информацию о заболевании, получить рекомендации врача в режиме реального времени или в режиме отложенной телемедицинской консультации. Для врачей и контролирующих органов будет реализована генерация отчетов.

Планируется, что пациенты, которым необходимо дистанционное диспансерное наблюдение, могут быть оснащены измерительными приборами длительного пользования в рамках обязательного медицинского страхования, либо приобретут их самостоятельно. Для взаимодействия с сервисом дистанционного мониторинга показателей здоровья потребуются сертифицированные медицинские приборы, совместимые с сервисом, поэтому важно еще на этапе проектирования определить типовые диагностические устройства, с помощью которых возможна передача показателей здоровья пациента в автоматическом режиме, и основные требования к ним.

Базовый вариант использования диагностических устройств при дистанционном мониторинге показателей здоровья включает применение простых приборов, например, тонометров, глюкометров и пульсоксиметров, которые время от времени передают данные. Приборы должны быть легкими в использовании и достаточно прочными, чтобы их можно было применять в повседневной практике; поэтому удобство использования программного обеспечения и аппаратных средств этих приборов имеет существенное значение [5]. Диагностические устройства должны быть сертифицированы, соответствовать стандартам и требованиям, а также быть совместимыми с проектируемым сервисом.

Существует целый ряд документов для стандартизации взаимодействия с медицинскими приборами, который вносит свой вклад в обеспечение интероперабельности медицинских и персональных медицинских приборов.

Реализация сервиса позволит изменить схему взаимодействия врача и пациента. В новой модели не пациент будет определять время обращения к врачу, а медицинские работники на основании объективных данных приборов и информации от пациента принимают решение о способе и срочности контакта с пациентом для предотвращения развития обострений и осложнений заболеваний.

В работе представлены обобщенные промежуточные результаты исследования в рамках магистерской диссертации «Проектирование сервиса дистанционного мониторинга показателей здоровья в рамках приоритетного проекта Санкт-Петербурга «Электронное здравоохранение»». На следующем этапе работы планируется проектирование интерфейса сервиса дистанционного мониторинга показателей здоровья.

СПИСОК ЛИТЕРАТУРЫ

1. Лебедев Г.С., Фомина И.В., Шадеркин И.А., Лисненко А.А., Рябков И.В., Качковский С.В., Мелаев Д.В. Основные направления развития интернет технологий в здравоохранении (систематический обзор). // Электронный научный журнал «Социальные аспекты здоровья населения». 2017. №5. URL: http://vestnik.mednet.ru/content/view/923/30/ (дата обращения: 05.04.2020)
2. Национальный проект «Здравоохранение» // Министерство здравоохранения РФ [Электронный ресурс]. URL: https://www.rosminzdrav.ru/poleznye-resursy/natsproektzdravoohranenie (дата обращения: 10.03.2020)
3. Проект «Электронное здравоохранение» — СПб ГБУЗ МИАЦ [Электронный ресурс]. URL: http://spbmiac.ru/ehlektronnoe-zdravookhranenie/proekt-ehlektronnoezdravookhranenie/obshhee-opisanie/(дата обращения: 03.03.2020).
4. Глазова А. Ю., Набиев Р. Системы домашнего мониторинга пациентов с хроническими заболеваниями: принципы функционирования и перспективы развития // Российский семейный врач. 2013. Т. 17, №2, С.4-9
5. Леванов В.М., Перевезенцев Е.А. Возможности комплексного использования телемедицинских технологий в системе медицинского обеспечения работающего населения на удалённых территориях (обзор литературы) // Вестник новых медицинских технологий. Электронное издание. 2019. №1. Публикация 2-2. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2019-1/2-2.pdf (дата обращения: 13.04.2020).

УДК 37.14

ПРОЕКТИРОВАНИЕ МЕХАНИЗМА ВЗАИМОДЕЙСТВИЯ СТЕЙКХОЛДЕРОВ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ СФЕРЫ ЖКХ

Карачай Виталина Анатольевна[1], Корохова Инна Валерьевна[2], Шаталова Ольга Ивановна[3]
[1] Университет ИТМО
Биржевая линия, В.О., 14, Санкт-Петербург, 199034, Россия
[2] Управление жилищно-коммунального хозяйства администрации города Невинномысска
Гагарина ул., 55, г. Невинномысск, Россия, 357100
[3] Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
Лермонтова ул., 189, г. Ставрополь, Россия, 355000
e-mails: vatalinakarachay@gmail.com, InnaKV-24@yandex.ru, shatalovaolga77@yandex.ru

Аннотация. Рассматривается проблема взаимодействия юридически независимых стейкхолдеров при формировании экономически обоснованной стоимости услуг по содержанию общего имущества многоквартирного дома. В качестве решения данной проблемы предлагается использовать спроектированную авторами информационно-аналитическую систему, основанную на сервис-ориентированной архитектуре.

Ключевые слова: проектирование, ЖКХ, стоимость услуг, информационная система, сервис-ориентированная архитектура.

DESIGNING THE INFORMATION AND ANALYTICAL SYSTEM, CONTAINING THE STEKEHOLDERS' INTERACTION MACHANISM

Karachay Vitalina[1], Korokhova Inna[2], Shatalova Olga[3]
[1] ITMO University
14 Birzhevaya line, Vasilievsky Island, St. Petersburg, 199034, Russia
[2] Departament of Housing and Communal Services of the Administration in Nevinnomyssk city
55 Gagarina St, Nevinnomyssk, 357100, Russia
[3] The Russian Presidential Academy of National Economy and Public Administration (RANEPA)
189 Lermontov St, Stavropol, 355002, Russia
e-mails: vatalinakarachay@gmail.com, InnaKV-24@yandex.ru, shatalovaolga77@yandex.ru

Abstract. The issue of interaction of legally independent stakeholders in the formation of the economically justified cost of services for the maintenance of common property of the multy apartment building is considered. As a solution of this problem, it is proposed to use a designed by authors information and analytical system based on a service-oriented architecture.

Keywords: designing, housing and utilities, the cost utilities, information system, service oriented architecture.

В настоящее время осуществляется масштабное интегрирование информационных технологий в государственное и муниципальное управление с целью реорганизации бизнес-процессов, направленных на повышение эффективности соотношения качества и стоимости предоставляемых услуг для граждан. В связи

с этим, одним из приоритетных направлений исследований является сфера жилищно-коммунального хозяйства (далее - ЖКХ).

Актуальной проблемой сферы ЖКХ является осуществление контроля при формировании экономически обоснованной стоимости услуг по содержанию общего имущества многоквартирных домов (далее – ОИ МКД). Поскольку стейкхолдеры, участвующие в бизнес-процессе расчета экономически обоснованной стоимости услуг по содержанию ОИ МКД, являются юридически независимыми, следовательно, управляющие организации становятся неподконтрольными муниципалитету и могут формировать цены на свои услуги произвольно. Таким образом, возникает проблема формирования экономически обоснованной стоимости услуг по содержанию ОИ МКД [1].

Целью исследования является разработка механизма контроля формирования экономически обоснованной стоимости услуг по содержанию ОИ МКД при взаимодействии стейкхолдеров сферы ЖКХ [2].

Задачи исследования:

– анализ проблемы формирования экономически обоснованной стоимости услуг по содержанию ОИ МКД при взаимодействии стейкхолдеров;

– проектирование механизма взаимодействия институциональных единиц сферы ЖКХ;

– интегрирование обозначенного выше механизма при разработке информационно-аналитической системы расчета экономически обоснованной стоимости услуг по содержанию ОИ МКД.

В данном исследовании были проанализированы обращения граждан города Невинномысска в период 2015-2020 гг., касающиеся вопросов содержания ОИ МКД. Был проведен опрос собственников помещений относительно их участия в общих собраниях МКД. В ходе анализа обращений было выявлено, что наибольшее количество обращений содержат нарекания на несоответствие качества и стоимости услуг ЖКХ, а также отсутствие расшифровки по статьям затрат. Таким образом, возникает проблема отсутствия «прозрачности» формирования стоимости услуг по содержанию ОИ МКД. А отсутствие возможности цифрового участия (посредством информационных технологий) у определенных возрастных групп граждан порождает гражданскую пассивность.

Для решения проблемы формирования экономически необоснованной стоимости услуг по содержанию ОИ МКД был смоделирован механизм контроля формирования стоимости услуг, основанный на парадигме построения сервис ориентированной архитектуры (далее - СОА), которая включает в себя обмен данными посредством использования определенных сервисов.

Сервис (служба) – программный компонент, к которому можно удаленно обратиться, используя компьютерную сеть, и представляющая некоторые функциональные возможности запрашивающей стороны.

Сервисы обеспечивают бизнес-логику и средства управления состояниями, относящиеся к проблеме формирования экономически обоснованной стоимости услуг по содержанию ОИ МКД. Имея согласованные общие интерфейсы, они используют единые правила (контракт) для определения того, как вызывать сервисы и как они будут взаимодействовать друг с другом. СОА поддерживается языком WSDL (Web Services Description Language), в котором описание сервисов делится на интерфейс и оболочку. Интерфейс описывает содержимое запросов, а оболочка определяет протоколы транспорта и данных передачи по сети.

Работа с сервисами позволяет производить интеграцию запрашиваемых данных. Таким образом, спроектированный механизм включает в себя следующие необходимые сервисы [4]:

– сервис получения средней стоимости услуг по содержанию ОИ МКД;

– сервис оценки качества выполненных работ (услуг);

– сервис согласования стоимости выполненных работ;

– сервис предоставления образовательных курсов.

В результате выполненных действий, собственники помещений, а также специалисты сферы ЖКХ получат следующие преимущества:

– получение доступа к информации о качестве, стоимости, сроках выполнения работ, что будет способствовать заинтересованности собственников помещений в совместной деятельности с управляющими организациями по установлению стоимости работ, выполняемых управляющими организациями;

– повышение качества оказываемых услуг за счет возможности отслеживания недобросовестных подрядных организаций посредством получения отзывов о выполнении работ и услуг, и ведения рейтинговой системы в личном кабинете помещений на основе обратной связи от собственников помещений;

– снижение количества обращений граждан в административные органы муниципалитета по вопросам предоставления выполняемых услуг управляющими и подрядными организациями, привлекаемыми для выполнения работ (услуг).

Таким образом, при разработке информационно-аналитической системы будет внедрен механизм контроля формирования экономически обоснованной стоимости услуг по содержанию ОИ МКД. Помимо экономического эффекта от формирования экономически обоснованной стоимости услуг по содержанию ОИ МКД для всех институциональных единиц следует выделить и социальный эффект от внедрения информационно-аналитической системы, заключающийся в повышении уровня удовлетворенности граждан качеством выполняемых работ (услуг) [3].

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Правительства РФ от 06.05.2011 года № 354-ФЗ (ред. от 13.07.2019) «О предоставлении коммунальных услуг собственникам и пользователям в многоквартирных домах и жилых домов». СПС Консультант Плюс.
2. Постановление Правительства РФ от 26 декабря 2011 г. № 1498 «О вопросах предоставления коммунальных услуг и содержания общего имущества в многоквартирном доме». СПС Консультант Плюс.
3. Корохова И.В., Карачай В.А. Разработка и внедрение информационной системы расчета стоимости услуг в сфере ЖКХ г. Невинномысске Ставропольского края // Сборник тезисов докладов конгресса молодых ученных. Электронное издание. СПб: Университет ИТМО, 2019.
4. Корохова И.В., Шаталова О.И., Оптимизация сферы ЖКХ реализации национальной программы «Цифровая экономика» // Сборник докладов конференции по итогам работы Международной молодежной школы. Издательство: СЕКВОЙЯ, Ставрополь, 2019.

УДК 004.9:379.83

ЦИФРОВЫЕ ТРАНСФОРМАЦИИ ТУРИЗМА: ТЕНДЕНЦИИ И ПРИМЕРЫ-САНКТ-ПЕТЕРБУРГА

Кононова Ольга Витальевна[1], Прокудин Дмитрий Евгеньевич[2], Рябысько Юлия Сергеевна[1]
[1] Университет ИТМО
Биржевая линия, В.О., 14, Санкт-Петербург, 199034, Россия
[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mails: ovkononova@corp.ifmo.ru, hogben.young@gmail.com, u.rbs@yandex.ru

Аннотация. В ходе исследования осуществлено формирование терминологического ядра и сравнительный анализ понятийного аппарата предметной области. Выявлены актуальные направления и технологии, рассмотрены примеры трансформаций туризма Санкт-Петербурга.

Ключевые слова: цифровой туризм; электронный туризм; умный туризм; экосистема цифрового туризма; цифровые сервисы; цифровые технологии; цифровые решения.

DIGITAL TRANSFORMATION OF TOURISM ON THE INSTANCE OF ST. PETERSBURG

Kononova Olga[1], Prokudin Dmitry[1], Ryabysko Yuliya[2]
[1] ITMO University
14 Birzhevaya line, Vasilievsky Island, St. Petersburg, 199034, Russia
[2] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: ovkononova@corp.ifmo.ru, hogben.young@gmail.com, u.rbs@yandex.ru

Abstract. In the course of the study, the formation of the terminological core and a comparative analysis of the conceptual apparatus of the subject area were carried out. Relevant trends and technologies, examples of tourism transformation in St. Petersburg are considered.

Keywords: digital tourism; e-tourism; smart tourism; digital tourism ecosystem; digital services; digital technology; digital solutions.

Современный уровень цифровизации общества формирует новые формы взаимодействий между производителями и потребителями, в том числе и в области туристических услуг [1]. Производители туристских услуг вынуждены внедрять современные цифровые технологии, тем самым формируя новое направление – «цифровой туризм». Хотя устоявшегося определения термина «цифрового туризма» пока нет, в научном и медиа дискурсе предлагаются некоторые подходы и видение этого феномена через призму цифровизации. Так, в стратегии развития туризма до 2035 года [2] можно выделить группы понятий, ассоциируемые с цифровизацией: цифровые технологии, цифровые решения и цифровые сервисы. Цифровая форма туризма в документе не определена явным образом, но анализ научных публикаций позволил определить базовые термин-концепты, определяющих процессы цифровизации в туризме: цифровой туризм, интеллектуальный туризм, электронный туризм и ряд других [3-8].

Исследования в области цифрового, электронного, умного туризма не теряют актуальности и востребованности. Большинство зарубежных аналитиков считают полученные результаты недостаточными, отражающими лишь наиболее заметные аспекты происходящих цифровых трансформаций. В исследовании был использован авторский синтетический метод [9], направленный на извлечение контекстных знаний из неструктурированных или полуструктурированных информационных ресурсов.

К настоящему моменту широкое распространение в туристической отрасли получили технологии больших данных, интернета вещей (IoT), технологии дополненной реальности, искусственного интеллекта, блокчейн технологии, мобильные и интернет технологии [10]. Искусственный интеллект используется для автоматизации обслуживания самолетов, улучшения управления доходностью отелей и авиакомпаний, персонализации механизмов бронирования, управление трафиком аэропортов, работы чат-ботов на сайтах туристических компаний. Технологии виртуальной и дополненной реальности (AR / VR) в индустрии туризма нашли свое применение в навигации, информационной поддержке управления и организации экскурсионной деятельности, виртуальных путешествиях. Пример использования технологии Big Data – экспликация и анализ информации из различных источников, в том числе социальных сетей, для построения или выбора оптимальных маршрутов. Источники и актуальность данных обеспечиваются технологиями интернета вещей [11]. Так, сенсоры и датчики

в умном отеле могут собирать огромное количество данных, использование которых позволяет улучшить качество туристических продуктов, персонализировать обслуживание путешественников. При комплексном подходе к использованию этих технологий в будущем индустрия туризма станет качественно иной – максимально удобной для путешественников и прибыльной для предприятий отрасли. Использование мобильных устройств стало важнейшим трендом в туристическом бизнесе в последние годы.

Санкт-Петербург известен мобильными приложениями и сервисами, которые помогают туристам ориентироваться, делают их пребывание в городе комфортнее и насыщеннее. «Visit Petersburg.ru» – официальный городской туристический портал Санкт-Петербурга, который располагает большой базой объектов туристской индустрии города на девяти языках. Существуют и другие приложения-гиды для Санкт-Петербурга: «peterburg.center», «izi.TRAVEL», «KudaGo», «TripAdvisor» и другие. Приложения-гиды по музеям и достопримечательностям Петербурга: «Эрмитаж», «Кунсткамера. Гид по музею», «Казанский собор — аудиогид», «Эрарта 2.0», «RM Guide» (гид по русскому музею). С конца 2019 года в Санкт-Петербурге и Ленинградской области начали действовать электронные туристические визы. Технологии AR/VR в Санкт-Петербурге представлены следующим рядом: мобильное приложение «Музей улиц AR», VR-фильм «Эрмитаж VR. Погружение в Историю», виртуальный тур по музею РЖД, виртуальная автобусная VR экскурсия по Петербургу «Я вижу град Петров» и др. Использование данной технологии AR/VR позволяет снять барьеры и обеспечить культурный досуг всем категориям граждан даже в условиях пандемии.

Дальнейшее направление исследований может быть связано с расширением спектра рассматриваемых технологий и типов данных, полезных для туристической отрасли, а также рассмотрения туризма как одного из комплексных сложно структурированных компонентов социокультурного интернет пространства города.

СПИСОК ЛИТЕРАТУРЫ

1. Черевичко Т.В., Темякова Т.В. Цифровизация туризма: формы проявления // Изв. Сарат. ун-та. Нов. сер. Сер. Экономика. Управление. Право. 2019. Т. 19, Вып. 1. С. 59–64.
2. Об утверждении Стратегии развития туризма в Российской Федерации на период до 2035 года: Распоряжение Правительства РФ от 20.09.2019 г. № 2129-р // СЗ РФ. 2019. №39. Ст. 5460.
3. Kontogianni A., Alepis E. Smart tourism: State of the art and literature review for the last six years // Array. 2020. Vol. 6. 100020. DOI: 10.1016/j.array.2020.100020.
4. Li J., Xu L., Tang L., Wang S., Li L. Big data in tourism research: A literature review // Tourism Management. 2018. No. 68. P. 301-323. DOI: 10.1016/j.tourman.2018.03.009
5. Li Yu., Hu C., Huang Ch., Duan L. The concept of smart tourism in the context of tourism information services // Tourism Management. 2017. No. 58. P. 293-300. — DOI: 10.1016/j.tourman.2016.03.014
6. Molz J. G. Travel connections: Tourism, technology and togetherness in a mobile world. — London: New York, Routledge. 2012.
7. Navío-Marco J., Ruiz-Gómez L.M., Sevilla-Sevilla C. Progress in information technology and tourism management: 30 years on T and 20 years after the internet - Revisiting Buhalis & Law's landmark study about eTourism // Tourism Management. 2018. No. 69. P. 460–470. DOI: 10.1016/j.tourman.2018.06.002
8. Shaee S., Ghatari A.R., Hasanzadeh A., Jahanyan S. Developing a model for sustainable smart tourism destinations: A systematic review // Tourism Management Perspectives. 2019. No. 31. P. 287–300. DOI: 10.1016/j.tmp.2019.06.002
9. Кононова О.В., Ляпин С.Х., Прокудин Д.Е. Исследование терминологической базы междисциплинарного научного направления «цифровая экономика» с использованием инструментов контекстного анализа // International Journal of Open Information Technologies. 2018. Т. 6, № 12. С. 57-66.
10. Градинарова А.А. Современные тенденции цифровой трансформации в туристической отрасли // Труды конференции «Проблемы и перспективы развития туризма в Южном федеральном округе». – Симферополь: Изд-во «Типография «Ариал», 2017. С. 69-73.
11. Воронкова Л.П. Интернет как информационный ресурс международного туризма // Информационное общество. 2018. № 2. С. 49–53.

УДК 654

ОСНОВНЫЕ ПАРАДИГМЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ГОСУДАРСТВАХ АРКТИЧЕСКОГО СОВЕТА

Митько Арсений Валерьевич, Сидоров Владимир Константинович
Санкт-Петербургский университет государственной противопожарной службы МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Аннотация. В статье рассмотрены проблемы развития информационных технологий в Арктических регионах. В последнее время Арктика все больше привлекает внимание как регион с огромными потенциалами в сфере природопользования, развития судоходства и создания для этого необходимой инфраструктуры, а также как площадка для научного, культурного сотрудничества и туризма. Анализируя Арктические стратегии стран Северной Европы, можно сделать вывод, что правительства намерены работать над улучшением доступа Северных территорий к надежной и функционально цифровой инфраструктуре.

Ключевые слова: информационные технологии; парадигма, государство, Арктический совет.

MAIN PARADIGMS OF INFORMATION TECHNOLOGY DEVELOPMENT IN THE ARCTIC COUNCIL STATES

Mitko Arsenii, Sidorov Vladimir
Saint-Petersburg University of State Fire Service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Abstract. The article deals with the problems of development of information technology provision in the Arctic regions. Recently, the Arctic has been attracting more and more attention as a region with enormous potential in the field of natural resources, the development of shipping and the creation of the necessary infrastructure for this, as well as a platform for scientific, cultural cooperation and tourism. Analyzing the Arctic strategies of the Nordic countries, it can be concluded that governments intend to work to improve the access of the Northern Territories to a reliable and functional digital infrastructure.

Keywords: information technology; the paradigm of the state, the Arctic Council.

В эпоху повсеместной информатизации и автоматизации процессов, связанных с промышленностью, нефте- и газодобывающей индустрией, улучшением качества жизни и госуправления, вопрос о развитии инфокоммуникационных технологий (ИКТ) является приоритетным в рамках работы правительств северных стран. Общепризнанным фактом является характеристика Северной Европы как высокоразвитого Арктического региона. Так, согласно Индексу Человеческого развития, где один из основных критериев является коэффициент дифференциации уровня профессионального образования, отражающий различия в степени охвата обучением второй и третьей ступени образования, все 5 циркумполярных стран (Норвегия, Дания, Швеция, Исландия, Финляндия) находятся на лидирующих позициях, наравне с США Великобританией и Германией.

Органы исполнительной власти смогут эффективно выполнять работу с помощью электронных порталов. Например, правительство может обеспечить гражданам доступ к информации об удостоверениях личности и позволить им подавать заявки на оформление документов в Интернете [1]. Подобный подход поможет оптимизировать работу госучреждений на местах. Положительным фактором использования ИКТ является возможность обеспечения более активного политического участия местного населения в жизни страны и более эффективную реализацию социальных программ, направленных на борьбу с суицидом, алкоголизмом и безработицей.

Арктический регион в первую очередь ассоциируется с большими расстояниями между населенными пунктами, и только современные технологии могут сблизить людей, что важно, как для реализации социальных программ, так и для бизнес-сектора. Спутниковая навигация, мобильная связь и системы наблюдения также важны для поисково-спасательных работ и исследований вопросов изменения климата.

В Норвегии это университетский центр на Шпицбергене (UNIS), который является самым северным высшим учебным заведением в мире, расположенным в Лонгйире на 78º N. Одно из исследовательских направлений UNIS это арктические технологии. Также активно реализуются программы по изучению развития ИКТ в Арктике в столичном университете науки и техники. Исследования прикладного характера проводятся в многопрофильной научно-исследовательской и инновационной компании Norut. Исследователи имеют более чем 30-летний опыт, проводят фундаментальные исследования, прикладные исследования и коммерческие проекты.

Финский подход отличается унификацией структур и созданию общих групп, занимающихся определенным вопросом. Так, например, команда Arctic Finland стремится обеспечить устойчивое развитие с максимальной надежностью, безопасностью, качеством и эксплуатационной эффективностью технологий, которые используются в Арктике. В данную группу входят университеты и исследовательские центры, целью которой является создание научной базы для использования ноу-хау. Комбинированные доходы компаний Team Arctic Finland составляют 15 млрд. евро, что говорит о востребованности консолидирующего проекта. Одной из главных целей «команды» является привлечение инвестиций. С декабря 2017 года по январь 2018 года научный центр Arktikum провел выставку Arctic Expo 2017, на которой были представлены новейшие технологии, созданные для работы в экстремальных условиях, а также решения по обеспечению труднодоступных районов ИКТ. Благодаря ранее проведенным акциям по привлечению инвестиций, финнам удалось реализовать проект ICEYE. Это первая коммерческая спутниковая компания в Финляндии, история которой началась со спутникового проекта в Университете Аалто, входящего в команду Arctic Finland.

Основные научные работы Швеции в технологической сфере проводятся в Университете технологий Лулео. В сентябре 2017 года университет выступил с инициативой наладить сотрудничество с другими исследовательскими центрами арктического региона. Организованная университетом конференция впервые собрала 80 представителей научного сообщества. Было подписано соглашения о межвузовских программах по освоению Арктики с финскими и норвежскими университетами, в том числе в сфере развития ИКТ [2].

Датский университет технологий (DTU) является единственным университетом в Дании, предлагающим программу Arctic Technology. Программа предусматривает обучение высокоспециализированных специалистов, а также проведения исследований в данной области. Совместно с техническим колледжем Гренландии (Teknikimik Ilinniarfik, KTI) в Сисимиуте DTU создал исследовательский центр ARTEK, который имеет в сферах научных интересов развитие ИКТ в Гренландии. Центр финансируется за счет средств правительства Гренландии, частных фондов и DTU.

Исландия рассматривает вопросы развития ИКТ в рамках работы Совета исландской политики в области науки и техники, который тесно сотрудничает с центром исследований (RANNIS). Центр отчитывается перед Министерством образования, науки и культуры и действует в соответствии с Законом о государственной поддержке научных исследований. В мае 2017 года в г. Фэрбанксе, Аляска, прошел Арктический форум по вопросам широкополосного доступа в Интернет. Форум собрал экспертов, исследователей, педагогов, представителей промышленности и коренных народов, а также политиков со всего мира с целью обсуждения успехов и проблем в создании «Соединенной Арктики». Участниками форума стали более двухсот человек из 6 стран [3].

Программа «Онлайн вместе с библиотеками» (Online with Libraries, OWL) на Аляске, в Соединенных Штатах, обеспечивает образовательную поддержку жителей арктических территорий с помощью видеоконференций.

Программа OWL была запущена в 2011 году в форме проекта OWL с федеральным финансированием, предоставленным в рамках «Закона об оздоровлении национальной экономики и реинвестировании» 2009 г., и администрировалась через Программу по развитию технологий широкополосной связи Министерства торговли США. В 2013 г. успешный проект стал финансироваться штатом Аляска и был переименован в «Аляскинскую программу «Онлайн вместе с библиотеками». Программа объединяет 95 библиотек в разных уголках Аляски в сотрудничестве с Университетом Аляски и дает возможность организовывать телемосты с одновременным подключением до 10 объектов. Директор одной из библиотек говорит по этому поводу: «Расстояния между поселениями огромные, дорог туда нет. Видеоконференции зачастую являются единственным способом для жителей отдалённых районов получить высшее образование, пройти курсы повышения квалификации, обучиться родному языку, поучаствовать в занятиях и программах по истории и культуре, в медико-санитарных просветительских мероприятиях, пройти собеседование для приёма на работу» [4].

В целом, потенциал развития данной сферы высок, и совместная работа Арктических государств позволит улучшить нынешнее положения информационно-коммуникационных технологий, что в свою очередь послужит ощутимым импульсом для дальнейшего устойчивого развития Арктического региона.

СПИСОК ЛИТЕРАТУРЫ

1. Kristina Schönfeldt «The Arctic in International Law and Policy», Hart publishing, 2017.
2. Зайков К.С. «Инновационный вектор экономического развития северных и арктических территорий России и стран Северной Европы». Журнал «Экономические и социальные перемены: факты, тенденции, прогноз» Том 10, № 3, 2017.
3. Арктический форум по вопросам широкополосного доступа в Интернет // [Электронный ресурс]. URL: https://ru.uarctic.org/novosti/2017/5/arkticheskii-forum-po-voprosam-shirokopolosnogo-dostupa-v-internet-akfentiruet-vnimanie-na-obshie-potrebnosti-chast-1/ (дата обращения: 16.07.2020).
4. Арктический форум по вопросам широкополосного доступа в Интернет// [Электронный ресурс]. URL: https://ru.uarctic.org/novosti/2017/6/obrazovanie-i-zdravookhranenie-arkticheskii-forum-po-voprosam-shirokopolosnogo-dostupa-v-internet-akfentiruet-vnimanie-na-obshikh-potrebnostyakh-chast-2/ (дата обращения: 16.07.2020).

УДК 004.942:332.154

ЦЕННОСТНО-ОРИЕНТИРОВАННЫЙ ПОДХОД В КОНЦЕПЦИИ УМНОГО ГОРОДА

Митягин Сергей Александрович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: mityagin@itmo.ru

Аннотация. Рассматривается подход к построению умного города как комплекса решений, ориентированных на ценности, потребности и ожидания горожан. Методологической основой выступает системный подход к описанию жизни и активности горожан при их взаимодействии с городской средой, позволяющий выявлять, систематизировать и учитывать требования всех групп населения и других участников городского развития к условиям жизни в городе и активностям по преобразованию городской среды. Такой подход позволяет обеспечить соответствие решений и активностей, связанных с формированием умного города и преобразованием городской среды, условиям жизни и потребностям горожан.

Ключевые слова: умный город; ценности; потребности; ожидания; урбанистика.

VALUE-ORIENTED APPROACH IN SMART CITY VISION

Mityagin Sergey
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: mityagin@itmo.ru

Abstract. An approach to building a smart city as a set of solutions focused on the values, needs and expectations of citizens is considered. The methodological basis is a systematic approach to describing the life and activity of citizens in their interaction with the urban environment, which allows to identify, systematize and take into account the requirements of all population groups and other participants in urban development to the living conditions in the city and activities to transform the urban environment. This approach allows us to ensure that decisions and activities related to the formation of a smart city and the transformation of the urban environment correspond to the living conditions and needs of citizens.

Keywords: smart city; values; needs; expectations; urban studies.

Развитие городских территорий является сложным процессом, предполагающим организацию комплексов взаимосвязанных мероприятий, совместно обеспечивающих достижение поставленных целей развития. Для современных городов целеполагание развития территорий характеризуется значительной неоднозначностью. Целью развития современных городов является повышение качества жизни населения [1]. Однако это понятие носит субъективный характер и определяется во многом особенностями общества. Необходимо учитывать, что развитие современных городов может иметь нелинейные и сложно прогнозируемые эффекты, порождающие новые формы проблем и новые вызовы развитию городов, что не всегда сочетается с определением развития и противоречит целеполаганию [2, 3].

Такие особенности в условиях, в целом, успешности применения информационных технологий для управления отдельными процессами развития города характеризуют актуальность применения интеллектуальных технологий, для решения комплексных задач развития города как сложной социотехнической системы [4, 5]. Поэтому, одним из актуальных направлений исследований является разработка методов представления и обработки знаний о городе, что связано с современным периодом развития искусственного интеллекта [6].

Традиционными можно считать подходы, предполагающие сбор и последующую обработку городских данных для выработки решений в области управления городом и оптимизации городских процессов [7, 8]. Применение подхода, основанного на данных в управлении развитием городских территорий [9, 10].

В современных исследованиях рассматриваются формы представления знаний о городе в логике семантических структур городских объектов [11, 12]. Применение данного подхода обосновано развитием технологий BIM/CIM, предполагающих оцифровку городских объектов в новом технологическом цикле развития территорий. Данный подход, с одной стороны, требует значительного уровня детализации при описании городской среды [13]. В целом этот подход позволяет обеспечить построение семантических баз знаний о городе.

Однако, описанные особенности целеполагания и управления развитием городских территорий требуют восстановления знаний о фактическом использовании людьми городских территорий и возникающих в результате эффектах, полноте и разнообразии возможностей, предоставляемых городом человеку. Без ответа на эти вопросы невозможно обеспечить ожидаемое качество жизни в городе.

Предлагаемый подход нацелен на формирование общей методологии систематизации и представления знаний о городе и взаимодействия с городом представителей целевых групп населения, а также формируемых в результате этого взаимодействия жизненных сценариев. Применение предлагаемого подхода в задачах исследования и развития городских территорий должно обеспечить учет всех важных составляющих для создания комфортной городской среды для всех категорий горожан. Кроме того, учет формируемых жизненных сценариев как результатов взаимодействия людей с городской средой позволит сформулировать задачу создания городской среды, формирующей новые, целевые сценарии жизни в городе.

Выявление и оценка такого рода эффектов требует сбора и систематизации сведений в рамках четырех направлений:

Во-первых, описание исследуемой территории. Чаще всего территория определяется полигоном своих границ [14], а ее характеристики определяются использованием, с учетом нормативных и регламентных требований. Анализу в том случае подлежит городская среда, сформированная на исследуемой территории.

Во-вторых, описание заинтересованных сторон с точки зрения развития территории. При этом заинтересованными сторонами могут выступать как сами горожане, так и представители бизнеса, а также туристы и лица, временно пребывающие на территории города. Их описание требует достаточно подробной декомпозиции на целевые группы, так как от их состава зависит качество оценки территории. При этом необходимо учитывать изменчивость состава и потребностей горожан в различных ситуациях и во времени.

В-третьих, описание форм взаимодействия горожан с городской средой. Формы взаимодействия определяют способ удовлетворения потребностей горожанами используя рассматриваемую территорию. При этом необходимо учитывать несопоставимость отдельных форм взаимодействия [15].

В-четвертых, выявление и описание эффектов, возникающих в результате взаимодействия конкретных категорий горожан с конкретными составляющими городской среды. Фактически, оцениваемые эффекты являются производной от городской среды, состава горожан и форм их взаимодействия.

Полученная структура позволяет описать городскую среду на требуемом уровне детализации с учетом ее использования горожанами. Однако необходимо учитывать, что эта модель описывает фактическую ситуацию и не позволяет делать вывод о наличии недостающих элементов городской среды или необеспеченных жизненных стратегиях горожан. Этот подход может быть полезен для создания комфортных городов, предоставляющих необходимые, желательные и дополнительные возможности для горожан. То есть создания более конкурентоспособных и привлекательных городов для жизни. По этой причине предложенный подход назван жизне-ориентированным цифровым моделированием города, так как проживание в городе рассматривается как разнообразное множество всевозможных жизненных стратегий.

СПИСОК ЛИТЕРАТУРЫ

1. Psyllidis A., Bozzon A., Bocconi S., Bolivar C.T. A Platform for Urban Analytics and Semantic Data Integration in City Planning. Springer, 2015.
2. Стратегическое управление социально-экономическим развитием территорий: методологические основы и прикладной инструментарий: моногр. / под общ. ред. А.В. Мехренцева. Екатеринбург: Урал. гос. лесотехн. ун-т, 2015. 235 с.
3. Agarwal A.K., Singh A.K. Management and Socio-Economic Development. Mittal Publications New Delhi, 2014.
4. Zhang Y. et al. Real-time Machine Learning Prediction of an Agent-Based Model for Urban Decision-making //Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems. – International Foundation for Autonomous Agents and Multiagent Systems, 2018. P. 2171-2173.
5. Kontokosta C. E., Tull C. A data-driven predictive model of city-scale energy use in buildings //Applied energy. 2017. Vol. 197. P. 303-317. DOI: 10.1016/j.apenergy.2017.04.005
6. Wu N., Silva E.A. Artificial intelligence solutions for urban land dynamics: a review // Journal of Planning Literature. 2010. Vol. 24 (3). P. 246-265. DOI: 10.1177/0885412210361571
7. Hawas M.A. Are We Intentionally Limiting Urban Planning and Intelligence? A Causal Evaluative Review and Methodical Redirection for Intelligence Systems // EEE Access. 2017. Vol. 5. P. 13253-13259. DOI: 10.1109/ACCESS.2017.2725138
8. Alonso L., Zhang Y.R., Grignard A., Noyman A., Sakai Y., ElKatsha M., Larson K. Cityscope: a data-driven interactive simulation tool for urban design. Use case volpe // International Conference on Complex Systems. Springer, Cham, 2018. P. 253-261. DOI: 10.1007/978-3-319-96661-8_27
9. Liu F., Zheng X., Huang Q. Predictive measurement of the structure of land use in an urban agglomeration space // Sustainability. 2017. Vol. 10 (1). P. 1-16. DOI: 10.3390/su10010065

10. Liu L. et al. A machine learning-based method for the large-scale evaluation of the qualities of the urban environment // Computers, Environment and Urban Systems. 2017. Vol. 65. P. 113-125. DOI: 10.1016/j.compenvurbsys.2017.06.003
11. Stojanovski T. City information modeling (CIM) and urbanism: Blocks, connections, territories, people and situations // SimAUD '13 Proceedings of the Symposium on Simulation for Architecture & Urban Design, Society for Computer Simulation International. 2013. P. 86-93.
12. Buccella A., Cechich A., Gendarmi D., Lanubile F., Semeraro G., Colagrossi A. Building a global normalized ontology for integrating geographic data sources / A. Buccella, A. Cechich, D. Gendarmi, F. Lanubile, G. Semeraro, A. Colagrossi // Comput. Geosci. 2011. Vol. 37, № 7. P. 893–916. DOI: 10.1016/j.cageo.2011.02.022
13. Simonelli L., Amorim A. L. City Information Modeling: General Aspects and Conceptualization // American Journal of Engineering Research. 2018. Vol. 7 (10). P. 319-324.
14. Rodoman B.B. Districting As a Way of Possessing Space // Regional Research of Russia. 2019. Vol. 8. P. 301-307. DOI: 10.1134/S2079970518040081
15. Magarotto M., de Deus R.F., Costa M.F., Masanet E. Green areas in coastal cities – Conflict of interests or stakeholders' perspectives? // International Journal of Sustainable Development and Planning. 2017. Vol. 12, № 8. P. 1260–1271. DOI: 10.2495/SDP-V12-N8-1260-1271.

УДК 303.42

ГИС СОВМЕСТНОГО УЧАСТИЯ В КАК ПЕРСПЕКТИВНЫЙ ЦИФРОВОЙ ИНСТРУМЕНТ ГОРОДСКИХ ИССЛЕДОВАНИЙ

Ненько Александра Евгеньевна, Галактионова Анастасия Алексеевна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: al.nenko@itmo.ru, aagalaktionova@itmo.ru

Аннотация. В статье рассматриваются геоинформационные системы совместного участия (ГИССУ) как цифрового инструмента городских исследований, который позволяет анализировать пространственное поведение и пространственные предпочтения жителей города. Главная ценность ГИССУ - вовлечение конечных пользователей в картирование повседневных практик использования конкретной городской территории или всего города, преимуществ и недостатков территории, а также запросов на новые качества и функциональное наполнение территории. Приводится описание преимуществ инструмента, описываются возможные области применения и приводятся кейсы использования ГИССУ Mapsurvey в исследованиях Университета ИТМО.

Ключевые слова: ГИС совместного участия, совместное картирование, городские исследования, городское развитие, цифровые инструменты общественного участия, Mapsurvey.

PPGIS AS A PERSPECTIVE DIGITAL TOOL FOR URBAN RESEARCH

Nenko Aleksandra, Galaktionova Anastasiia
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: al.nenko@itmo.ru, aagalaktionova@itmo.ru

Abstract. The paper considers public participation geographic information systems (PPGIS) as a digital tool for conducting urban research, apt for analyzing spatial behaviour and spatial preferences of the city inhabitants. PPGIS' major value is involvement of the end users into mapping their everyday activities of a certain urban territory or the whole city, their favourite and disliked places, positive and negative features of the territory as well as demand for new qualities and functionality of the territory. The advantages of the tool are described and the possible areas of implementation on various spheres of urban development are given, followed with illustrations of application of Mapsurvey PPGIS in ITMO University studies.

Keywords: PPGIS, participatory mapping, urban research, urban development, public participation digital tool, Mapsurvey.

Геоинформационные системы общественного участия (на англ. PPGIS - public participation GIS) уже более 40 лет активно применяются в городском планировании и развитии [1]. ГИС общественного участия - это "сфера географической информационной науки, которая фокусируется на том, как публики используют геопространственные технологии для участия в общественных процессах, таких как картирование и принятие решений" [2]. Совместное картирование уходит своими корнями в исследования К. Линча и С. Милгрэма, посвященных ментальному картированию - анализу воспринимаемого образа города, а также в практики "народной географии", которые фокусируются на повседневном использовании городского пространства жителями [3-5].

ГИС общественного участия направлены на изучение пространственного поведения и пространственных предпочтений человека. Они позволяют получить ответы на вопросы, которые имеют пространственную привязку, а именно:

а) вопросы о повседневных привычных (рутинных) практиках и маршрутах: "Где Вы обычно гуляете в этом районе?", "Каким путем Вам обычно ходите в школу?";

б) вопросы об эмоциональном восприятии пространства: "Какие места в этом районе Вы любите и считаете значимыми для района?", "По каким дорогам Вы не любите, боитесь ходить?";

в) вопросы о желаемых новых качествах и функциях пространства: “Где, на Ваш взгляд, стоило бы сделать новую зеленую зону в этом районе?”, “Где, на Ваш взгляд, необходимо сделать дополнительное освещение улиц в этом районе?”.

Структура инструментов ГИССУ обычно сочетает в себе черты классического социологического опросного листа, но при этом имеется возможность отметить ответы на вопросы на интерактивной карте в виде точек, линий или полигонов. ГИС совместного участия является перспективным цифровым инструментом совместного исследования и планирования города, поскольку одно мероприятие вовлекает в среднем 200 человек, то есть, гораздо больше среднего числа участников публичных слушаний или проектных семинаров [6].

Преимущества ГИС общественного участия как инструмента сбора и анализа данных в рамках городских исследований таковы:

– субъектность - непосредственное участие пользователя в сборе данных, которое приводит к повышению ответственности, точности регистрации мнения конечного пользователя;
– субъективность - возможность изучения субъективных ландшафтов городского пространства, например, эмоционального ландшафта (сочетания привлекательных и отталкивающих мест в районе или в городе);
– гибкость - возможность варьирования различных инструментов выражения социального мнения, вербализация и субъективное геокодирование;
– точность - точная пространственная привязка субъективного мнения к пространству;
– тиражируемость - цифровая природа инструмента позволяет воспроизводить городские исследования.

Вследствие данных преимуществ, области применения ГИС общественного участия в анализе городских процессов и явлений и городском развитии достаточно обширны:

– городское планирование, формирование мастер-планов;
– создание сред, дружественных к определенным социальным группам (например, детям - “город для детей”);
– оптимизация размещения городских сервисов и инфраструктуры;
– изучение мнений сообществ, имеющих пространственную привязку (соседские сообщества);
– изучение естественной структуры города - альтернативных центров, вернакулярных районов;
– брендинг и плейсмейкинг территорий.

Лаборатория качества городской жизни Института дизайна и урбанистики Университета ИТМО разработала ГИССУ Mapsurvey, с помощью которой проводит исследования качества городской жизни и качества городской среды. Среди примеров исследований - изучение набережных малых рек Санкт-Петербурга с точки зрения текущего использования и перспективных, значимых для пользователей, вариантов развития набережных; исследование безопасности перемещения, мест повседневной активности и эмоционально значимых мест школьников Санкт-Петербурга, живущих в районах с различной морфологией застройки; исследование рекомендуемых (символически значимых) и актуальных (реально используемых) мест для романтических свиданий в городе.

Работа выполнена при поддержке гранта РФФИ, проект № 20-013-00891 “Эмоциональное восприятие среды как фактор городской устойчивости (resilience)” 2020-2022.

СПИСОК ЛИТЕРАТУРЫ

1. Brown G., Kyttä M. Key issues and priorities in participatory mapping: Toward integration or increased specialization? //Applied geography. – 2018. – Vol. 95. – P. 1-8.
2. Tulloch D. Public participation GIS (PPGIS) //Encyclopedia of geographic information science. – SAGE Publications, 2008. – P. 352-355.
3. Линч К. Образ города. М.: Стройиздат, 1982. С. 5.
4. Milgram S. Psychological maps of Paris // Environmental Psychology. – New York, 1976. – P. 88-113.
5. Egenhofer M. J., Mark D. M. Naive geography //International Conference on Spatial Information Theory. – Springer, Berlin, Heidelberg, 1995. – P. 1-15.
6. Brown G. An empirical evaluation of the spatial accuracy of public participation GIS (PPGIS) data // Applied geography. – 2012. – Vol. 34. – P. 289-294.

УДК 004.8

СИСТЕМА МОНИТОРИНГА УДОВЛЕТВОРЕННОСТИ НАСЕЛЕНИЯ КАЧЕСТВОМ ЖИЗНИ-В ГОРОДЕ

Олисеенко Валерий Дмитриевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: vdo@dscs.pro

Аннотация. Рассматриваются методы и средства разработанные в процессе изучения социоинженерных атак и социальных сетей позволяющие автоматизировать анализ социальных сетей для выявления настроений жителей города, получение рейтингов муниципальных служб.

Ключевые слова: социальные сети; идентификация пользователя; машинное обучение; оценка удовлетворенности пользователей.

MONITORING SYSTEM OF POPULATION SATISFACTION WITH THE QUALITY OF LIFE-IN THE CITY

Oliseenko Valerii
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: vdo@dscs.pro

Abstract. The methods and tools developed in the process of studying socioengineering attacks and social networks that allow automating the analysis of social networks to identify the mood of city residents, obtaining ratings of municipal employees are considered.

Keywords: social networks; user identification; machine learning; user satisfaction assessment.

Современный мир меняется огромными темпами. Часто муниципальные службы, чиновники не могут оперативно реагировать на изменения в общественном запросе [1]. Для решения данной проблемы предлагается создание комплекса автоматизации оценки удовлетворенности жителей жизнью в городе, действиями муниципальных служб, чиновников, инфраструктурой и прочими аспектами. Предполагается создание теоретической и практической (прикладной, программной) основы для получения оценок посредством анализа комментариев и постов в социальных сетях с применением методов машинного обучения.

Для получения оценок развивается идея обнаружения психологических особенностей пользователя, представленная в [2] По полученным оценкам можно будет скорректировать действия администрации города (районов), муниципальных служб и прочих причастных людей для повышения удовлетворенности жителей. Кроме того, объектом анализа могут также выступать ресурсы гражданских инициатив (change.org и т.п.).

Таким образом, разработанный комплекс поможет, в соответствии с пунктом стратегии научно-технологического развития Российской Федерации [3]: “сформировать эффективную современную систему управления в области науки, технологий и инноваций, обеспечивающую повышение инвестиционной привлекательности сферы исследований и разработок, а также эффективности капиталовложений в указанную сферу, результативности и востребованности исследований и разработок”. Комплекс поможет улучшить взаимодействие с муниципальными властями, что повлечёт за собой повышения доверия граждан и улучшение инвестиционного климата городов РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Сантрян Н. А., Момотова О. Н. Проблемы муниципальной службы в современном российском обществе // Kant. 2014. №3 (12). URL: https://cyberleninka.ru/article/n/problemy-munitsipalnoy-sluzhby-v-sovremennom-rossiyskom-obschestve (дата обращения: 18.07.2020).
2. Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей // СПб. ГУАП, 2018. 266 с. ISBN 978-5-8088-1377-5.
3. Стратегия научно-технологического развития Российской Федерации [Электронный ресурс]. URL: http://нтр.рф (дата обращения: 19.07.2020).

УДК 004.9:351.9

РАЗВИТИЕ ПОРТАЛОВ ЭЛЕКТРОННОГО УЧАСТИЯ НА РЕГИОНАЛЬНОМ И МУНИЦИПАЛЬНОМ УРОВНЕ В РОССИИ: РЕЗУЛЬТАТЫ МОНИТОРИНГА 2019 ГОДА

Панфилов Георгий Олегович[1], Кабанов Юрий Андреевич[1,2], Чугунов Андрей Владимирович[1]
[1] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] Национальный исследовательский университет «Высшая школа экономики» (Санкт-Петербург)
Канала Грибоедова наб., 123, Санкт-Петербург, 190068, Россия
e-mails: panfilovgeorg@mail.ru, ykabanov@itmo.ru, chugunov@itmo.ru

Аннотация. В докладе представлены основные результаты исследования Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО, посвященного оцениванию веб-ресурсов электронного участия в регионах России. Методика позволяет оценить различные каналы электронного участия и осуществить кросс-региональные и кроссплатформенные сравнения. В декабре 2019 – январе 2000 было оценено 198 региональных и 155 муниципальных ресурсов электронного участия шести основных типов во всех 85 регионах России. Был построен общий рейтинг, отображающий уровень развития рассматриваемых ресурсов – их распространённость в регионах и качество реализации.

Ключевые слова: информационные ресурсы; порталы электронного участия; e-participation; регионы России; мониторинг; рейтингование.

E-PARTICIPATION PORTALS DEVELOPMENT AT THE REGIONAL AND MUNICIPAL LEVEL IN RUSSIA: 2019 MONITORING RESULTS

Panfilov Georgii[1], Kabanov Yury[1 2], Chugunov Andrei[1]
[1] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
[2] National Research University Higher School of Economics (St. Petersburg)
123 Griboedova Canal Emb, St. Petersburg, 190068, Russia
e-mails: panfilovgeorg@mail.ru, ykabanov@itmo.ru, chugunov@itmo.ru

Abstract. The report presents the main results of a comprehensive study of the resources of electronic participation in the regions of Russia, carried out in December 2019 – January 2020. The study was conducted using a methodology that allows us to evaluate various web resources of electronic participation and make cross-regional and cross-platform comparisons. The methodology was applied to evaluate 198 regional and 155 municipal resources of six basic types in all 85 regions of Russia. As a result, a rating of regions was built according to the general level of development of electronic participation.

Keywords: information resources; electronic participation portals; e-participation; Russian regions; monitoring; rating.

Работа представляет результаты мониторинга порталов электронного участия в российских регионах. Мониторинг проводился Центром технологий электронного правительства Института дизайна и урбанистики Университета ИТМО в 2019 г. Он развивает методику и результаты, полученные в 2017 - 2018 гг. [1], и направлен на более широкий и системный анализ состояния электронного участия по шести ключевым каналам: сайты подачи жалоб и заявлений, электронные петиции, электронные голосования, порталы инициативного бюджетирования, порталы открытого бюджета и краудсорсинг. Помимо региональных порталов, оценивалось также и состояние электронного участия на муниципальном уровне.

Методика мониторинга основана на системном подходе [2] и включила в себя 15 индикаторов, по каждому выставлялась оценка от 0 до 2 баллов. В итоговую выборку вошли 198 ресурсов регионального и 155 - муниципального уровня (см. табл. 1). По полученным данным был построен общий рейтинг, отображающий общую ситуацию в регионах (муниципалитетах), а также рейтинг по каждому из шести типов ресурсов.

Результаты мониторинга демонстрируют существенный разброс итогового балла по регионам (от 0 до 83) и муниципалитетам (то 0 до 62). Различаются и подходы властей в том, какие каналы развивать и использовать. Так, если порталы открытого бюджета присутствуют во всех регионах, то порталы электронных петиций, голосований и краудсорсинговые платформы встречаются редко, в основном, в регионах – лидеров.

В целом, в регионах лучше развиваются «информационные» ресурсы (например, открытый бюджет), нежели механизмы более активного вовлечения граждан в городские или региональные процессы принятия решений.

К регионам с относительно развитыми механизмами электронного участия по результатам мониторинга можно отнести 32 субъекта. Как правило, в таких субъектах каналы электронного участия реализованы на достаточно высоком уровне и отличаются разнообразием: присутствуют ресурсы типа «открытый бюджет», ресурсы для инициативного бюджетирования и сообщения о проблемах.

В результате исследования выявлена позитивная тенденция создания платформенных решений и комплексных ресурсов, объединяющих различные каналы электронного участия, что позволяет гражданам не только фиксировать нарушения или недостатки, но и предлагать пути решения проблем, а также вступать в прямой диалог с представителями органов власти по этим вопросам.

Используемая методика оценка доказала свою валидность и применимость для дальнейшего использования. Данные доступны в различных разрезах, что позволяет кастомизировать рейтинг под конкретные исследовательские, аналитические и управленческие задачи.

С научной точки зрения, мониторинг отражает важные характеристики состояния электронного участия в контексте регионального и муниципального развития. Показанные различия нуждаются в объяснении, и данные мониторинга могут стать зависимой переменной в анализе факторов, способствующих или препятствующих развитию электронного участия. Перспективными тут представляются сопоставления полученных данных с социально-экономическими показателями, а также уровнем развития информационного общества в регионах. Используя данные мониторинга в качестве независимой переменной, возможно, в частности проследить соотношение развития электронного участия и эффективности регионального управления.

С практической точки зрения, полученный рейтинг может быть полезен лицам, принимающим решения, в частности, отвечающим за информатизацию государственного управления и взаимодействие с гражданами. Данные позволяют определить преимущества и недостатки разработанных каналов электронного участия, определить слабые места и точки роста. Кроме того, существует возможность сопоставления показателей регионов и муниципалитетов между собой.

В дальнейшем команда исследователей планирует продолжение ежегодного мониторинга в сочетании с применением иных методов.

Работа выполнена при поддержке Российского научного фонда, проект №18-18-00360 «Электронное участие как фактор динамики политического процесса и процесса принятия государственных решений».

СПИСОК ЛИТЕРАТУРЫ

1. Чугунов А.В., Кабанов Ю.А., Федяшин С.В. Развитие электронных приемных в регионах Российской Федерации: результаты пилотного исследования в 2017-2018 гг. // Информационные ресурсы России. 2019. № 3. С. 32- 36.
2. Кабанов Ю.А., Панфилов Г.О., Чугунов А.В. Мониторинг ресурсов электронного участия: методика и некоторые результаты // Государство и граждане в электронной среде. Выпуск 4 (Труды XXIII Международной объединенной научной конференции «Интернет и современное общество», IMS-2020, Санкт-Петербург, 17 – 20 июня 2020 г. Сборник научных статей). — СПб: Университет ИТМО, 2020.

УДК 528.93.516.004

АЛГОРИТМЫ И МЕТОДИКА КАРТОГРАФИЧЕСКОЙ ГЕНЕРАЛИЗАЦИИ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ 3D МОДЕЛЕЙ ГОРОДОВ

Присяжнюк Сергей Прокофьевич[1], Аль-Дамлахи Июссеф[2]
[1] ЗАО «Институт телекоммуникаций»
Кантемировская ул., 5, Санкт-Петербург, 194100, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: office@itain.ru, Youssef.d-86@mail.ru

Аннотация. Предлагается методика и алгоритмы для генерализации объектно-ориентированных трехмерных объектов моделей города с целью их использования в ситуационных центрах управления города лицом принимающего решения поставленных задач для повышения детальности их отображения в любом масштабе с изменением расстояния обзора.

Ключевые слова: генерализация; объектно-ориентированная модель; трехмерная модель города; ситуационный центр управления города; трехмерная модель здания.

ALGORITHMS AND METHODOLOGY FOR CARTOGRAPHIC GENERALIZATION OF OBJECT-ORIENTED 3D CITY MODELS

Prisyazhnyuk Sergey[1], Al-Damlakhi Youssef[2]
[1] JSC "Institute of Telecommunications"
5 Kantemirovskaya St, St. Petersburg, 194100, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: office@itain.ru, Youssef.d-86@mail.ru

Abstract. A methodology and algorithms are proposed for generalizing object-oriented three-dimensional objects of city models with the aim of using them in emergency management situational city center by a decision maker to increase the detail of their display at any scale with changing the view distance to solve the assigned tasks.

Keywords: generalization; object oriented model; three-dimensional city model; emergency management situational city center; three-dimensional building model.

В современных условиях роль геоинформационного обеспечения ситуационных центров управления городами многократно возрастает с учетом активного и массового внедрения в управление специальных геоинформационных технологий с объектно-ориентированной электронной картографией. Возникает остро потребность оперативно в мультимасштабном виде представить лицам, принимающим решения объектно-ориентированную трехмерную модель города повышенной точности.

Существующие алгоритмы и методики трехмерной генерализации для отображения трехмерных объектов города не удовлетворяет требованиям по точности и оперативности, поскольку они предназначены для получения генерализованных моделей зданий только при определенных уровнях детализации как LoD2 – LoD4. Для обеспечения мягкого перехода между трехмерными моделями зданий с изменением масштаба и расстояния обзора возникает потребность разработки алгоритма и методики генерализации трехмерных моделей зданий в любом масштабе и с любом расстоянием обзора для повышения точности отображения деталей моделей зданий в реальном времени. В ситуационном центре управления города потребуется представления и отображения трёхмерных моделей города лицом, принимающим ращения с отображением деталей этих объектов в реальном времени, чтобы дать более точное представление и повысить восприятие человека, принимающего решения поставленных задач таких как реагирование на чрезвычайные ситуации и др. Поэтому разработка методики и алгоритмов оперативной генерализации объектно-ориентированной трёхмерной модели городов повышенной точности является насущной задачей.

Однако вопрос разработки эффективных алгоритмов картографической генерализации, объектно-ориентированной трехмерных моделей городов и методики их реализации не рассматривался.

В докладе предложены эффективные алгоритмы генерализации 3D моделей городов с полиноминальной временной и емкостной сложностью и методика их реализации в ситуационных центрах городов.

СПИСОК ЛИТЕРАТУРЫ

1. Kolbe T. H., Gröger G., Plümer L. CityGML–3D city models and their potential for emergency response //Geospatial information technology for emergency response. – 2008. – С. 257-274.
2. Lee J. A three-dimensional navigable data model to support emergency response in microspatial built-environments //Annals of the Association of American Geographers. – 2007. – Т. 97. – №. 3. – С. 512-529.
3. Mao B., Ban Y., Harrie L. A Framework for generalization of 3D city models based on CityGML and X3D //ISPRS Workshop on Quality, Scale and Analysis Aspects of Urban City Models. – 2009.
4. Trapp M. et al. 3D generalization lenses for interactive focus+ context visualization of virtual city models //2008 12th International Conference Information Visualisation. – IEEE, 2008. – С. 356-361.
5. Tsai F., Lin W. J., Chen L. C. Method of Generalizing 3-Dimensional Building Models Having Level of Detail+ : заяв. пат. 13548826 США. – 2013.
6. Uyar A., Ulugtekin N. N. A proposal for generalization of 3D models //ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences. – 2017. – Т. 4. – С. 389.

УДК: 378.046

СОЗДАНИЕ ГОРОДСКОГО ЦЕНТРА ПО ПРОФОРИЕНТАЦИИ И СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКОЙ АДАПТАЦИИ ВОЕННОСЛУЖАЩИХ, ПРОХОДЯЩИХ СЛУЖБУ В ВС РФ И УВОЛЬНЯЕМЫХ В РЕЗЕРВ, ДЛЯ ВЫСОКОТЕХНОЛОГИЧНОЙ ИННОВАЦИОННОЙ СФЕРЫСАНКТ-ПЕТЕРБУРГА

Рассохо-Анохина Валентина Николаевна, Резункова Ольга Петровна
Международная Академия информационных технологий
Большая Морская ул., 53/8, Санкт-Петербург, 190121, Россия
e-mail: ararog@mail.ru

Аннотация. Социально-психологическая адаптация военнослужащих, проходящих военную службу в ВС РФ и увольняемых в запас и включения их в систему совершенствования кадровой политики для высокотехнологичных предприятий Санкт-Петербурга, обеспечивающих разработку и производство инновационной конкурентной продукции и способствующих решению задач промышленного и социально-экономического развития Санкт-Петербурга на долговременную перспективу остается все еще не решенной.

Ключевые слова: социально-психологическая адаптация военнослужащих, непрерывное образование, профессиональная ориентация, карьера.

ESTABLISHING A CITY CENTER FOR PROFORIENTATION AND SOCIAL AND PSYCHOLOGICAL ADAPTATION OF MILITARY SERVICE SERVICES IN THE RF AF AND DISCHARGED IN STOCK FOR HIGH-TECHNOLOGY INNOVATIVE SPHERE SAINT PETERSBURG

Rassokho-Anokhina Valentina, Rezunkova Olga
International Academy of Information Technology
53/8 Bolshaya Morskaya St, St. Petersburg, 190005, Russia
e-mail: ararog@mail.ru

Abstract. Socio-psychological adaptation of servicemen doing military service in the RF Armed Forces and being transferred to the reserve and their inclusion in the system of improving personnel policy for high-tech enterprises of St. Petersburg in the long term remains unresolved.

Keywords: social and psychological adaptation of military personnel, continuing education, vocational guidance, career.

Уникальность сегодняшней ситуации заключается в том, что обеспечение качества дополнительного профессионального образования, профессиональная переподготовка, с одной стороны, и ускоренное развитие приоритетных и высокотехнологичных отраслей науки и производства, с другой стороны, возможны только при объединении усилий, интеллектуального потенциала и ресурсов университетов, академической и отраслевой науки, а также высокотехнологичных предприятий промышленности. В свою очередь, профессиональная подготовка, переподготовка увольняемых в запас с военной службы кадров и закрепление их на высокотехнологичных предприятиях и научных, научно-исследовательских учреждениях является решением одной из важнейших задач социальной защиты военнослужащих.

Для решения этой комплексной задачи необходимо создать инновационно-образовательный промышленно-экономический кластер. Такой кластер – это консорциум или ассоциативное объединение образовательных учреждений, предприятий промышленности, проектных и научных организаций, имеющих совпадающие долгосрочные цели совместной деятельности в области профессиональной подготовки и повышения квалификации кадров, разработки и внедрения новых технологий и видов инновационной конкурентоспособной продукции, создания совместной научно-образовательной инфраструктуры, поддерживающей кадровое обеспечения высокотехнологичного производства, полный инновационный цикл разработки и выпуска продукции [2, 4, 5].

В рамках кластерного подхода к управлению интеграционными процессами можно регулировать кадровую политику в части адаптации и профессиональной пригодности уволенных в запас из ВС РФ военнослужащих, а также – решить комплексно задачи в научной, образовательной и инновационной сферах. В частности, могут быть разработаны единая политика и программа подготовки и повышении квалификации кадров, включая подготовку

кадров высшей научной квалификации, единая политика и программа проведения НИОКР в интересах участников кластера, единое инфраструктурное обеспечение научной и образовательной деятельности [1, 3].

В рамках кластера проще решаются задачи унификации и разделения труда в интересах всех партнеров. Наяву обратная связь: в отношении кадрового обеспечения участников кластера это позволяет оперативно формировать гибкие по содержанию и структуре вариативные программы основного и дополнительного профессионального образования, построенные по модульному принципу и реализуемые в рамках сетевого взаимодействия учреждений профессионального образования и работодателей, что расширяет перечень профессий и специальностей при выборе их военнослужащими, увольняемыми в запас из ВС РФ.

Целевые задачи кадровой политики заключаются в создании системы кадровой политики, которая обеспечивает в перспективе социальную адаптацию военнослужащих в гражданской жизни:

Обучение и подготовку специалистов высшей квалификации с уровнем качества, обеспечивающего решение задач высокотехнологичных предприятий по разработке и производству инновационной конкурентной продукции с минимальной адаптацией на предприятии;

Непрерывную переподготовку и повышение квалификации специалистов предприятий под решение задач проектирования и производства перспективной инновационной конкурентной продукции;

Закрепление высококвалифицированных кадров на высокотехнологичных предприятиях.

Инструментом кадровой политики являются совокупность законодательных, нормативно-правовых, организационных и учебно-методических документов межгосударственные, федеральные целевые, региональные, межотраслевые и отраслевые программы, инвестиционные проекты и комплексы внепрограммных мероприятий, направленных на совершенствование и развитие системы кадровой политики.

Для этого необходимо решить следующие задачи:

1. Выявить феноменологию, структуру и динамику процесса социально-психологической адаптации офицеров, увольняемых в запас и ведущие факторы, определяющие их адаптационную успешность.

2. Создать на региональном уровне систему прогнозирования на среднесрочный и долгосрочный периоды развития рынка труда.

3. Выявить и применить на практике реальные возможности и совершенные, современные способы получения дополнительного профессионального образования в период прохождения гражданами РФ военной службы в ВС РФ [6].

4. Создать инновационную систему подготовки и переподготовки специалистов, включающую:

Систему обеспечения интегральной подготовки, учитывающей взаимоувязанность учебных планов дополнительного профессионального образования и интересы работодателей;

Индивидуальную схему подготовки и переподготовки специалистов на основе модульности учебного процесса и обеспечивающей требования работодателей;

Реализацию рациональной взаимоувязанной и взаимодополняющей сети научно-исследовательских, учебных и учебно-производственных центров для профессиональной переподготовки военнослужащих, увольняемых в запас.

Рациональную систему специализации и кооперации образовательных учреждений, реализующих дополнительное образование взрослых.

5. Экспериментально обосновать возможности применения оптимальной модели социально-психологической адаптации офицеров, предложения и рекомендации по ее успешному осуществлению.

Ожидаемые конечные результаты реализации концепции и показатели ее социально-экономической эффективности:

Решение задачи социальной адаптации военнослужащих, увольняемых в запас, не только на территории Санкт-Петербурга, но и России.

Решение задач подготовки, переподготовки и закрепления кадров на высокотехнологичных предприятиях, в частности – Санкт-Петербурга в необходимых объемах и номенклатуре и качестве.

Создание современной научно-исследовательской, учебной и учебно-производственной базы образовательных организаций Санкт-Петербурга, которая позволит обеспечить высокотехнологичные предприятия высокопрофессиональными кадрами техников, инженеров и специалистов высшей квалификации, адаптированных под условия разработки и производства перспективной наукоемкой, инновационной конкурентной продукции.

Сохранение новых рабочих мест в организациях высокотехнологичных отраслей промышленности Санкт-Петербурга.

Уменьшение оттока специалистов высокой квалификации из Санкт-Петербурга.

СПИСОК ЛИТЕРАТУРЫ

1. Лысенко В.Н., Резунков А.Г., Резункова О.П. Целевое профессиональное обучение специалистов для предприятий радиоэлектронного комплекса Санкт-Петербурга // Известия СПбГЭТУ «ЛЭТИ». СПб.: 2011. № 7. С. 125–130.
2. Дмитриев И.В. Социально-психологическая адаптация офицеров, уволенных в запас, к условиям гражданской среды: Автореф. дис.канд. психол. наук. М.: 1999. 25 с.
3. Резунков А.Г., Резункова О.П., Семикин В.В. и др Концепция непрерывной подготовки кадров «ПРОФКАРЬЕРА» для высокотехнологичной сферы Санкт-Петербурга: методическое пособие // СПб.: ГОУВПО «ЛЭТИ им. В.И. Ульянова (Ленина)». 2011. 18 с.
4. Чепляев В.Л. Социальная адаптация военнослужащих. html//scvr.sarnode.ru:8102/jornal/number5/chepl.htm
5. Шелест Б.Е. Социальная адаптация офицеров запаса Вооруженных Сил России: Автореф. дисс. кан. социол. наук. М.: 1997. 24 с.
6. Рассохо-Анохина В.Н. Социальная адаптация военнослужащих, увольняемых в запас Вооруженных Сил Российской Федерации» // Вестник Сибирского отделения Академии военных наук. Омск.: 2019. № 55. С.118-121.

УДК 004.89

РАЗВИТИЕ ПОРТАЛА «НАШ ПЕТЕРБУРГ»: ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УЛУЧШЕНИЯ ВЗАИМОДЕЙСТВИЯ С ГРАЖДАНАМИ

Рыбальченко Павел Анатольевич[1], Беген Петр Николаевич[2], Чугунов Андрей Владимирович[2]
[1] СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Черняховского ул., 59, Санкт-Петербург, 191040, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: pashaspb1@gmail.com, begen@itmo.ru, chugunov@itmo.ru

Аннотация. В докладе рассмотрено развитие портала в 2019–2020 гг., создание автоматизированного классификатора сообщений граждан в рамках оптимизации процедуры подачи сообщения и его дальнейшей проверки и отработки на портале. Разработанное решение позволило снизить процент отклоняемых сообщений по причине неверно выбранной категории почти в 3 раза, а также уменьшить время проверки сообщения модератором на соответствие тематики в среднем на 30%. Определены перспективы использования полученных в ходе исследования результатов в рамках концепции «Умный город» в проектах развития информационных систем электронного взаимодействия граждан с органами власти.

Ключевые слова: электронное управление, электронное участие, заявления граждан, Санкт-Петербург, искусственный интеллект, автоматизированный классификатор.

DEVELOPMENT OF "OUR ST. PETERSBURG" PORTAL IN 2019-2020: USING ARTIFICIAL INTELLIGENCE TOOLS FOR ELECTRONIC INTERACTION BETWEEN CITIZENS AND AUTHORITIES

Rybalchenko Pavel[1], Begen Petr[2], Chugunov Andrei[2]
[1] St. Petersburg Information and Analytical Center
59 Tcherniahovskogo St, St. Petersburg, 191040, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: pashaspb1@gmail.com, begen@itmo.ru, chugunov@itmo.ru

Abstract. The paper presents portal development for 2019-2020, a citizens' messages automated classifier creation in frames of optimizing the procedure for submitting a message to the portal and its further verification and check. The developed solution allowed reducing the percentage of rejected messages due to an incorrectly selected category by almost 3 times, as well as reducing time for moderator for checking the message for compliance with the topic by an average of 30%. Prospects of using results obtained in the course of study within the borders of the "Smart city" concept in projects for information systems for electronic interaction between citizens and authorities' development are determined.

Keywords: E-Governance, E-Participation, citizens' applications, St. Petersburg, Artificial Intelligence, automated classifier.

За шесть лет функционирования портал «Наш Санкт-Петербург» стал востребованным инструментом электронного участия, — благодаря публичности и открытости многие проблемы были оперативно доведены до администрации города и успешно решены в кратчайшие сроки.

В период 2019–2020 гг. в портал «Наш Санкт-Петербург» были внесены обновления и изменения, которые можно условно разделить на три группы:

– улучшение юзабилити портала и внедрение новых технологических решений, связанных с представлением информации на портале;

– совершенствование отдельных компонентов портала и создание новых функциональных возможностей для различных групп пользователей;

– изменены принципы и форма подачи сообщений, включая внедрение нейронных сетей для классификации направляемых на портал сообщений.

Третья группа модернизации касается изменения принципов и формы подачи сообщений, включая внедрение нейронных сетей для классификации направляемых на портал сообщений. Теперь гражданину не надо заранее знать и изучать классификатор категорий и пытаться найти ту категорию, которая подходит для конкретного сообщения. Достаточно коротко изложить суть проблемы в текстовом виде, и система самостоятельно определит соответствие категории классификатора или подберет до трех вариантов, из которых можно определить наиболее подходящую. Вместе с тем, у пользователя остается возможность не согласиться с предложенным вариантом и самостоятельно выбрать категорию из всего перечня классификатора.

В докладе более подробно рассматривается именно эти изменения, т.к. они показательны точки зрения опыта применения технологий искусственного интеллекта в государственных информационных системах.

В ходе проведенного анализа работ в данном процессе были обнаружены некоторые недостатки и проблемы, связанные с нетривиальной классификацией сообщений. Анализ статистики функционирования портала показал, что неудобство для пользователя и сложность самостоятельного выбора категории

проблемы (из 200 доступных на портале), приводит к отклонениям 20–25% сообщений по причине неправильного выбора категории. Это приводит и к высокой нагрузке на службы модерации, что, в свою очередь, имеет следствием увеличение сроков рассмотрения и отработки сообщений. Поэтому была поставлена задача разработать алгоритм и интеллектуальный классификатор с целью оптимизации вышеупомянутых процессов и повышения результативности корректной обработки поступающих на портал сообщений.

В исследовании [1] была рассмотрена задача автоматизации выбора тематики сообщений граждан, которая затрагивает третий пункт указанного порядка действий пользователя.

Для того, чтобы повысить эффективность деятельности службы модерации (т.е. сократить время на проверку и отработку поступающих на портал сообщений), а также минимизировать риск ошибочного определения категории проблемы пользователем и повысить удобство при подаче сообщения, был предложен следующий подход:

– пользователю при подаче сообщения о проблеме не нужно самостоятельно выбирать категорию проблемы из классификатора или вводить ключевые слова в поисковую форму: достаточно сразу написать текст сообщения, на основе которого автоматизированный классификатор предложит 3 наиболее вероятных варианта категории (последующий порядок действий, таких как указание местоположения существующей проблемы на карте и т. д., сохраняется);

– для службы модерации разработать модуль автоматической классификации текста сообщения (интеллектуального автоматизированного помощника), который представит результат работы в виде ранжированного списка из трех определенных категорий с соответствующим процентом точности классификации для последующего выбора модератором, а также подскажет, если по тексту сообщения невозможно определить категорию, т. е. данная проблема отсутствует в классификаторе.

Для эффективной работы разрабатываемого алгоритма автоматической классификации сообщений граждан, основанного на применении методов машинного обучения и обработки естественного языка, для обучения и тестирования разрабатываемых моделей была использована локальная копия базы данных портала за 2018 год, содержащая 1,5 млн проверенных сообщений граждан. Все текстовые данные были предварительно подготовлены, разделены на обучающую и тестовую выборку и переведены в числовой вид. [2-3]

В качестве нейронных сетей были предложены три сети с разной архитектурой и конфигурацией: сеть прямого распространения (FFNN), сверточная сеть (CNN) и рекуррентная сеть (RNN) с LSTM-блоком. Каждый представленный метод машинного обучения имеет свои достоинства и недостатки, поэтому было решено применить их в разработке и проанализировать итоговый результат в рамках исследовательской задачи. Реализация проводилась на языке программирования Python 3.x, с использованием различных открытых библиотек и фреймворков для машинного обучения, обработки и анализа данных.

В ходе разработки алгоритма автоматической классификации сообщений граждан и интеллектуального классификатора было проведено несколько запусков обучения и тестирования моделей, которые постоянно модифицировались путем изменения различных параметров обучения, структур самих моделей, добавлением новых обучающих данных.

На основе полученных метрик для измерения качества классификации было отмечено, что модели, основанные на нейронных сетях, показали процент точности определения больше 80%, а значит они удовлетворяли условию перечня критериев успешности функционирования, по которому можно снизить процент отклонения сообщения на портале. Наилучший результат точности классификации показал класс сверточных нейронных сетей (CNN) – почти 83%. Модель на основе CNN была использована при подсчете статистики и анализа 32 548 сообщений, которые поступали в двухнедельный период июня 2019 года, для оценки эффективности обучения и точности классификации.

За счет разработанного алгоритма автоматической классификации сообщений граждан, основанного на методах машинного обучения и обработки естественного языка, удалось снизить средний процент отклоняемых сообщений по причине неверно определенной категории проблем почти в 3 раза (с 23% до 8%), достигнув более 90% средней точности определения категории проблем. Также удалось снизить время проверки модератором текста сообщения на соответствие тематики примерно на 30%; упростить процедуру подачи сообщения на портал для гражданина.

СПИСОК ЛИТЕРАТУРЫ

1. Беген П.Н., Чугунов А.В. Разработка интеллектуального классификатора сообщений граждан на портале «Наш Санкт-Петербург»: опыт применения методов машинного обучения // Научный сервис в сети Интернет: труды XXI Всероссийской научной конференции (23–28 сентября 2019 г., г. Новороссийск). 2019. С. 131–140. DOI: 10.20948/abrau-2019-92
2. Jackson P., Moulinier I. Natural Language Processing for Online Applications: Text Retrieval, Extraction and Categorization. John Benjamins Publishing Co., 2007. 244 p.
3. Goldberg Y. A Primer on Neural Network Models for Natural Language Processing // Journal of Artificial Intelligence Research. 2016. Vol. 57 (1). P. 345–420. DOI: 10.5555/3176748.3176757

УДК 349.44:004.891.2

РАЗРАБОТКА КЛАССИФИКАТОРА СУЩНОСТЕЙ ГОРОДСКОЙ СРЕДЫ НА ОСНОВЕ ПРАВООТНОШЕНИЙ ДЛЯ ЗАДАЧ УПРАВЛЕНИЯ УМНЫМ ГОРОДОМ

Спирова Наталия Юрьевна, Кудинов Сергей Александрович
Университет ИТМО
Биржевая линия, В.О., 14, Санкт-Петербург, 199034, Россия
e-mails: nyspirova@itmo.ru, sergei.kudinov@itmo.ru

Аннотация. Исследование посвящено формированию принципов классификации объектов, субъектов и явлений в городской среде с учётом определения этих сущностей в нормативно-правовом пространстве. Предложена структура объединённого классификатора на примере анализа законодательства РФ и Санкт-Петербурга. Показано применение классификации в задачах городского планирования и управления умным городом для характеристики существующих и перспективных объектов, выявления противоречий действующего законодательства.

Ключевые слова: умный город; сущности городской среды; классификация; правовое регулирование.

DEVELOPMENT OF A CLASSIFIER OF URBAN ENVIRONMENT ENTITIES BASED ON LEGAL RELATIONSHIPS FOR SMART CITY MANAGEMENT

Spirova Nataliya, Kudinov Sergei
ITMO University
14 Birzhevaya line, Vasilievsky Island, St. Petersburg, 199034, Russia
e-mails: nyspirova@itmo.ru, sergei.kudinov@itmo.ru

Abstract. The research is devoted to the formation of principles of classification of objects, subjects and phenomena in the urban environment, taking into account the definition of these entities in the legal space. The structure of the combined classifier is based on the analysis of the legislation of the Russian Federation and Saint Petersburg. The article shows the use of classification in urban planning and smart city management to characterize existing and prospective objects and identify contradictions in current legislation.

Keywords: smart city; urban environment entities; classification; legal relations.

Задачи классификации в сфере городского планирования и градостроительства приобрели особую актуальность вместе с процессами широкой информатизации систем городского управления, в том числе, в контексте развития концепции «Умный город». Одним из инструментов, применяемых при создании «Умных городов», является цифровая модель городской среды [1], которая неизбежно должна опираться на некоторую спецификацию сущностей.

Существует разработки, касающиеся классификаций в смежных областях, которые велись и в России, и за рубежом. Так, Е. В. Франгуловой в 2011 году была описана муниципальная система управления земельно-имущественным комплексом, предназначенная для автоматизации деятельности муниципалитетов в задачах учёта имущества и земельных участков и интеграции с ГИС [2]. В США разработана и активно используется стандартная классификация землепользования (Land Based Classification Standards, LBCS) [3]. Она применяется с целью стандартизации описания земельных участков, а также как основа для разработки информационных систем. В базовом случае каждый земельный участок в ней можно описать определённым набором параметров, в ходе чего обеспечивается пятимерное описание земельного участка. Такой метод описания, благодаря своей гибкости, позволяет адаптировать систему классификации к различным ГИС-системам и системам поддержки принятия решений. В Европе было предпринято несколько попыток создания общих правовых онтологий [4]. В общем случае они предназначены для перевода существующих правовых баз в машиночитаемый формат и стандартизации описания правовых данных и обмена правовой информацией. В числе разработок для платформ проектов «Умных городов» стоит отметить онтологическую классификацию KM4City, которая описывает городские сущности для базы городских данных цифровой модели города [5].

Все решения в перечисленных системах строятся на ситуативном подходе, абстрагировано от законодательства. Даже если речь идёт о системах правосудия, рассматривается некоторая ситуация, её контекст, ищутся причины и следствия, и решение принимается исключительно на основании фактических значений параметров среды, без учёта нормативно-правовых аспектов. Выстраивание системы классификации городских сущностей на основании законодательства поможет избежать такой проблемы, при этом принимая во внимание законодательное разнообразие различных регионов РФ. Более того, классификаторы, построенные на основе правоотношений смогут посодействовать улучшению нормативно-правовой системы благодаря отслеживанию правовых связей и, соответственно, лёгкому обнаружению конфликтов и правовых коллизий.

Предложенная методика построения структуры реестра сущностей городской среды (СГС) разрабатывалась с учётом универсальности с точки зрения территориального применения и юрисдикции. Первый шаг – составление первичного перечня СГС. Предлагается составлять его на основе базовой терминологии (предметного указателя) произвольного регионального справочника либо учебника по градостроительству и управлению городом. Термины должны рассматриваться в контексте местной

юрисдикции и существенности в задачах управления развитием города. Для каждого термина из подготовленного таким образом перечня устанавливается нормативно-правовой акт (НПА), в котором содержится его юридическое определение или определение синонима. Далее формируется реестр таких НПА.

Второй шаг заключается в уточнении и дополнении первичного перечня на основании определений, содержащихся в НПА, из реестра, составленного на первом шаге. На основании анализа тех же НПА составляется перечень правоотношений, в которых задействованы СГС. Основной задачей этапа является создание типологии СГС, при этом сущности, которые участвуют в одних и тех же правоотношениях в одной роли, должны быть отнесены к одному типу. Типология может быть представлена как ориентированный граф, вершинами которого являются структурные группы СГС, а рёбрами – правоотношения между ними. На данном этапе возможно дополнительное проведение экспертных интервью, в ходе которых может быть расширен перечень СГС и НПА, а также выявлены правовые противоречия.

Третий шаг заключается в построении классификаций СГС внутри каждого из выделенных типов. При этом виды сущностей, которые не могут быть преобразованы друг в друга законным образом, должны быть отнесены к разным структурным группам. Дробление элементов классификации должно быть обосновано наличием специфических правоотношений, применяемых к группе сущностей внутри элемента классификации.

Последний этап заключается в оптимизации полученной классификационной системы на основании принципа экономии – поиска критериев, которые позволяют максимально сократить количество выделяемых групп, не снижая точности описания каждого вида СГС и его признаков.

Методика построения классификатора СГС была апробирована на примере законодательства РФ и Санкт-Петербурга. На первом этапе были использованы учебники по градостроительству и градорегулированию [6, 7] и классификатор элементов благоустройства Санкт-Петербурга [8]. Методом поиска правовых определений для ОГС было выделено 78 НПА, в том числе: 10 кодексов РФ, 19 федеральных законов, 5 постановлений Правительства РФ, 10 НПА министерств. В результате анализа была построена система описания СГС, которая включает 6 высших структурных групп: «Пространства», «Имущество», «Роли», «Контейнеры», «Акторы» и «Операции». Все классификаторы, кроме классификатора «Контейнеры», имеют внутреннюю иерархическую структуру. Например, классификатор «Имущество» включает все СГС, которые можно отнести к движимому или недвижимому имуществу согласно Гражданскому кодексу. СГС типа «Имущество» может иметь различные «Роли» (комбинации ролей), находиться во владении различных «Акторов» и располагаться в различных «Пространствах». В классификатор «Пространства» входят СГС, которые могут быть охарактеризованы границами и правовыми режимами, действующими исключительно в пределах этих границ.

В результате была составлена онтологическая классификационная система в виде текстового документа, состоящего из классифицированных в соответствии с определёнными правилами сущностей, к каждой из которых приложено максимально возможное подробное определение из законодательства, описание её роли в городской среде и в некоторых случаях описание её связей с другими сущностями. Классификатор был протестирован на предмет устойчивости: в ходе его разработки в ряд НПА были внесены существенные изменения, которые были легко интегрированы в классификатор путём уточнения структур нескольких подклассов. Также, оценка классификатора была проведена экспертным методом со стороны нескольких подразделений органов государственной власти Санкт-Петербурга, в ходе которых были определены сильные и слабые стороны предложенной системы классификации. Так, в дальнейшем работа должна быть сконцентрирована на разработке механизмов исключения коллизий законодательства по субъективным причинам, обеспечения полного единства терминологии с учётом сложившихся принципов и порядков деятельности отдельных органов государственной власти.

Дальнейшая работа может быть нацелена на реализацию разработанного классификатора в рамках существующих или перспективных государственных информационных систем, использующихся в задачах управления городским хозяйством для повышения эффективности принятия решений. Перспективным с точки зрения технологий форматом реализации такого классификатора является онтологическая структура базы знаний.

СПИСОК ЛИТЕРАТУРЫ

1. Vakali A., Anthopoulos L.G. The Future Internet // Urban Planning and Smart Cities: Interrelations and Reciprocities. Berlin, 2012.
2. Франгулова Е.В. Разработка муниципальной интегрированной системы управления земельно-имущественным комплексом // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2011. № 2. С. 166-171.
3. American Planning Association (APA) // Land Based Classification Standards (LBCS). 2020. https://www.planning.org/lbcs/ (дата обращения: 2.05.2020).
4. Getman A., Karasiuk V., Hetman Y. Ontologies as a Set to Describe Legal Information // Proceedings of the 4th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2020). 2020. № 1. P. 347-357.
5. Nesi P., Soderi M., Bellini P. Km4City – The Knowledge Model 4 the City (ENG version). 2020. http://www.disit.org/drupal/?q=en-US&axoid=urn%3Aaxmedis%3A00000%3Aobj%3Aed964c20-d166-48fc-92f6-3b317f347e5e# (дата обращения 14.02.2020).
6. Бандорин Л.Е., Гудзь Т.В., Сафарова М.Д., Холопик К.В. Градорегулирвоание: Основы регулирования градостроительной деятельности в условиях становления рынка недвижимости. М.: Фонд «Институт экономики города», 2008.
7. Шепелев Н.П., Шумилов М.С. Реконструкция городской застройки. М.: Издательство «Высшая школа», 2000.
8. Комитет по градостроительству и архитектуре Санкт-Петербурга. Общегородской классификатор объектов внешнего благоустройства Санкт-Петербурга. СПб, 2009.

УДК 004.056

НОРМАТИВНО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАБОТ ПО ФОРМИРОВАНИЮ СИСТЕМЫ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Сторожик Виктор Сергеевич[1], Сторожик Илья Викторович[2]
[1] Центр экспертиз и оценок безопасности «СИНЕРЭФ-центр»
Смолячкова ул., 12/2, лит. А, пом. 11Н, офис 403, Санкт-Петербург, 194044, Россия
[2] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mails: svs@sinrf.ru, istorozhik@yandex.ru

Аннотация. Рассматриваются нормативные правовые акты, национальные стандарты и методические документы, определяющие порядок обеспечения работ по формированию системы безопасности значимого объекта критической информационной инфраструктуры.

Ключевые слова: автоматизированная система управления, безопасность критической информационной инфраструктуры, защита информации, значимый объект критической информационной инфраструктуры, информационная технология, компьютерная атака, компьютерный инцидент, критическая информационная инфраструктура, объект критической информационной инфраструктуры, система безопасности значимого объекта, субъекты критической информационной инфраструктуры.

LEGAL AND METHODOLOGICAL SUPPORT OF WORK CREATING A SECURITY SYSTEM FOR A SIGNIFICANT OBJECT CRITICAL INFORMATION INFRASTRUCTURE

Storozhik Viktor[1], Storozhik Ilya[2]
[1] Center for security expertise and assessments «CINEREF-center»
12/2 Smolyachkova St, lit. A, room 11N, office 403, Saint Petersburg, 194044, Russia
[2] Russian State Hydrometeorological University
79 Voronezhskya St., St. Petersburg, 192007, Russia
e-mails: svs@sinrf.ru, istorozhik@yandex.ru

Abstract. Regulatory legal acts, national standards and methodological documents that determine the procedure for ensuring the formation of a security system for a significant object of critical information infrastructure are considered.

Keywords: automated control system, security of critical information infrastructure, information protection, significant object of critical information infrastructure, information technology, computer attack, computer incident, critical information infrastructure, object of critical information infrastructure, security system of significant object, subjects of critical information infrastructure.

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, к основным национальным интересам в информационной сфере отнесено обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры (далее – КИИ) и единой сети электросвязи Российской Федерации в условиях проведения компьютерных атак.

В Федеральном законе от 26 июня 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определены нормы направленные на решение задач повышения уровня защищенности информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а так же российских юридических лиц и (или) индивидуальных предпринимателей, которые обеспечивают взаимодействие указанных систем или сетей.

Указом Президента Российской Федерации от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085» ФСТЭК России определена как федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Территориальные органы ФСТЭК России во взаимодействии с субъектами КИИ, которым принадлежат значимые объекты КИИ, обеспечивают проведение ими работ по созданию систем безопасности в соответствии с Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК России от 21 декабря 2017 г. № 235. Основные усилия в этой работе сосредотачиваются на назначении в субъектах КИИ ответственных за безопасность значимых объектов КИИ из числа руководителей субъектов КИИ, на создании подразделений по обеспечению безопасности таких объектов и их укомплектовании или назначении штатных специалистов по обеспечению безопасности таких объектов, а также на разработке организационно-распорядительных документов по безопасности объектов.

Рассматриваются нормативные правовые акты, национальные стандарты и методические документы, определяющие порядок обеспечения работ по формированию системы безопасности значимого объекта критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Указ Президента Российской Федерации от 25 ноября 2017 г. № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085».
4. Указ Президента Российской Федерации от 2 марта 2018 г. № 98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203».
5. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
6. Постановление Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».
7. Постановление Правительства Российской Федерации от 8 июня 2019г. № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры Российской Федерации».
8. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
9. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (зарегистрирован в Минюсте России 22 февраля 2018 г. № 50118).
10. Приказ ФСТЭК России от 27 марта 2019 г. № 64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235».
11. Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (в ред. приказа ФСТЭК России от 21 марта 2019 г. № 59).
12. Приказ ФСТЭК России от 21 марта 2019 г. № 59 «О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236».
13. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60).
14. Приказ ФСТЭК России от 26 марта 2019 г. № 60 «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239».
15. Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 8 февраля 2018 г. № 49966).
16. Приказ ФСТЭК России от 9 августа 2018 г. № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239» (зарегистрирован в Минюсте России 05 сентября 2018 г. № 52071).
17. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
18. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
19. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
20. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.
21. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.
22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 15 февраля 2008 г.
23. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14 февраля 2008 г.
24. Меры защиты информации в государственных информационных системах, утвержденные ФСТЭК России 11 февраля 2014 г.
25. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
26. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.
27. ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
28. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
29. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
30. ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем.

УДК 004.9:159.923

ФОРМИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К СЕРВИСУ АВТОМАТИЧЕСКОЙ ПЕРЕДАЧИ СВЕДЕНИЙ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Тимофеева Ангелина Олеговна
Университет ИТМО
Биржевая линия, В.О., 14, Санкт-Петербург, 199034, Россия
e-mail: linatim@yandex.ru

Аннотация. В ходе исследования рассмотрены подходы к разработке и управлению функциональными требованиями, а также исследованы государственные информационные системы (далее – ГИС) «Реестр ГИС Санкт-Петербурга» и «Открытые данные Санкт-Петербурга», выявлены нормативные требования по размещению общедоступной информации государственными органами власти о своей деятельности, а также рассмотрены требования к электронному сервису «Системы межведомственного электронного взаимодействия».

Ключевые слова: государственная информационная система; открытые данные; управление требованиями; функциональные требования.

FORMATION OF FUNCTIONAL REQUIREMENTS FOR THE AUTOMATIC TRANSMISSION OF INFORMATION SERVICE IN STATE INFORMATION SYSTEMS

Timofeeva Angelina
ITMO University
14 Birzhevaya line, Vasilievsky Island, St. Petersburg, 199034, Russia
e-mail: linatim@yandex.ru

Abstract. In the course of the study, approaches to the development and management of functional requirements were considered, and a general description of the State IS " STATE IS Register of St. Petersburg" and the State IS "Open Data of St. Petersburg" was compiled, regulatory requirements for the placement of publicly available information by state authorities about their activities were identified, and also requirements for the electronic service "Systems of interdepartmental electronic interaction".

Keywords: state information system; open data; requirements management; functional requirements.

Существуют различные подходы и методики управления требованиями к разработке государственных информационных систем. Разница между сложившейся практикой управления разработкой ГИС обусловлена возрастающей сложностью проектов и бурным развитием информационных технологий [1].

Открытые данные являются информацией, которая создается исполнительными органами государственной власти и публикуется в виде машиночитаемых форматов. Целью публикации открытых данных является облегчение к ним доступа заинтересованных лиц, которые могут работать с ними, и далее реализовать ценные исследования, аналитику и т. д. Опубликованные данные являются основой для большого числа социально-значимых и общественно-полезных проектов. Следовательно, актуальность таких данных очень важна. В настоящее время в ГИС «Открытые данные Санкт-Петербурга» содержатся открытые данные из ГИС «Реестр ГИС Санкт-Петербурга», однако эти данные обновляются в ручном режиме. Периодичность обновления данных из «Реестр ГИС Санкт-Петербурга» в ГИС «Открытые данные Санкт-Петербурга» ежеквартальная. Как показывает практика, такой период обновления данных из Реестра ГИС является не оптимальным, поскольку эти же данные в Реестре ГИС обновляются по мере изменения на постоянной основе. Неактуальность данных о ГИС Санкт-Петербурга может привести к ошибочным результатам деятельности пользователей, вплоть до подрыва доверия граждан к деятельности органов власти. В связи с этим возникает потребность передачи данных в автоматическом режиме, для чего необходимо создание специального электронного сервиса. При проектировании сервиса необходимо учитывать рекомендации по разработке сервисов в «Системе межведомственного электронного взаимодействия».

Целью данной работы является выявление и систематизация функциональных требований к сервису автоматической передачи сведений из ГИС «Реестр ГИС Санкт-Петербурга» в ГИС «Открытые данные Санкт-Петербурга». Для достижения цели были решены следующие задачи:

1. Рассмотрены подходы и методики к управлению требованиями для проектирования электронных сервисов: методики управления функциональными требованиями [2-4] методические рекомендации по разработке сервисов в «Системе межведомственного электронного взаимодействия»;
2. Исследованы ГИС «Реестр ГИС Санкт-Петербурга» и ГИС «Открытые данные Санкт-Петербурга»;
3. Выявлены нормативные требования к размещению общедоступной информации о деятельности исполнительных органов власти;
4. Сформированы функциональные требования к электронному сервису «Системы межведомственного электронного взаимодействия».

На первом этапе работы был осуществлен сравнительный анализ методик и подходов к управлению требованиями к разработке, а также рассмотрены методические рекомендации по разработке сервисов в «Системе межведомственного электронного взаимодействия». На втором этапе были описаны цели, назначение, функциональная структура и действующие веб-сервисы рассматриваемых государственных информационных

систем. На следующем этапе исследования был определён и описан состав передаваемых данных для проектируемого сервиса, составлена информационная модель данных. После рассмотрения и систематизации нормативных требований по предоставлению общедоступной информации о деятельности органов власти, сформированы функциональные требования к проектируемому сервису.

Исходя из проведенного исследования, можно сделать вывод, что для наиболее успешной (с наименьшими затратами человеческих и временных ресурсов) реализации проекта официально используется ГОСТ 34.602-89, но компания разработки начинает комбинировать и внедрять методы и подходы Agile. В ходе работы были определены заинтересованные стороны, а также, сформулировано техническое задание на создание сервиса. После изучения Реестра ГИС, получен состав данных для нового проектируемого сервиса. Далее, в ходе изучения ГИС «Открытые данные Санкт-Петербурга» определены входные реквизиты сервиса. Сделан вывод, что данные, передаваемые из Реестра ГИС необходимо представить в форме, в которой их может принимать ГИС «Открытые данные Санкт-Петербурга», т. е. в форме плоской таблицы, на основе чего составлена модель данных.

Дальнейшая исследовательская работа может быть связана с моделированием процесса в сфере городской информатизации для актуализации сведений о деятельности исполнительных органов государственной власти для дальнейшего применения этого процесса в регионах Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Вигерс К., Битти Д. Разработка требований к программному обеспечению. М.: Русская редакция, 2014. 736 с.
2. Gorelits N.K., Kildishev D.S., Khoroshilov A.V. Requirements management for safety-critical systems. Overview of solutions // Proc. Inst. Syst. Program. RAS. 2019. Vol. 31, № 1. С. 25–48.
3. Андреевский И.Л., Аминов Х.И. Бизнес-аналитика: Учебное пособие. СПб: Изд-во СПбГЭУ, 2019. 73 с.
4. Agile: практическое руководство / Пер.с анлийского. – М.: Олимп–Бизнес, 2018.

ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ИНФОРМАТИЗАЦИИ

УДК 004.02

ОРГАНИЗАЦИЯ УНИВЕРСАЛЬНОГО ПРОТОКОЛА СВЯЗИ УСТРОЙСТВ ЦОС ДЛЯ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ УСТРОЙСТВ РАДИОЛОКАЦИОННОЙ СТАНЦИИ

Афанасьев Дмитрий Сергеевич, Виноградов Алексей Борисович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: Dmitr-afanas@yandex.ru, vvcehanovsky@mail.ru

Аннотация. Рассмотрен универсальный протокол связи устройств цифровой обработки сигналов комплекса радиолокационных станций. В рамках протокола сформулированы требования к порядку взаимодействия устройств между собой и с объектами внешней среды, организация информационных потоков и каналов передачи. Применение универсального протокола связи позволило предложить механизм выявления ошибок синхронизации в реальном масштабе времени и причины расхождения результатов между приемными каналами отдельно взятых устройств.

Ключевые слова: телекоммуникационные системы; радиолокационная станция; цифровая обработка сигналов; протокол связи.

THE UNIVERSAL PROTOCOL OF THE WORK FOR INFORMATION WORK THE RADAR STATION

Afanasiyev Dmitriy, Vinogradov Aleksey
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: Dmitr-afanas@yandex.ru, vvcehanovsky@mail.ru

Abstract. The universal protocol of communication of digital signal processing devices of the radar stations complex is considered. The protocol sets out requirements for the order of interaction between devices and with objects of the environment, the organization of information flows and transmission channels. The application of a universal communication protocol has provided a mechanism for detecting real-time synchronization errors and the cause of the discrepancy between the receiving channels of individual devices.

Keywords: telecommunication systems; radar; digital signal processing; communication Protocol.

Декларативный язык программирования Пролог рассматривается в качестве коммуникативного программно-технического средства организации интерфейсов. В наследии академика А.Н. Колмогорова [1], следуя интерпретации его терминологии, в развитие положений классической логики, может являться логика задач интерпретации интуиционистской логики по процедурам последовательных замен переменных. «логикой. Язык Пролог восходит к развитию положений классической логики с интерпретацией терминологии интуиционистской логики [2, с. 90]. Современное IT-понятие «интуитивно понятный интерфейс» может иметь интерпретацию понятия «интуитивно понятный язык программирования» Пролог, как язык, опирающийся на «совокупность «интуитивно убедительных» умственных построений», а именно на интуиционистскую логику.

Декларативный язык программирования Пролог предоставляет гибкую оперативную модификацию предметных задач, удобен для решения задач с выраженными объектами информатизации и их коммуникационными связями, логика программы языка программирования Пролог выражается в терминах отношений, представленных в виде фактов и правил. Пролог как язык программирования реализует аппарат математической логики, логического программирования, методологии проектирования и анализа экспертных систем, систем принятия решений, баз знаний - из фундаментальных методов исследований объектов информационных технологий, и модернизации современных достижений с преобразованиями в направлении интеллектуальных агентов, императивного программирования, интеллектуальных процедур обработки информации. В профессиональных информационных системах язык Пролог формально применим в силу принадлежности к стандартам ISO, ISO/IEC JTC1/SC22/WG17. и реализации для операционных систем семейства и мобильных платформ Unix, Windows, Java, NETOC с дополнительными расширениями и диалекты [3], [4]. Ряд понятий языка Пролог предлагается заменить и наполнить новым смысловым содержанием. Предикаты Пролога переименовываются в Задачи и переменные хорновских дизъюнктов, которым в Прологе соответствуют предикаты. Термы этих предикатов будут пониматься как исходные данные и требуемые результаты решения этих задач, унификация предикатов - как доказательство принадлежности соответствующей задачи искомому

решению. Процесс выполнения программ на Прологе можно представить как процесс поиска последовательности решений элементарных подзадач путем соответствующих подстановок, в отличии от выполняемого процесса получения пустого дизъюнкта по правилу резолюции.

СПИСОК ЛИТЕРАТУРЫ:

1. Габидулин Э.М, Пилипчук Н.И. Лекции по теории информации. Изд-во МФТИ, 2007. - 214 с.
2. Майстренко К.А., Будилов А.В., Афанасьев Д.С., Мустафин Н.Г. Влияние параметров реализации подсистемы синхронизации на характеристики распределённой системы цифровой обработки сигналов // XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Материалы конференции. СПб, 24-26 октября 2018 г. - С. 43-44.

УДК 004

МОДЕЛИРОВАНИЕ СТЕГОСИСТЕМЫ С РАССРЕДОТОЧЕНИЕМ ВО ВРЕМЕНИ ДЛЯ КАНАЛОВ С ШУМОМ

Бочаров Михаил Вячеславович, Ковцур Максим Михайлович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: bocharovm1998@gmail.com, maxkovzur@mail.ru

Аннотация. В докладе описываются различные математические модели каналов с шумом и их возможное применение в стеганографии, а также с помощью компьютерного моделирования рассматривается возможность применения на практике стегосистемы с рассредоточением вложения во времени для каналов связи с шумом.

Ключевые слова: стеганография, стегосистемы на основе каналов с шумом, модели каналов связи, цифровые аудио сигналы, компьютерное моделирование.

SIMULATION OF A TIME-DISTRIBUTED STEGOSYSTEM BASED ON NOISY CHANNELS

Bocharov Mikhail, Kovzur Maksim
Bonch-Bruevich Saint-Petersburg state university of communication
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: bocharovm1998@gmail.com, maxkovzur@mail.ru

Abstract. The report describes various mathematical models of channels with noise and their possible use in steganography are described, and using computer simulation, we consider the possibility of applying in practice a spread-time stegosystem based on noisy channels.

Keywords: steganography, stegosystems based on noisy channels, models of communication channels, digital audio signals, computer simulation.

В настоящее время особый интерес представляют стегосистемы, покрывающие объекты в которых подвергаются влиянию помех различного происхождения после прохождения по каналу связи. На практике цифровые объекты в большинстве случаев подвергаются изменениям при передаче или хранении в общедоступных информационных системах. Такие изменения могут быть вызваны в результате работы алгоритмов обработки самих информационных систем либо помехами в каналах связи. Использование многих стеганографических алгоритмов после таких изменений покрывающих объектов не представляется возможным из-за следующих причин: низкой степени секретности стегосистемы, искажения вложений. Для решения этих проблем были разработаны стегосистемы, учитывающие влияние помех на передаваемый стегосигнал.

В докладе рассмотрены стегосистемы на основе каналов с шумом [1], т.к. они позволяют обеспечить более высокий уровень секретности по сравнению с другими существующими стегосистемами такого типа. Информационный сигнал в стегосистемах на основе каналов с шумом передается по естественному каналу с шумом, в результате, перед атакующим стоит задача статистически отличить сигнал без вложения и с вложением после прохождения по каналу связи, при этом в стегосистемах на основе каналов с шумом статистика погружаемой информации неотделима от статистики шума канала связи [2]. Стегосистемы на основе каналов с шумом могут быть использованы только при выполнении следующих условий существует естественный канал с шумом и нелегитимный пользователь получает стегосигнал только после прохождения по каналу с шумом.

Для обеспечения безопасной передачи секретной информации уровень вкладываемого сигнала должен быть очень низким, что на практике для передачи цифровых сигналов оказывается трудно реализуемым. Данная проблема решается модификацией стегосистем на основе гауссовского шума – стегосистемы с рассредоточением вложения во времени [3]. Принцип построения стегосистемы с рассредоточением во времени заключается в том, что вложение секретного сообщения производится с определенной вероятностью, а каждый информационный бит передается при помощи N_0 последовательных отсчетов.

Главным преимуществом рассмотренной стегосистемы является то, что покрывающий объект может быть известен атакующему, что является неприемлемым для всех других стегосистем. В данном докладе рассмотрены результаты, полученные при помощи компьютерного моделирования стегосистемы с рассредоточением во времени, доказана практическая реализуемость данной стегосистемы, выделены основные достоинства и недостатки.

СПИСОК ЛИТЕРАТУРЫ

1. Korzhik V., Morales-Luna G., Loban K. Stegosystems based on noisy channels // International journal of computer science and applications. – 2011. – Т. 8. – № 1. – С. 1-13.
2. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография. [монография] : – СПбГУТ. – СПб., 2016 – 226 с
3. Коржик В.И., Лобан К.А. Стегосистема с рассредоточением во времени для каналов с гауссовским шумом // Труды учебных заведений связи. ГОУВПО СПбГУТ, № 181. –2009. – С. 23-32.
4. Korzhik V., Morales-Luna G., Nebaeva K., Alekseevs M. A stegosystem with blind decoder based on a noisy channel // 18th International Conference, Digital Signal Processing, 2013. – P. 1–5.
5. Коржик В.И., Небаева К.А., Алексеевс М. Использование модели канала с шумом для построения стегосистемы // Телекоммуникации. – 2013. – № S7. – С. 33-36.

УДК 681.518.3:681.3.06

ПРОГРАММНЫЕ ИНТЕРФЕЙСЫ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ ДЛЯ РАБОТЫ С ИЗОЛИРОВАННЫМИ ПРОСТРАНСТВАМИ

Егоров Сергей Сергеевич, Широков Владимир Владимирович, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: ssegorov@mail.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. Рассматривается вариант формирования программных интерфейсов информационно-управляющих систем для работы с изолированными пространствами. Из набора программных интерфейсов операционной системы создают процессы с использованием трех программных интерфейсов. В базовые механизмы доступа к данным включены «posix»-возможности процессов, пространства имен процессов и списки контроля доступа. Пространства имен процессов позволяют создать изолированную среду выполнения в изолированном пространстве очередей сообщений, сетевых адресов, доменных имен, точек монтирования, идентификаторов пользователей.

Ключевые слова: программный интерфейс операционной системы; списки контроля доступа; «posix»-возможности процессов; пространства имен процессов.

THE PROGRAMALS OF THE WORLD SYSTEM FOR WORK WITH THE EXPLORES ARE

Egorov Sergey, Shirokov Vladimir, Schigoleva Marina
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: ssegorov@mail.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Abstract. Is considered the option of forming software interfaces of information-control systems to work with isolated spaces. From a set of software interfaces, the operating system creates processes using three software interfaces. Basic data access mechanisms include "posix" process capabilities, process name spaces, and access control lists. Process name spaces allow you to create an isolated execution environment in an isolated space of message queues, network addresses, domain names, mounting points, user identifiers.

Keywords: application programming interface of operating system; access control lists; "posix"-capabilities of the processes; process namespaces.

Развитый программный интерфейс операционных систем [1] позволяет создать приложения для управления списками контроля доступа с возможностью применения удобного пользовательского интерфейса информационно-управляющих систем. В операционной системе выделяется набор программных интерфейсов для запуска процессов в изолированном пространстве очередей сообщений, сетевых адресов, доменных имен, точек монтирования, идентификаторов пользователей. Процессы создаются с использованием трех программных интерфейсов из набора программных интерфейсов операционной системы: (1) Программный интерфейс, при котором сам процесс формирует для своего выполнения изолированное пространство имен; (2) Программный интерфейс, при котором процесс-родитель формирует изолированное пространство имен процесса-потомка; (3) Программный интерфейс, при котором процесс может подсоединиться к некоторому изолированному пространству имен другого процесса.

Изолированность пространства должна быть подтверждаема и проверяема на эффективность изоляции, для чего предусмотрено формирование набора действий, который убедит в изолированности процессов друг от друга по соответствующему виду ресурса. Так при выполнении процессов:

– в изолированных пространствах очередей сообщений - две очереди, созданные в этих процессах с одним и тем же именем, не должны быть видны;

– в изолированных пространствах сетевых адресов - процессы могут открыть сокеты с одним и тем же номером порта;

– в изолированных пространствах сетевых имен - процессы могут присвоить своему хосту разные сетевые имена.

Формирование изолированных пространств направлено на поддержание безопасности компьютерного и информационного ресурса системы и недопущения информационного ущерба разделам данных информационно-управляющей системы. Проверка списков контроля доступа осуществляется развитым программным интерфейсом [2], внешними командами для чтения и установки списков контроля доступа, приложениями для управления списками контроля доступа с возможностью применения удобного сервиса пользовательского интерфейса.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс]. URL: http://manpages.org/namespaces/7 (дата обращения: 10.08.2020)
2. [Электронный ресурс]. URL: http://manpages.org/acl/5 (дата обращения: 10.08.2020)

УДК 51-76

СЛАБОФОРМАЛИЗОВАННАЯ СРЕДА И АЛГОРИТМЫ ЕЕ ОБРАБОТКИ

Копыльцов Антон Александрович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: kopyl2001@mail.ru

Аннотация. Рассматриваются методы и средства обработки слабоформализованной среды, используемые для построения инструментальных средств поддержки искусственного интеллекта при проведении научных исследований.

Ключевые слова: моделирование; алгоритм; слабоформализованная среда; искусственный интеллект; научное исследование.

WEAKLY FORMALIZED ENVIRONMENT AND ALGORITHMS FOR ITS PROCESSING

Kopyltsov Anton
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: kopyl2001@mail.ru

Abstract. Methods and means of processing a weakly formalized environment used to build tools to support artificial intelligence in conducting scientific research are considered.

Keywords: modeling; algorithm; weakly formalized environment; artificial intelligence; scientific research.

При проведении научных исследований как экспериментальных, так и теоретических часто имеют дело с информацией, измеренной с некоторой погрешностью, иногда противоречивой, каждому экспериментальному факту сопоставляется несколько противоречивых теоретических объяснений [1, 2]. Таким образом, при исследовании явлений и процессов окружающей среды получаем информацию не полную, иногда противоречивую или просто неверную. Для обработки такой информации, поступающей из внешней среды, предлагается алгоритм, в основу которого положена идея обработки информации в живом организме [3-5].

Первоначально любой живой организм собирает информацию. Затем распознает собранную информацию, т.е. в первую очередь оценивает, представляет ли она угрозу или нет. Если угрозы нет, то осуществляется оценка, может ли она представлять какой-либо интерес для организма, например, питание и др. Таким образом, осуществляется классификация поступающей информации. После этого осуществляется оценивание степени достоверности информации и степени безопасности информации. Если степени достоверности и безопасности информации достаточно велики, то осуществляется установление связей новой поступившей информации с информацией, которая поступала прежде, и которая хранится в памяти. Если это сравнение приведет к тому, что эта информация представляет опасность то, срабатывает рефлекс избегания опасности (убежать от опасности, спрятаться от опасности и др.). Если же это сравнение приведет к тому, что эта информация не представляет опасности, а является пищей, например, то срабатывает рефлекс нападения. Если же информация не представляет никакого интереса для живого организма, то внимание переключается на другие объекты и процессы. После установления связей вновь поступившей информации с информацией, которая хранится в памяти, осуществляется ее запоминание и отнесение к какому-либо классу, например, опасность, пища и др. Таким образом, осуществляется поддержка принятия решений, т.е. организм либо убегает, либо нападает, либо не обращает внимания на эту информацию. Возможно, что было принято неправильное решение, т.е. организм решил, что это пища, а оказалось опасность, например. В этом случае это тоже запоминается. В процессе многократного сталкивания организма с внешней средой вырабатываются признаки поведения организма в окружающей среде, т.е. вырабатывается устойчивая реакция на внешние раздражители, что приводит к тому, что организм обучается избегать опасности и находить питание, например.

Этот алгоритм по аналогии может быть использован при проведении научных исследований. Также есть внешняя среда, которую исследуют экспериментальными и теоретическими методами. Проводятся эксперименты, которые подтверждают или опровергают выдвинутую гипотезу. Полученная в ходе

экспериментов или наблюдений информация собирается, классифицируется и хранится. На основе собранной информацию принимаются решения о проведении новых экспериментов, выдвигаются новые гипотезы и теории. На основе многолетних исследований вырабатывается устойчивая реакция, т.е. стереотип проведения исследований, соответствующий данному уровню развития цивилизации. В случае успеха развиваются научные школы и направления, возникают новые парадигмы.

СПИСОК ЛИТЕРАТУРЫ

1. Юсупов Р.М., Заболотский В.П. Научно-методологические основы информатизации. – СПб.: Наука, 2000, 456 с.
2. Адамар Ж. Исследование психологии процесса изобретения в области математики. – М.: Советское радио, 1970, 152 с.
3. Ухтомский А.А. Доминанта. –Л.: Наука, 1966, 276 с.
4. Копыльцов, А.А. Модель классификации информации и алгоритм ее предварительной обработки для статических и динамических объектов // Известия СПбГЭТУ “ЛЭТИ” (известия государственного электротехнического университета), серия “Информатика, управление и компьютерные технологии”. 2013. № 6. С. 134-139.
5. Копыльцов, А.А. Применение обобщенного алгоритма обработки слабоформализованной информации для управления неравновесной химической реакцией // Инженерный вестник Дона. 2015. № 1. ч.2. [Электронный ресурс]. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2812 (дата обращения: 20.09.2016).

УДК 004.413

УНАСЛЕДОВАТЕЛЬНОСТЬ И ПРОАКТИВНОСТЬ КАК ФАКТОР РАЗВИТИЯ В ЖИЗНЕНОМ ЦИКЛЕ СЕРВИС-ОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Мустафин Николай Габдрахманович[1], Савосин Сергей Валентинович[1], Соколов Борис Владимирович[2]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: nikolay.mustafin@gmail.com, svsavosin@etu.ru, sokolov_boris@mail.ru

Аннотация. Рассмотрены вопросы унаследовательности и проактивности в жизненом цикле сервис-ориентированных информационных систем с учетом накопленных знаний и данных об объекте информатизации, процессах принятия решений, опыте использования предыдущих версий систем и представлений о возможной эволюции внутренних и внешних условий и требований, предъявляемых к системе.

Ключевые слова: унаследованность; проактивность; информационная система; жизненный цикл; функциональность; сервис-ориентированная архитектура; взаимодействие функциональных элементов. внешние факторы; внутренние факторы; требования.

INHERITANCE AND PROACTIVITY AS A FACTOR OF DEVELOPMENT IN THE LIFE CYCLE OF SERVICE-ORIENTED INFORMATION SYSTEMS

Mustafin Nikolay[1], Savosin Sergey[2], Sokolov Boris[3]
[1,2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
[3] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: nikolay.mustafin@gmail.com, svsavosin@etu.ru, sokolov_boris@mail.ru

Abstract. Issues of inheritance and proactivity in the life cycle of service-oriented information systems are considered, taking into account the accumulated knowledge and data on the object of informatization, decision-making processes, the experience of using previous versions of systems and ideas about the possible evolution of internal and external conditions and requirements for the system.

Keywords: inheritance; proactivity; information system; life cycle; functionality; service-oriented architecture; the interaction of functional elements; external factors; internal factors; requirements.

Рациональное развитие информационной системы на различных этапах жизненного цикла в значительной степени определяется факторами унаследовательности и проактивности. Фактор унаследовательности предполагает перенос и сохранение достигнутой функциональности, диалоговых и инструментальных решений. Фактор проактивности требует предвидения будущих новых требований и изменений внутренних и внешних условий в жизненном цикле информационной системы.

Процесс непрерывного развития корпоративных информационных систем (КИС) обуславливается, с одной стороны, постоянным развитием требований пользователей, а с другой стороны, развитием информационных технологий, включая аппаратно-программные средства, сетевые структуры, диалоговые средства, модели, методы и инструменты систем поддержки принятия решений.

Эволюция КИС становится все более стремительной. Одним из самых значимых инициирующих фактором такой эволюции является необходимость обеспечения возможности быстрой перестройки бизнес-процессов организации и соответственно оперативной поддержки этих процессов функциональными возможностями КИС.

Стоит заметить, что даже небольшие изменения в бизнес-процессах могут потребовать модификации множества компонентов КИС, часть из которых использовались длительное время и планируются к использованию в дальнейшем. ИС-системы, которые по тем или иным причинам перестали удовлетворять изменившимся потребностям применений, но продолжают использоваться ввиду больших затруднений, возникающих при попытке их замены, принято называть унаследованными системами (УС).

Новые технологические решения (сервис-ориентированная архитектура (СОА), облачные сервисы) привели к тому, что монолитные приложения унаследованных систем, сменяются распределенными решениями, основанными на сервисной архитектуре, обеспечивающей возможность быстрой перестройки бизнес-процессов.

Чтобы в современных условиях компании сохранить конкурентоспособность, нужно продолжать эволюцию КИС, однако затраты на подобные перестройки необходимо уменьшить.

В рамках процесса перехода к новой архитектуре можно выделить некоторое число унаследованных систем, которые, с одной стороны, обслуживают важнейшие бизнес-процессы, а с другой быстрая замена их аналогичным современным решением часто проблематична, так как:

- отсутствуют готовые сервисы во внедряемой платформе,
- сложность реализации унаследованных бизнес-процессов приводит к неприемлемым краткосрочным временным и стоимостным затратам.

В связи с этим часто возникает необходимость адаптации унаследованных систем к требованиям, диктуемым новыми технологиями.

Есть несколько направлений преобразования унаследованных систем в рамках сервис-ориентированной архитектуры:

- заменить УС на современную, с требуемой функциональностью,
- разработать новую систему с учетом новых требований и ограничений архитектуры,
- «завернуть» УС в интерфейс промежуточного программного обеспечения.

Существуют различные альтернативы превращения разрозненной ИТ-среды в сервисную, в которой отдается предпочтение слабым связям, абстрагированию низкоуровневой логики, гибкости, а также возможности многократного использования инструментов и различных бизнес решений.

Первая альтернатива — заменить традиционную систему на новую. Эта операция возможна, если есть готовое современное коммерческое решение, соответствующее старой системе по функциональности и другим характеристикам. Такое решение проще внедрять, но с выходом новых модификаций затраты возрастут.

Вторая альтернатива — «обернуть» имеющуюся систему связующим программным обеспечением, которое позволит соединить ее с веб-сервисами. В этом случае старая функциональность будет «одета» в сервисный слой и подключена к среде СОА. Некоторые задачи при этом могут остаться нерешенными: если старое приложение реализует сразу несколько возможных сервисов, ожидаемого избавления от зависимостей можно не получить. Но все же данный вариант приемлем, когда нет ресурсов для «переписывания» имеющейся системы, либо нет необходимости от нее отказываться и требуется сократить затраты на адаптацию.

Третья альтернатива — «переписать» имеющуюся систему.

Этот вариант может оказаться лучшим, тогда можно переработать архитектуру приложений и достичь нужной степени размежевания. Но старые приложения, как правило, выполняют на предприятиях критически важные функции, и иногда их сложно или дорого переписывать. В таких случаях обязательна тщательная оценка всех рисков.

При планировании интеграции приложений в рамках проекта СОА, переходный этап могут облегчить доступные готовые продукты, однако разные решения различаются по возможностям и уровням сложности, так что окончательное решение будет зависеть от выбора альтернативы.

Исследования, выполненные по данной тематике, проводились при частичной финансовой поддержке грантов РФФИ (№№17-29-07073-офи-м, 18-07-01272, 18-08-01505, 19–08–00989, 20-08-01046), в рамках бюджетной темы №№0073–2019–0004.

СПИСОК ЛИТЕРАТУРЫ

1. Nicolas Serrano, Josune Hernantes, Gorka Gallardo, Service-Oriented, Architecture and Legacy Systems. IEEE Software, September/October 2014, IEEE Computer Society.
2. Мустафин Н.Г., Савосин С.В., Подсытник Д.А Унаследованная система в качестве стартовой площадки // Программные продукты и системы. 2004. №3. С.12–16.
3. А.В. Иконникова, И.А. Петрова, С.А. Потрясаев, Б.В. Соколов. Динамическая модель комплексного планирования модернизации и функционирования информационной системы // Изв.вузов. Приборостроение. 2008. Т. 51, №11. С. 62–69.
4. Б.В. Соколов, С.А. Потрясаев, А.В. Иконникова, Д.А. Иванов. Модель и алгоритм оперативного перераспределения функций управления между узлами катастрофоустойчивой информационной системы // Международная Научная Школа «Моделирование и Анализ Безопасности и Риска в Сложных Системах (МАБР-2007)», РФ, г.Санкт-Петербург, 4–8 сентября, 2007: Труды школы. С. 440–445.
5. Мустафин Н.Г., Савосин С.В., Соколов Б.В. Унаследовательность как фактор развития информационных систем // Перспективные направления развития отечественных информационных технологий: материалы круглых столов: тезисы докладов / Севастопольский государственный университет; науч. ред. Б.В. Соколов. Севастополь: «РИБЕСТ», 2017. С. 18–21.

УДК 004.62

РАСПРЕДЕЛЕННАЯ СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ КАК ПРОТОТИП ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ

Новопашин Владимир Сергеевич, Нечитайленко Роман Александрович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: Novopashin.vladimir@gmail.com, rnet2005@gmail.com

Аннотация. Распределенная система обработки информации представлена как информационно-аналитическая система для обработки и анализа данных. Проверка разрабатываемых аналитических средств поддержки информационного обеспечения распределенной системы осуществляется на основе прототипов распределенной системы и средств поддержки распределенной системы, создаваемых и/или выбираемых в ходе аналитического исследования. Прототип распределенной системы соответствует набору базовых понятий, установленным требованиям к распределенной системе, набору контрольных параметров, принимаемым для оценки особенностей распределенной системы.

Ключевые слова: распределенная система обработки информации; информационное обеспечение; сервисные приложения.

THE DISTRIBUTION SYSTEM OF THE INFORMATION HOW TO BE A FINAL INFORMATION-ANALYSIS

Novopashin Vladimir, Nechitailenko Roman
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: Novopashin.vladimir@gmail.com , rnet2005@gmail.com

Abstract. Distributed information processing system is presented as an information and analytical system for data processing and analysis. The analysis of the distributed system information support support is tested on the basis of distributed system prototypes and distributed system support tools. created and/or selected in the analytical study. The distributed system prototype corresponds to a set of basic concepts set by the distributed system requirements, and a set of control parameters adopted to evaluate the features of the distributed system.

Keywords: distributed information processing system; information support; service applications.

Распределенная система обработки информации представлена как информационно-аналитическая система для поиска, обработки и анализа данных, сопровожденная сервисным обслуживанием, интерфейсным обслуживанием, утвержденной коммуникативной формой. Проверка разрабатываемых аналитических средств поддержки информационного обеспечения распределенной системы обработки информации [1] осуществляется на основе прототипов распределенной системы и прототипов средств поддержки распределенной системы, создаваемых и/или выбираемых в ходе аналитического исследования.

Прототип распределенной системы содержит и соответствует набору базовых понятий [2], установленным требованиям к распределенной системе, набору контрольных параметров, принимаемым для оценки особенностей распределенной системы. В качестве обязательных основных требований установлены: прозрачность системы (включая местоположение, доступ, параллелизм доступа, репликации), открытость системы, надежность.

Прототип распределенной системы и средств её поддержки позволяет представить распределенную систему для восприятия пользователями как однородный объект, а не как набор автономных объектов, которые специфично взаимодействуют между собой.

Прозрачность местоположения заключается в отсутствии необходимости знать, где расположены необходимые пользователю ресурсы - файлы могут перемещаться на различные узлы распределенной системы. При сбое на узле распределенной системы УРС1 данные могут быть восстановлены на другом узле УРС2, пользователь-потребитель ресурса будет видеть лишь единое файловое пространство, при том, что пользователь-администратор будет иметь картину распределения ресурса физически на разных серверах с перемещением между узлами УРС1 и УРС2.

Прозрачность доступа заключается в наличии схем сокрытия различий доступа при предоставлении данных категориям пользователей. Прозрачность параллелизма доступа состоит в сокрытии факта совместного использования ресурсов, когда различным пользователям распределенной системы обеспечена возможность параллельного доступа к общим данным, но факт совместного использования ресурсов скрыт как по составу информационного ресурса, так и по факту одновременной работы с ним.

Прозрачность репликации, особенно на распределенных файловых системах - с целью обеспечения сохранности данных и соблюдения комплексной защиты информационного ресурса системы, необходимым образом обеспечивается репликация данных, при которой пользователю не должно быть известно, что репликация данных существует и для сокрытия фактора репликация данных, у предоставляемых данных или ресурсов, объявлены одинаковые имена.

Формы сервисного и интерфейсного обслуживания предлагаются исходя из состава пакета проблем проектирования и управления распределенной системой, но с обязательной адаптацией сервисных и интерфейсных приложений для всех объектов конфигурирования архитектуры распределенной системы, форм администрирования системы, восстановления информационного ресурса системы и переносимости её программного обеспечения.

Прототип распределенной системы и средств её поддержки поддерживает обработку данных с использованием встроенных сервисных приложений распределенной системы [3] для рассылки данных на распределенные узлы системы; сбора данных из распределенных узлов; агрегирования данных в общее пространство данных распределенной системы - как основных функциональных составляющих распределенной системы по обработке и передаче данных, восстановления данных в случае возникновения ошибок.

В качестве надежности системы основным показателем, определяющим надежность всей распределенной системы обработки информации, для выбранного прототипа, является отказоустойчивость. Принципом Отказоустойчивости устанавливается возможность продолжения действий, заданных программой функционирования, после возникновения неисправностей.

Рассмотренная концепция принятых прототипов средств поддержки информационного обеспечения распределенной системы обработки информации позволила:

Согласовать локальные параметрические и алгоритмические требования к обработке данных в узлах распределенной системы с требованиями, влияющими на общие свойства задач распределенной системы;

Провести анализ свойств данных централизованной обработки распределенной системой (рассылка данных на распределенные узлы системы, сбор данных из распределенных узлов, агрегирование данных в общее пространство данных распределенной системы);

Установить категории классификации распределенных систем: по количеству элементов в системе, по уровню организации распределенных систем, по типу предоставляемых ресурсов, для последующего качественного сравнения вариантов балансировки информационной нагрузки с применением сервисных приложений распределенной системы обработки информации.

СПИСОК ЛИТЕРАТУРЫ

1. Карабутов Н.Н. Идентификация систем. Структурный и информационный анализ. Часть 1. - М.: Изд-во Альтаир - МГАВТ, 2005. - 79 с.
2. Tanenbaum A., Van Steen M. Distributed systems. Pearson Prentice Hall, 2007. - 803 p.
3. Шокин Ю.И. и др. Распределенная информационно-аналитическая система для поиска, обработки и анализа пространственных данных // Вычислительные технологии. 2007. Т. 12. №. 3. С. 108-115.

УДК 623.611

ОПТИМИЗАЦИЯ АЛГОРИТМОВ МНОЖЕСТВЕННОГО ДОСТУПА В САМООРГАНИЗУЮЩЕЙСЯ СЕТИ РАДИОСВЯЗИ ДЕКАМЕТРОВОГО ДИАПАЗОНА

Панин Роман Сергеевич[1], Путилин Алексей Николаевич[2]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
[2] ПАО «Интелтех»
Кантемировская ул., 8, Санкт-Петербург, 197342, Россия
e-mails: paninrs@yandex.ru, a.n.putilin@yandex.ru

Аннотация. Рассматривается задача оптимизации алгоритма множественного доступа в самоорганизующейся декаметровой радиосети. Основным отличием от традиционных задач является необходимость учёта в этом случае ее анизотропности. Предложен подход к решению задачи параметрического синтеза системы множественного доступа в самоорганизующихся сетях связи.

Ключевые слова: самоорганизующиеся сети связи; множественный доступ; декаметровый диапазон; система передачи данных, пакетная сеть радиосвязи.

OPTIMIZATION OF MULTIPLE ACCESS ALGORITHMS IN A DECAMETER SELF-ORGANIZING RADIO NETWORK

Panin Roman[1], Putilin Alexey[2]
[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
[2] PAO “IntelTech”
8 Kantemirovskaya St, St. Petersburg, 197342, Russia
e-mails: paninrs@yandex.ru, a.n.putilin@yandex.ru

Abstract. The problem of optimizing the multiple access algorithm in a self-organizing decameter radio network is considered. The main difference from traditional problems is the need to take into account its anisotropy in this case. An approach to solving the problem of parametric synthesis of a multiple access system in self-organizing communication networks is proposed.

Keywords: self-organizing communication networks; multiple access; decameter range; data transmission system, packet radio network.

Введение. В настоящее время растет интерес к беспроводным децентрализованным самоорганизующимся сетям связи (ССС или MANET – Mobile Ad hoc Network). Использование на принципах множественного доступа группы выделенных радиоканалов обеспечивает ССС устойчивость к изменениям инфраструктуры сети, устойчивость к изменению помеховой обстановки, простоту и высокую скорость развертывания. Эти преимущества указывают на несомненный интерес данной технологии для систем управления критическими структурами. В настоящее время предложены ряд стандартов для реализации ССС в гигагерцовых диапазонах. Однако ареал покрытия таких сетей не превышает сотен метров. Использование для критических структур требует перехода в диапазоны, обеспечивающие обмен данными на тысячи километров. Этому требованию отвечают диапазоны, находящиеся ниже 30 МГц. Среди них наибольшей информационной ёмкостью обладает декаметровый диапазон.

Однако в отличие от гигагерцовых диапазонов в данном диапазоне наиболее ярко проявляется анизотропия выделяемых для организации сети радиоканалов как по их частоте, так и по направлению передачи. Пригодный для передачи данных в одном направлении радиоканал может оказаться совершенно непригодным для другого направления. Острота данной проблемы снижается при использовании всеми станциями сети сигналов последовательным расширением спектра, то есть систем радиосвязи с псевдослучайным переключением рабочих частот. Вероятность наличия для любого направления связи пригодного радиоканала растет с увеличением числа используемых радиоканалов. С другой стороны, увеличение этого числа выше потребностей ССС, определяемых входной нагрузкой, приводит к нерациональному использованию частотного ресурса, к простою радиоканалов.

Реализация ССС в декаметровом диапазоне невозможна без выбора оптимального числа коллективно используемых ССС радиоканалов, их подбора на основе априорного знания их пригодности по направлениям связи, а также определения оптимальных параметров алгоритма доступа к ним. Данная работа предлагает подход к формулировке данной задачи оптимизации и определению принципов построения математической модели рассматриваемой системы радиосвязи.

Структура сети определяется следующими параметрами. В сети имеется S абонентов (радиостанций). В соответствии со схемой организации связи (СхОС) в сети Dd - направлений передачи данных. Все каналы имеют одинаковую скорость передачи R. Передаваемые пакеты имеют длину Lp. Скорость передачи в пакетах Sp=R/Lp. Пакет передается в одном временном слоте, поэтому время в сети дискретно по слотам передачи. Время слота Ts=1/Sp. Коэффициент связности сети

C=2*Dd/(S(S-1)), $0 \le C \le 1$, где S(S-1)/2 – максимальное количество каналов в сети, когда каждый связан с каждым. Таким образом, множеством параметров описывающих структуру сети определяется как α=(S,Dd,Sp,Lp).

Среда передачи описывается следующими параметрами. В ССС разрешено использование Fc радиоканалов, находящихся в разных участках декаметрового диапазона [1]. Ионосферно-волновой и частотно-диспетчерской службой (ИВ ЧДС) до начала функционирования ССС, априорно определена матрица вероятностей установления соединения в направлении передачи данных d в радиоканале f – P(d,f), где $d \in \{1,Dd\}$, $f \in \{1,Fc\}$. Из множества FB выбранных частот вследствие воздействия преднамеренных или системных помех может оказаться непригодными для всех информационных направления до Fj радиоканалов [2]. Таким образом, среда передачи описывается множеством параметров δ=(Fc,P,Fj).

Следует определить четыре возможных типа матриц P(d,f).

Тип 1: радиосеть изотропна по направлениям и радиоканалам. P(d,f)=P* для всех d и f. Ситуация типична для работы радиосети с антеннами зенитного излучения (NVIS – Near Vertical Incidence Skywave propagation) на дальность до 300 км на частотах 2...8 МГц или для работы радиосети при отсутствии прогноза по оценке качества радиоканалов: отсутствие службы ИВ ЧДС или отсутствие возможности достоверного прогноза вследствие чрезвычайных условий.

Тип 2: радиосеть изотропна по направлениям и анизотропна по частотам. P(d,f)=P(f) для всех d. Ситуация типична для работы сети из двух групп абонентов, имеющих локальные области расположения в которых они связаны между собой альтернативными каналами: провод, оптоволокно, УКВ и проч. Типичный примеры: взаимодействие двух АСУ, разделенных в пространстве.

Тип 3: радиосеть изотропна по частотам и анизотропна по направлениям. P(d,f)=P(d) для всех f. Это разновидность радиосети типа 1 при наличии сосредоточенных по направлениям помех искусственного или естественного происхождения.

Тип 4: сеть анизотропна по направлениям и частотам. Общий случай. Степень анизотропии существенно влияет на эффективность функционирования сети. Гипотетически возможны варианты фрагментации сети на несколько независимых подсетей или направлений радиосвязи: для различных групп направлений связи все рабочие частоты различны.

Поступающая в сеть нагрузка определяется следующими параметрами. Среднее число пакетов, поступающих в сеть в единицу времени (слот) $0 \le Ap \le Dd$, нормированное число пакетов $0 \le \lambda \le 1$, где λ=Ap/Dd. Поток пакетов стохастический без памяти, направление передачи данных в которое поступает пакет выбирается случайно. Закон распределения времени между возникновением пакетов – геометрический. Требуемое время доставки пакета в сети – Td. Требуемая вероятность доставки пакета в сети – Pr. Множеством параметров, описывающих нагрузку в сети определяется как β=(Ap,Am,Td,Pr).

Используется алгоритм множественного доступа с контролем занятости (МДКЗ, см. [3]). Он определяется следующими параметрами. Количество используемых радиоканалов Fb. Из множества возможных радиоканалов FS выбирается подмножество FB. Вероятность использования свободного канала при возникновении заявки на установление соединения Pu. Таким образом, множество параметров алгоритма множественного доступа есть γ=(Fb,FB,Pu). Эти параметры являются предметом оптимизации.

Для оценки эффективности функционирования ССС представляется достаточным использование следующих показателей качества.

1. Вероятность своевременной доставки пакета в направлении за требуемое время

$$Pd(\alpha,\beta,\gamma,\delta)=Pf(\beta)*Pc(\alpha,\beta,\gamma,\delta), \text{ где}$$

Pf(β) - вероятность наличия свободного канала при возникновении заявки за требуемое время,

Pc(α,β,γ,δ) - вероятность установления соединения в направлении.

2. Производительность сети Pn(α,β,γ,δ).

В соответствии с методом выбора доминирующего показателя качества наиболее обоснованным представляется выбор производительности сети в качестве показателя эффективности функционирования системы множественного доступа ССС при ограничении на вероятность своевременной доставки пакета:

$$\mathrm{Pn}(\mathrm{Dd},\mathrm{FS},\mathrm{FB}) = \frac{1}{Dd}\max_{0\le\lambda\le 1}\sum_{d=1}^{Dd}\frac{1}{\mathrm{V}(\alpha,\delta)\mathrm{Tm}(\alpha,\beta,\gamma,\delta)}, \text{ где}$$

Tm(α,β,γ,δ) – среднее время доставки пакета в направлении d на стартовых каналах FB,

V(α,δ) – скорость передачи в направлении d на выбранных частотах.

Задача оптимизации параметров системы множественного доступа ССС (задача синтеза) состоит в определении:

$\gamma^* = \arg\max_{\gamma\in Y} \mathrm{Pn}(\alpha,\beta,\gamma,\delta)$ при условии, что Pd(α,β,γ,δ)≥ Pd для всех d.

Заключение. Предложенный подход позволяет построить формализованную модель, направленную на решение задачи параметрического синтеза системы множественного доступа в ССС. Он разделяет группы параметров, описывающих структуру сети, среду передачи, поступающую нагрузку и, собственно, алгоритм множественного доступа. Это позволяет при необходимости выполнить независимую корректировку исходных данных по любой из названных четырех составных частей. Представлена формулировка задач анализа и синтеза рассматриваемой системы связи, которая является методической основой для построения математической модели функционирования и разработки методики оптимизации параметров системы множественного доступа в ССС.

СПИСОК ЛИТЕРАТУРЫ

1. Recommendation ITU-R F.1487 Testing of HF modems with bandwidths of up to about 12 kHz using ionosfpheric cannel simulators, 2000: [Электронный ресурс]. URL: https://www.itu.int
2. Путилин А.Н. Модель взаимодействия линии радиосвязи и станции радиоэлектронного подавления // Доклад на конф. «Региональная информатика 2012», 24-26 октября 2012 г. – СПб.: СПОИСУ, 2012.
3. Бунин С.Г., Войтер А.П. Вычислительные сети с пакетной радиосвязью - Киев: Тэхника, 1989.- 129 с.

УДК 004.891

ПРИМЕНЕНИЕ СЕРВИС-ОРИЕНТИРОВАННОГО ПОДХОДА ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РЕШЕНИЯ ПРИРОДООХРАННЫХ И ГИДРОМЕТЕОРОЛОГИЧЕСКИХ ЗАДАЧ

Соболевский Владислав Алексеевич

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mail: arguzd@yandex.ru

Аннотация. Рассматриваются модели и методы сервис-ориентированной архитектуры при проектировании распределённых программных комплексов на базе искусственного интеллекта в приложении к решению прикладных задач гидрометеорологического прогнозирования и охраны природы.

Ключевые слова: искусственный интеллект; искусственные нейронные сети; сервис-ориентированная архитектура; экология.

APPLICATION OF A SERVICE-ORIENTED APPROACH IN THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS FOR SOLVING ENVIRONMENTAL AND HYDROMETEOROLOGICAL PROBLEMS

Sobolevskii Vladislav

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science

39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

e-mail: arguzd@yandex.ru

Abstract. Models and methods of service-oriented architecture in the design of distributed software systems based on artificial intelligence as applied to the solution of applied problems of hydrometeorological forecasting and environmental protection are considered.

Keywords: artificial intelligence; artificial neural networks; service-oriented architecture; ecology.

Современные методы мониторинга природных объектов и процессов, для решения различных классов задач, всё активнее автоматизируются. Для Российской Федерации данная задача является особо актуальной, из-за размеров страны и протяжённости многих природных объектов. Мониторинг силами специалистов на местах всё ещё имеет место быть, но всё активнее в работу вводятся автоматические станции, подключённые к глобальной сети Интернет, способные в режиме реального времени пересылать данные в любой конец страны.

А поскольку для пересылки данных используются публичные сети, наиболее продуктивными подходоми проектирования систем мониторинга и прогнозирования, использующих данные от автоматических станций, являются сервис-ориентированная архитектура (СОА) или же интернет вещей (ИВ) [2]. Оба подхода имеют схожие требования к отдельным сервисам, которые включены в подобные программные комплексы. И эти требования распространяются не только на поставщиков данных, но и на сервисы обработки и анализа данных, которые так же должны разрабатываться с учётом работы с публичными сетями.

С другой стороны, для решения задач моделирования и прогнозирования, в приложении к природным объектам, всё чаще начинают применяться модели и методы искусственного интеллекта, в частности искусственных нейронных сетей (ИНС). Данный класс моделей характеризуется способностью работать со сложно формализованными объектами, поведение которых нелинейно зависит от сотен входных параметров. И природные объекты являются наиболее яркими примерами таких случаев, что и обуславливает эффективность ИНС в решении ряда задач.

Но с распространением подобных моделей встаёт вопрос и требований к кадрам, способным проектировать такие системы. ИНС имеют весьма специфическую архитектуру и программные библиотеки, реализующие данные модели, требовательны к уровню знаний специалистов, работающих с ними. Встаёт вопрос не только автоматизации станций мониторинга, поставляющих данные с мест, но и автоматизации проектирования сервисов, способных обрабатывать поступающие данные.

В данном докладе предлагается использование программного комплекса, автоматизирующего процесс создания подобных сервисов. В настоящее время уже существует ряд разработок, решающих задачи автоматизации процесса создания программных комплексов на базе ИНС [3]. Их наличие демонстрирует актуальность данной задачи, а результаты показывают перспективность подобного подхода. Программный комплекс, описываемый в данном докладе, делает акцент на автоматизацию процесса генерации программных оболочек и на интеграцию разработанных ИНС различных архитектур в крупные программные комплексы. В разрабатываемом программном комплексе генерируется автономный сервис, содержащий заданную пользователем ИНС, обученную для решения конкретной задачи. При этом, пользователь не обязан быть специалистом в проектировании и обучении ИНС, поскольку в программном комплексе уже реализованы заготовки, которые дообучаются на представленных пользователем данных, для решения конкретных задач. Процесс дообучения, в свою очередь, максимально автоматизирован и требует от пользователя лишь навыков в формализации входных данных. Созданный программным комплексом сервис состоит из самой ИНС, а также программных оболочек, реализующих интерфейс REST и SOAP. Данный сервис кроссплатформенный и без предварительной установки и настройки дополнительного программного обеспечения может быть запущен на ряде операционных. А реализация нескольких программных оболочек позволяет обращаться к ИНС как к сервису, через наиболее распространённые веб-интерфейсы.

Описываемый программный комплекс уже был апробирован при решении задачи прогнозирования уровня воды во время весеннего ледохода для реки Северная Двина, в рамках создания программного комплекса «ПРОСТОР» [4]. Данный программный комплекс предназначен для прогнозирования и мониторинга уровня воды в реках, с целью своевременного предупреждения городских служб о возможности экстренных ситуаций, связанных с возможностью затопления. Апробация была проведена успешно и созданный сервис на базе ИНС был успешно внедрён в систему «ПРОСТОР».

Таким образом, модели и методы СОА при проектировании распределённых систем на базе ИНС, реализованные в описанном программном комплексе, подтверждают свою актуальность и реализуемость в современных условиях для решения задач как гидрометеорологии, так и охраны природных объектов в Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. Lantrip J., Griffin M., Aly A. Results of near-term forecasting of surface water supplies. In: World Water Congress 2005: Impacts of Global Climate Change - Proceedings of the 2005 World Water and Environmental Resources Congress. Anchorage, Alaska, US. 2005. Pp. 436. Doi: 10.1061/40792(173)447.
2. Bell M. Introduction to Service-Oriented Modeling, in Service-Oriented Modeling: Service Analysis. – Design and Architecture, Wiley & Sons, 2008, pp. 390, ISBN 978-0-470-14111-3.
3. Geng Z. Automated design of a convolutional neural network with multi-scale filters for cost-efficient seismic data classification / Z. Geng, Y. Wang // Nature Communications. – 2020. – Volume 11, Issue 1.
4. Zelentsov V.A., Alabyan A.M., Krylenko I.N., Pimanov I.Yu., Ponomarenko M.R., Potryasaev S.A., Semenov A.E., Sobolevskii V.A., Sokolov B.V., Yusupov R.M. A Model-Oriented System for Operational Forecasting of River Floods. Herald of the Russian Academy of Sciences. 2019. Volume 89, Issue 4. P. 405-417. DOI: 10.1134/S1019331619040130.

УДК 681.518.3:681.3.06

ЗАДАЧИ ОРГАНИЗАЦИИ ИНТЕРФЕЙСОВ НА БАЗЕ ДЕКЛАРАТИВНОГО ЛОГОЧЕСКОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ ПРОЛОГ

Соничев Александр Викторович, Егоров Сергей Сергеевич, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: avson@mail.ru, ssegorov@mail.ru, vvcehanovsky@mail.ru

Аннотация. В качестве коммуникативного программно-технического средства организации интерфейсов рассматривается декларативный язык программирования Пролог. Язык Пролог используется для решения задач с выраженными объектами информатизации с их коммуникационными связями, понятным языком программирования, допускает замену и наполнение новым смысловым содержанием традиционных понятий языка.

Ключевые слова: операционная система; Язык Пролог; Хорновские дизъюнкты; предикаты.

THE PROBLEM OF THE INTERFACES ON THE BASIS OF THE DECLARATIVE LOGO HISTORY PROLOG

Sonichev Aleksandr, Egorov Sergey, Schigoleva Marina
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: avson@mail.ru, ssegorov@mail.ru, vvcehanovsky@mail.ru

Abstract. As a communicative software tool for interface organization is considered declarative programming language Prologue. Prologue language is used to solve problems with expressed objects of informatization with their communication connections, understandable programming language, allows for the replacement and filling with new meaning content of traditional concepts of language.

Keywords: operating system; Language Prolog; a Horn clause; predicates.

Декларативный язык программирования Пролог рассматривается в качестве коммуникативного программно-технического средства организации интерфейсов. В наследии академика А.Н. Колмогорова [1], следуя интерпретации его терминологии, в развитие положений классической логики, может являться логика задач интерпретации интуиционистской логики по процедурам последовательных замен переменных. «логикой. Язык Пролог восходит к развитию положений классической логики с интерпретацией терминологии интуиционистской логики [2, с. 90]. Современное IT-понятие «интуитивно понятный интерфейс» может иметь интерпретацию понятия «интуитивно понятный язык программирования» Пролог, как язык, опирающийся на «совокупность «интуитивно убедительных» умственных построений», а именно на интуиционистскую логику.

Декларативный язык программирования Пролог предоставляет гибкую оперативную модификацию предметных задач, удобен для решения задач с выраженными объектами информатизации и их коммуникационными связями, логика программы языка программирования Пролог выражается в терминах отношений, представленных в виде фактов и правил. Пролог как язык программирования реализует аппарат математической логики, логического программирования, методологии проектирования и анализа экспертных систем, систем принятия решений, баз знаний - из фундаментальных методов исследований объектов информационных технологий, и модернизации современных достижений с преобразованиями в направлении интеллектуальных агентов, императивного программирования, интеллектуальных процедур обработки информации. В профессиональных информационных системах язык Пролог формально применим в силу принадлежности к стандартам ISO, ISO/IEC JTC1/SC22/WG17. и реализации для операционных систем семейства и мобильных платформ Unix, Windows, Java, NETOC с дополнительными расширениями и диалекты [3], [4]. Ряд понятий языка Пролог предлагается заменить и наполнить новым смысловым содержанием. Предикаты Пролога переименовываются в Задачи и переменные хорновских дизъюнктов, которым в Прологе соответствуют предикаты. Термы этих предикатов будут пониматься как исходные данные и требуемые результаты решения этих задач, унификация предикатов - как доказательство принадлежности соответствующей задачи искомому решению. Процесс выполнения программ на Прологе [3-4] можно представить как процесс поиска последовательности решений элементарных подзадач путем соответствующих подстановок, в отличии от выполняемого процесса получения пустого дизъюнкта по правилу резолюции.

СПИСОК ЛИТЕРАТУРЫ:

1. Kolmogoroff A. Zur Deutung der intuitionistischen Logik. — «Math. Zeitschrift», v.35, 1932 (Русский перевод: К толкованию интуиционистской логики. – В книге: Колмогоров А. Н. Избранные труды. Математика и механика. М., 1985). С. 142-148.
2. Братко И. Программирование на языке Пролог для искусственного интеллекта: Пер. с англ. – М.: Мир, 1990. 560 с.
3. А. Адаменко, А.Кучуков. Логическое программирование и Visual Prolog (с CD) - СПб.: БХВ-Петербург, 2003. 990 с.
4. Марков В.Н. Современное логическое программирование на языке Visual Prolog 7.5: учебник. - СПб.: БХВ-Петербург, 2016. 544 с.

УДК 004.8

СТРАТЕГИЯ ПРИНЯТИЯ РЕШЕНИЙ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ УПРАВЛЕНЧЕСКИХ ЗАДАЧ

Шеховцов Олег Иванович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: clarahena@mail.ru

Аннотация. Рассматривается подход к технологии управленческих задач. Информационная технология управленческих задач включает дидактическую компоненту и компоненту накопления знаний. Накопление знаний охватывает области процессов профессиональной деятельности, правил и приемов участников управляемого производственного процесса, программы-сценарии, управляющие производственным процессом, оценку действий участника процесса профессиональной деятельности.

Ключевые слова: информационные технологии; представление знаний; продукционная система; управление профессиональной деятельностью.

STRATEGY DECISION IN INFORMATION TECHNOLOGY MANAGEMENT GOALS

Shekhovtsov Oleg
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: clarahena@mail.ru

Abstract. Considers the approach to the technology of management tasks. Information technology for management tasks includes a didactic component and a component of knowledge accumulation. The accumulation of knowledge covers the areas of professional processes, rules and techniques of participants in the managed production process, scripted programs that manage the production process, and the evaluation of the actions of the participant in the professional process.

Keywords: operating system; Language Prolog; a Horn clause; predicates.

Деловая интеллектуальная стратегия принятия решений в информационных технологиях управленческих задач включает дидактическую компоненту и компоненту накопления знаний.

Компонента накопления знаний включает базу знаний, фиксирующую знания о некоторой предметной области в соответствии с выбранной моделью их представления. Для представления таких знаний выбрана, как наиболее подходящая, модель продукционной системы, то есть системы, основанной на правилах, сформированных в множества продукционных правил, реализующих все стадии формирования и проведения управленческого решения. Продукционная система включает три основных компоненты: интерпретатор (система управления); ситуационная модель (глобальная база данных); база знаний (множество продукционных правил). Компонента накопления знаний содержит знания о профессиональной деятельности, которые могут быть разделены на два рода знаний: знания I рода, включающие общезначимые факты и явления, признанные в данной области профессиональной деятельности, знания II рода, содержащие, в том числе, эвристические правила и приемы, приобретаемые конкретными участниками управляемого производственного процесса.

Компонента накопления знаний реализует двухэтапную процедуру наполнения базы знаний: настройку на исследуемую предметную область, включающую кодирование и ввод знаний I рода; настройку на конкретные задачи производственного процесса, задачи управления производственными процессами, процедуры выявления и ввода знаний II рода.

Характерными чертами знаний о профессиональной производственной деятельности и знаний об управлении производственной деятельностью, являются: логическая направленность, ситуационная природа, сравнительно частая модифицируемость. Согласно теории для представления таких знаний, уже с точки искусственного интеллекта, также наиболее подходит модель продукционной системы. Эффективность дидактической компоненты во многом зависит от способности системы управления объяснять свои действия при решении конкретных управленческих задач. Для выполнения этой функции реализуется специальная компонента объяснения.

Для эффективной работы компоненты накопления знаний о процессе профессиональной деятельности, помимо правил и приемов участников управляемого производственного процесса, необходимо содержать программы-сценарии, управляющие производственным процессом, включая оценку действий участника процесса профессиональной деятельности в достижении конечного результата его работы и процесса его достижения. Для решения этой задачи включены процедуры накопления и протоколирования знаний, их обобщение и представление в форме, удобной для размещения в базе знаний.

СПИСОК ЛИТЕРАТУРЫ

1. Хант Э. Искусственный интеллект, М., Изд-во: Мир, 1978, 558 с.
2. Логический подход к искусственному интеллекту: Пер. с франц./ Тейз А., Грибомон П., Луи Ж. и др. – М.: Мир, 1990. 429 с.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ И ТЕХНОЛОГИИ

УДК 004.056.2

ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ ДЕСТАБИЛИЗИРУЮЩИХ ФАКТОРОВ

Азманов Александр Васильевич, Емельянов Максим Владимирович, Кожевников Владимир Геннадьевич, Попов Дмитрий Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: azmanovavnsk@mail.ru, zibrovivan@mail.ru, kiyarmy@rambler.ru, bigwonder@rambler.ru

Аннотация. Рассмотрена информационная система в условиях воздействия дестабилизирующих факторов. Описаны дестабилизирующие факторы воздействия на информационную систему, приведена классификация дестабилизирующих факторов, в результате ослабления которых, возможно повышение устойчивости информационной системы.

Ключевые слова: информационная система; дестабилизирующие факторы; устойчивость.

ENSURING THE STABILITY OF THE INFORMATION SYSTEM UNDER THE INFLUENCE OF DESTABILIZING FACTORS

Azmanov Aleksander, Emelyanov Maksim, Kozhevnikov Vladimir, Popov Dmitry
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: azmanovavnsk@mail.ru, zibrovivan@mail.ru, kiyarmy@rambler.ru, bigwonder@rambler.ru

Abstract. The information system under the influence of destabilizing factors is considered. The article describes the destabilizing factors of influence on the information system, provides a classification of destabilizing factors, as a result of their weakening, it is possible to increase the stability of the information system.

Keywords: information system; destabilizing factors; stability.

Введение. Информация в современном мире превратилась в один из наиболее важных ресурсов, а информационные системы стали необходимым инструментом практически во всех сферах деятельности.

Информационная система – это взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели

Широкое внедрение информационных систем в жизнь современного общества привело к появлению ряда общих проблем информационной безопасности, т.е. воздействия дестабилизирующих факторов.

Дестабилизирующими факторами будем называть такие явления, события или угрозы, которые могут появляться на каком-либо этапе жизнедеятельности информационной системы и следствием которых могут быть нежелательные воздействия на информацию.

Перечень возможных типов дестабилизирующих факторов можно разделить на два вида: случайные и преднамеренные. В свою очередь к случайным угрозам относятся: стихийные бедствия и аварии, сбои и отказы технических средств, ошибки при разработке информационных систем, алгоритмические и программные ошибки, ошибки пользователей и обслуживающего персонала. К преднамеренным угрозам относятся: традиционный шпионаж и диверсии, несанкционированный доступ к информации, электромагнитные излучения и наводки, вредоносные программы.

В общем случае устойчивость функционирования информационной системы – способность информационной системы выполнять требования в условиях всех видов воздействия. Устойчивость функционирования информационной системы обеспечивается:

– разработкой мер при проектировании информационной системы общего пользования, направленных на выполнение требований к показателям надежности этой информационной системы общего пользования;

– соблюдением условий эксплуатации, установленных в технической и эксплуатационной документации соответствующих технических и программных средств информационной системы общего пользования;

– выполнением требований к информационной системе общего пользования в части технического обслуживания ее технических и программных средств;

– выполнением требований к управлению информационной системой общего пользования в части контроля функционирования и анализа технических неисправностей в информационной системе общего пользования.

Заключение. Показателем устойчивости функционирования информационной системы является коэффициент готовности, который определяется как вероятность того, что система окажется в работоспособном состоянии в произвольный момент времени ее функционирования. При выявлении несоответствия эксплуатационного значения коэффициента готовности технической норме, должны проводиться мероприятия, направленные на определение причин выявленного несоответствия, и их устранение.

СПИСОК ЛИТЕРАТУРЫ

1. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность: Учебное пособие. – М.: Форум, 2011. – 528 с.
2. Авраменко В.С., Бобрешов-Шишов Д. И., Беденков В. Н., Маликов А. В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. Т.3. – СПб.: СПБГУТ, 2017. – 535 с. С.13-18.
3. Паращук И.Б., Башкирцев А.С., Саяркин Л.А. Вариант формулировки показателей качества современных средств доверенной загрузки и их роль при решении проблем безопасности алгоритмов управления инфотелекоммуникационными системами специального назначения. // Вопросы оборонной техники. Научно-технический журнал. Серия 16, №5-6, 2016. С. 47-51.

УДК 004.942

ПЕРЕХОД НА РОССИЙСКОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Азманов Александр Васильевич, Зибров Иван Александрович, Кий Андрей Вячеславович, Попов Дмитрий Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: azmanovavnsk@mail.ru, zibrovivan@mail.ru, kiyarmy@rambler.ru, bigwonder@rambler.ru

Аннотация. Рассмотрена возможность замещения программ иностранного производства российскими, зарегистрированными в Едином реестре российских программ. Отмечено, что при переходе на российское программное обеспечение проблемы возникают из-за отсутствия стандартизации основных бинарных интерфейсов и команд различных дистрибутивов. Предложен перечень возможных методов портирования.

Ключевые слова: программное обеспечение; импортозамещение; операционная система; дистрибутив.

SWITCHING TO RUSSIAN SOFTWARE

Azmanov Aleksandr, Zibrov Ivan, Kij Andrej, Popov Dmitrij
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: azmanovavnsk@mail.ru, zibrovivan@mail.ru, kiyarmy@rambler.ru, bigwonder@rambler.ru

Abstract. The possibility of replacing foreign-made programs with Russian ones registered in the Unified register of Russian programs is considered. It is noted that when switching to Russian software, problems arise due to the lack of standardization of the main binary interfaces and commands of various distributions. A list of possible porting methods is proposed.

Keywords: software; import substitution; operating system; distribution.

Введение. В связи с развёрнутой в России политикой импортозамещения, коснувшейся и сферы информационных технологий, обозначен ряд проблем, которые необходимо решить в ближайшем будущем. Необходимо провести анализ существующих прикладных систем на предмет совместимости с выбранными импорто-независимыми операционными системами (ОС), общесистемными сервисами (такими, как служба каталогов и система защиты информации от НСД и др.), системой управления базами данных и другими базовыми технологиями. Для приложений, которые сами на ОС не запускаются, необходимо сделать выбор, обоснование и реализацию механизмов работы таких прикладных систем. К числу основных механизмов такого рода относятся: эмуляция, виртуализация различных типов (локальная, удаленная, контейнерная), терминальный доступ и др. [1].

Не менее сложная проблема стоит с миграцией офисных приложений, либо приложений, использующих для реализации части своих функций пакеты программ Microsoft Office. Проблема офисных систем заключается в том, что этот вид ПО является общесистемным. Например, недостаточно мигрировать офис. Необходимо еще в программах из состава прикладного программного обеспечения (ППО) мигрировать экспорт отчетов, отладить печать, обеспечить интеграционный обмен.

Перенос ППО, написанного для использования на различных версиях отечественных сборок ОС семейства Linux также вызывает ряд проблем. Это связано с наличием конкурирующих дистрибутивов Linux, имеющих существенные различия, несмотря на использование открытого и бесплатного ПО. В связи с тем, что отсутствует универсальный способ написания программ, гарантированно обеспечивающий их переносимость в рамках организации FSG (Free Standards Group – консорциум по развитию открытых стандартов), был разработан

стандарт LSB (Linux Standard Base – базовое семейство стандартов Linux), направленный на стандартизацию основных бинарных интерфейсов и команд различных дистрибутивов. Однако, даже имея исходные коды программы, ее бывает сложно перенести на новую АПП. Это связано с тем, что в ОС Linux тот слой, с которым взаимодействует пользовательское приложение, в основном реализован не в ядре ОС. Подавляющая часть функциональности обеспечивается внешними библиотеками поддержки. Масштабность ОС Linux и количество параметров сборки любого ее дистрибутива приводят к плохо совместимым между собой продуктам, что создает дополнительные проблемы для разработчиков прикладного ПО [2].

Анализ особенностей АПП как среды переноса ПО позволяет выделить следующий перечень возможных методов портирования [3]: повторное использование бинарных файлов; переиспользование исходного кода на языках высокого уровня; использование интерпретируемого кода; использование эмуляторов ABI; виртуализация; использование Web-технологий; разработка нового ПО.

Заключение. В целом, для качественного решения задачи портирования, перенос ППО на отечественную АПП должен опираться на требования государственных и международных стандартов в области автоматизированных систем и жизненного цикла программных средств, при этом особое внимание необходимо уделять предварительному анализу условий переноса, учету наиболее значимых факторов, влияющих на результаты переноса и оценке качества ППО после завершения переноса на новую АПП, что по мнению авторов, позволит учесть риски переноса и избежать неэффективных материальных и временных затрат.

СПИСОК ЛИТЕРАТУРЫ

1. Написание переносимых программ [Электронный ресурс]. URL: http://givi.olnd.ru/wclr/15_portable.html (дата обращения 02.04.2020г.)
2. Переносимость программного обеспечения GNU [Электронный ресурс]. URL: http://www.osp.ru/os/1993/02/178447/ (дата обращения 02.04.2020г.)
3. Методы обеспечения переносимости ПО. [Электронный ресурс]. URL: http://citforum.ru/SE/testing/portability/ (дата обращения 02.04.2020г.)

УДК 621.391, 004.056

МОДЕЛЬ РАСЧЕТА ЗОНЫ ПОКРЫТИЯ МОБИЛЬНОГО УСТРОЙСТВА ВСЕПРОНИКАЮЩЕЙ СЕНСОРНОЙ СЕТИ

Астахова Татьяна Николаевна[1], Колбанев Михаил Олегович[2], Шамин Алексей Анатольевич[1]
[1] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: mokolbanev@mail.ru, ctn_af@mail.ru, ngiei-spo@mail.ru

Аннотация. В настоящей работе главное внимание уделяется построению модели расчета зоны покрытия мобильного устройства в зависимости от энергопотребления.

Ключевые слова: всепроникающая сенсорная сеть; неголономные связи; система управления; уравнение движения; энергия; энергопотребление.

MODEL FOR CALCULATING THE COVERAGE AREA OF A MOBILE DEVICE OF UBIQUITOUS SENSOR NETWORKS

Astakhova Tatyana[1], Kolbanev Mikhail[2], Shamin Alexey[1]
[1] Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: mokolbanev@mail.ru, ctn_af@mail.ru, ngiei-spo@mail.ru

Abstract. In this work, the main attention is paid to the construction of a model for calculating the coverage area of a mobile device depending on energy consumption.

Keywords: ubiquitous sensor network; pervasive sensor network; nonholonomic ties; control system; equation of motion; energy; energy consumption.

Введение. В настоящей работе главное внимание уделяется построению модели расчета зоны покрытия мобильного устройства в зависимости от энергопотребления, которое необходимо для передачи сообщений от этих мобильных устройств сенсорной сети, например, на базовую станцию. Достижения в области беспроводной связи позволили разработать недорогие, маломощные, многофункциональные, мобильные миниатюрные сенсорные устройства, которые могут воспринимать окружающую среду, выполнять обработку данных и общаться друг с другом без привязки на коротких расстояниях и передвигаться [1].

Типичная всепроникающая сенсорная сеть состоит из тысяч сенсорных узлов, развернутых в соответствии с некоторым предопределенным статистическим распределением по заданной поверхности. Сам по себе мобильное сенсорное устройство имеет серьезные ограничения по ресурсам, такие как ограниченная память, мощность батареи, обработка сигналов, вычислительные и коммуникационные возможности; следовательно, оно

может воспринимать только небольшую часть окружающей среды и давать обратную связь в соответствии с определенными условиями. Однако множество датчиков, сообщающихся между собой, в совокупности, может эффективно выполнять гораздо более масштабную задачу. Они могут воспринимать и собирать необработанные данные из окружающей среды, выполнять локальную обработку, возможно, взаимодействовать друг с другом оптимальным образом для выполнения агрегации [2], а затем направлять агрегированные данные к приемникам или базовым станциям.

Всепроникающая сенсорная сеть является сетью интеллектуальных подвижных сенсорных устройств, которые в пределах сенсорного поля могут менять свое местоположение. Использование всепроникающей сенсорной сети является одним из наиболее востребованных и распространенных методов сбора и передачи данных [3].

Одним из важных критериев возможности развертывания эффективной всепроникающей сенсорной сети является поиск оптимальных стратегий распределения мобильных устройств, задание возможных траекторий движения, выбор протоколов маршрутизации и эффективных методов управления топологией [4].

С практической точки зрения, все мобильные устройства распределены по сенсорному полю в соответствии с вероятностным законом распределения и перемещаются согласно некоторому закону движения, а потому, весьма затруднительно правильно подобрать необходимый протокол маршрутизации, который сводит к минимуму все желательные показатели одновременно, такие как достаточный радиус покрытия и связность, низкие вычислительные и коммуникационные издержки. Понятие зоны покрытия можно рассматривать как меру качества обслуживания (QoS) в сенсорной сети, поскольку оно означает, насколько хорошо каждая точка в сенсорном поле покрыта датчиками. После развертывания узлов в области мониторинга они образуют коммуникационную сеть, которая может динамически изменяться во времени в зависимости от мобильности устройств, остаточного заряда батареи, статических и движущихся препятствий, наличия шума и т. д.

Объем энергопотребления интеллектуальными сенсорами является ключевой характеристикой всепроникающих сенсорных сетей. Важной особенностью является автономность и мобильность сенсорных устройств. Целесообразно получать информацию, в виде блоков данных в те моменты, когда они находятся ближе к базовой станции [5]. Значительная часть затрат энергии связана с информационным взаимодействием сенсорных устройств с базовой станцией. Причем, чем ближе сенсорное устройство находится к базовой станции, тем меньше энергии тратит при передаче информационного блока.

В процессе реализация протоколов маршрутизации необходимо определять зону действия или зону покрытия. Как правило, при моделировании эту зону считают кругом на плоскости, а если в пространстве шаром. Однако, с практической точки зрения, это не так, поскольку радиосигналы в разных направлениях имеют разный радиус действия.

Если обозначит это так, а это так, то система ДУ будет выглядеть следующим образом. Если функция управления, которая задает радиус действия в пространстве.

Зона покрытия мобильного устройства является важной характеристикой ВСС. Правильное определение этой зоны влияет на выбор протоколов маршрутизации. Эта зона зависит от энергии, которая тратиться мобильным устройством на передачу блока информации, а также от свойств пространства, в котором используется всепроникающая сенсорная сеть.

В докладе предлагается рассчитывать эту зону с учетом особенностей распространения радиосигнала в разных направлениях.

Пусть задана система управления движения мобильного устройства всепроникающей сенсорной сети:

$$\dot{x} = f(x,u),\ x \in D \subseteq \mathbb{R}^n, u \in U \subseteq \mathbb{R}^m, \quad (1)$$

где x – фазовый вектор, u – управление; точка обозначает производную по времени t. Будем предполагать, что D – область, $0 \in D$, U – замкнутая область, $f \in C^1(\mathbb{R}^n \times \mathbb{R}^m)$. И предположим, что заданная функция управления $u(t,e) \in U$, зависящая от параметра $e \in \mathbb{R}^k$. Эта функция может быть определена в зависимости от условий работы [6]. Неголономные системы, в которых связи не являются классическими, представляют большой интерес, к таким системам и относятся мобильные устройства всепроникающей сенсорной сети. Предположим, что движение мобильного устройства удовлетворяет условиям задачи о качании твердого тела без проскальзывания по неподвижной поверхности. Тогда, если это так, то эффективную зону покрытия можно определить в результате решения системы дифференциальных уравнений такого вида:

$$\dot{x} = v\cos\varphi, \dot{y} = v\sin\varphi, \dot{\varphi} = u(t,e),$$

где e – энергия, которая тратится мобильным устройством в разных направлениях; величины u, v рассматриваются в системе как управляющие воздействия. Таким образом система (1) имеет трехмерный вектор состояния (x, y, φ) и двумерный вектор управления (u, v). В случае $v \equiv 1$ система (1) известна в литературе как «машина Дубинса» [7]. Такая модель описывает движение машины по плоскости. Машина может ехать вперед с постоянной линейной скоростью и одновременно поворачиваться с угловой скоростью $u(t,e)$. Допустимые траектории машины – плоские кривые ограниченной кривизны, если управление u ограничено.

Управляющая функция может быть определена в городских постройках, формулы расчета зависят от условий сети.

Заключение. В докладе приводятся результаты расчёта для промышленных и сельскохозяйственных областей использования всепроникающей сенсорной сети. Результаты решений по предложенному алгоритму в дальнейшем предполагается использовать для определения зон покрытия на основе специализированного программного обеспечения с учетом мощности передатчика, диапазона частот, объема передаваемого блока

данных, интенсивности передачи, загрузки, характера рельефа, застройки местности и др. В представленной работе проведены имитационные исследования для изучения способов улучшения пространственного покрытия всепроникающей сенсорной сети при различных параметрах движения мобильных устройств.

СПИСОК ЛИТЕРАТУРЫ

1. Ghosh A., Das S. K. Coverage and connectivity issues in wireless sensor networks: A survey // Pervasive and Mobile Computing. Vol. 4. №. 3. 2008. P. 303–334.
2. Kokar M. M., Tomasik J.A., Weyman J. Data vs. decision fusion in the category theory framework, in: Proceedings of the 4th International Conference on Information Fusion, FUSION'01, Montreal, Australia, August 2001.
3. Koucheryavy A., Vladyko A., Kirichek R.: State of the art and research challenges for public flying ubiquitous sensor networks. In: Internet of Things, Smart Spaces, and Next Generation Networks and Systems, Springer, Cham, 299–308 (2015).
4. Santi P. Topology Control in Wireless Ad Hoc and Sensor Networks, John Wiley and Sons, 2005.
5. Bogatyrev A V., Bogatyrev V. A., Bogatyrev S. V.: Multipath Redundant Transmission with Packet Segmentation. In: 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 1–4 (2019). https://doi.org/10.1109/WECONF.2019.8840643
6. Егоров Л. Л., Кологривов В. А., Мелихов С. В. Алгоритм расчета зон покрытия базовых станций сотовой связи // Доклады ТУСУРа (Томск). 5(19), 2009. С. 15–20.
7. Аграчев А. А., Сачков Ю. Л. Геометрическая теория управления. – М.: Физматлит, 2004. 392 с.

УДК 621.396.4

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ: ОБЗОР И АНАЛИЗ СОВРЕМЕННЫХ ТРЕБОВАНИЙ

Башкирцев Андрей Сергеевич[1], Митрофанов Евгений Александрович[1], Паращук Игорь Борисович[2]
[1] Военный инновационный технополис ЭРА
Пионерский пр., 28, Анапа, Краснодарский край, 353456, Россия
[2] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: ab098@ya.ru, smetanaks81@mail.ru, shchuk@rambler.ru

Аннотация. Рассмотрен комплекс современных требований к автоматизированным системам управления телекоммуникационными сетями. Проведен детальный анализ общих требований, а также требований к техническому и иным видам обеспечения автоматизированных систем, которые призваны обеспечить своевременное и устойчивое управление телекоммуникационными сетями в современных условиях. Выполнение этих требований в комплексе позволит обеспечить оптимальное управление и, в конечном итоге, эффективное функционирование телекоммуникационных сетей.

Ключевые слова: требования, автоматизированная система управления, телекоммуникационная сеть, обеспечение, информация, функции, персонал.

AUTOMATED TELECOMMUNICATION NETWORK MANAGEMENT SYSTEMS: REVIEW AND ANALYSIS OF MODERN REQUIREMENTS

Bashkirtsev Andrey[1], Mitrofanov Yevgeny[1], Parashchuk Igor[2]
[1] Military Innovative Technopolis ERA
28 Pionersky Av, Anapa, Krasnodar Territory, 353456, Russia
[2] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: ab098@ya.ru, smetanaks81@mail.ru, shchuk@rambler.ru

Abstract. A set of modern requirements for automated telecommunication network management systems is considered. A detailed analysis of the general requirements, as well as the requirements for technical and other types of software for automated systems, which are designed to ensure timely and sustainable management of telecommunication networks in modern conditions, is carried out. The fulfillment of these requirements in the complex will ensure optimal management and, ultimately, the effective functioning of telecommunication networks.

Keywords: requirements, automated management system, telecommunications network, software, information, functions, personnel.

Введение. Появление и активное применение автоматизированных систем управления (АСУ) телекоммуникационными сетями (ТКС) привело, помимо повышения качества функционирования ТКС, к множеству полезных технико-экономических, социальных и других эффектов, таких как повышение своевременности и обоснованности решений администратора сети, снижению численности управленческого персонала, повышению качества управления ТКС в целом и другим [1, 2].

Автоматизированные системы управления должны обеспечивать достижение целей создания (развития) и функционирования сложных управляемых ТКС, причем в АСУ должна быть обеспечена совместимость между их частями, а также со всеми автоматизированными системами, взаимосвязанными с данной системой. При этом в случаях, когда АСУ ТКС или совокупность АСУ создана на базе вычислительной сети, для обеспечения совместимости между элементами такой сети должны быть применены системы протоколов многоуровневого

взаимодействия, а сама автоматизированная система в целом и все виды ее обеспечения должны быть приспособлены к модернизации, развитию и наращиванию. Надежность и адаптивность АСУ должны быть достаточными для достижения установленных целей функционирования ТКС в заданном диапазоне изменений условий применения. Кроме того, в АСУ ТКС должны быть предусмотрены контроль правильности выполнения автоматизируемых функций и диагностирование с указанием места, вида и причины возникновения нарушений правильности функционирования автоматизированной системы [3]. Много современных общих требований к АСУ ТКС касаются информации: любая поступающая в АСУ ТКС информация должна быть надежна и достоверна; информация, содержащаяся в базах данных АСУ ТКС, должна быть актуализирована в соответствии с периодичностью ее использования при выполнении функций системы; АСУ ТКС должна быть защищена от утечки информации. Система управления в необходимых объемах должна в автоматизированном режиме выполнять: сбор, обработку и анализ информации (сигналов, сообщений, документов и т. п.) о состоянии объекта управления; выработку управляющих воздействий (программ, планов и т. п.); передачу управляющих воздействий (сигналов, указаний, документов) на исполнение и ее контроль [4]; реализацию и контроль выполнения управляющих воздействий [4], а также обмен информацией с взаимосвязанными системами.

Особого внимания, на наш взгляд, заслуживают требования к техническому обеспечению АСУ ТКС. Комплекс технических средств АСУ ТКС должен быть достаточным для выполнения всех автоматизированных функций системы такого класса.

В комплексе технических средств АСУ ТКС должны, в основном, использоваться технические средства серийного отечественного производства. При необходимости допускается применение технических средств единичного производства. Тиражируемые АСУ ТКС и их части должны строиться на базе унифицированных технических средств. Технические средства должны быть размещены с соблюдением не только требований по предназначению, но и требований, содержащихся в технической, в том числе эксплуатационной, документации на них, и так, чтобы было удобно использовать их при функционировании АСУ ТКС и выполнять техническое обслуживание. Технические средства АСУ ТКС необходимо использовать в условиях, определенных в эксплуатационной документации. В случаях, например, когда необходимо их использование в среде, параметры которой превышают допустимые значения, установленные для этих технических средств, должны быть предусмотрены меры защиты отдельных технических средств АСУ ТКС от влияния внешних воздействующих факторов. В технических средствах АСУ ТКС должны быть использованы средства вычислительной техники, удовлетворяющие современным общим техническим требованиям.

Программное обеспечение АСУ ТКС должно быть достаточным для выполнения всех ее функций, реализуемых с применением средств вычислительной техники, а также иметь средства организации всех требуемых процессов обработки данных, позволяющие своевременно выполнять все автоматизированные функции во всех регламентированных режимах функционирования. Программное обеспечение АСУ ТКС должно обладать функциональной достаточностью (полнотой), защищенностью, надежностью (в том числе восстанавливаемостью, наличием средств выявления ошибок), адаптируемостью, модифицируемостью, модульностью построения и удобством в эксплуатации.

Информационное обеспечение АСУ ТКС должно быть достаточным, а для шифрования и кодирования информации, используемой в АСУ ТКС, должны быть применены известные системы и алгоритмы. Кроме того, информационное обеспечение АСУ ТКС должно быть совместимо с информационным обеспечением систем, взаимодействующих с ней, по содержанию, системе кодирования, методам адресования, форматам данных и форме представления информации, получаемой и выдаваемой АСУ ТКС. Лингвистическое обеспечение должно быть достаточным для общения различных категорий пользователей в удобной для них форме со средствами автоматизации и для осуществления процедур преобразования и машинного представления обрабатываемой в системе информации.

Лингвистическое обеспечение АСУ ТКС должно быть отражено в документации организационного обеспечения в виде правил общения пользователей с техническими средствами АСУ во всех режимах функционирования системы. Важной особенностью являются требования по безопасности, поскольку неправильные действия персонала АСУ ТКС не должны приводить к аварийной ситуации.

Требования по защите информации в АСУ ТКС. В автоматизированной системе управления ТКС объектами защиты являются [5]: информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация); программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации. При проектировании и построении системы, призванной осуществлять защиту АСУ ТКС должны быть: определены типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа); определены методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в АСУ ТКС.

Заключение. Таким образом, рассмотрен комплекс современных требований к автоматизированным системам управления телекоммуникационными сетями. Проведен детальный анализ общих требований, а также требований к техническому и иным видам обеспечения автоматизированных систем, которые призваны обеспечить своевременное и устойчивое управление телекоммуникационными сетями в современных условиях. Выполнение этих требований в комплексе позволит обеспечить оптимальное управление и, в конечном итоге, эффективное функционирование телекоммуникационных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Межгосударственный стандарт ГОСТ 34.003-90 Автоматизированные системы. Термины и определения. – М.: Стандартинформ, 1992. – 14 с.
2. Межгосударственный стандарт ГОСТ 24.104-85 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования. – М.: Стандартинформ, 1985. – 23 с.
3. Ермолаева В.В., Калашников Д.А. Автоматизированные системы управления // Молодой ученый. №11. 2016. С. 166-168.
4. Паращук И.Б., Башкирцев А.С., Ногин С.Б. Динамическая оптимизация параметров контроля в интересах управления связью между различными информационно-аналитическими и вычислительными системами // Естественные и технические науки. №4 (94), 2016. С. 24-28.
5. Приказ ФСТЭК России от 14 марта 2014 года №31. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. (с изменениями на 9 августа 2018 года). – М.: ФСТЭК. 2014. – 28 с.

УДК 004.946

ПРИМЕНЕНИЕ ТРЕНАЖЕРНО-ОБУЧАЮЩИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Белый Кирилл Иванович, Киреев Сергей Хаирбекович, Островский Юрий Николаевич, Юдин Анатолий Алексеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: Novpochta2000@mail.ru

Аннотация. Рассмотрены перспективы применения тренажерно-обучающих систем с применением технологий виртуальной и дополненной реальности в процессе подготовки специалистов для войск связи. Рассмотрен алгоритм работы тренажерно-обучающих систем с использованием технологии дополненной и виртуальной реальности.

Ключевые слова: тренажерно-обучающие системы; технологии виртуальной и дополненной реальности; обучающий процесс; модель; образовательный контент.

TRAINING AND TRAINING SYSTEMS USING VIRTUAL AND AUGMENTED REALITY TECHNOLOGIES

Beliy Kirill, Kireev Sergey, Ostrovski Yury, Yudin Anatoly
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: Novpochta2000@mail.ru

Abstract. The analysis of prospects of using training systems with the use of virtual and augmented reality technologies in the process of training specialists for the communications forces is carried out. The algorithm of operation of training systems using augmented and virtual reality technology is considered.

Keywords: training systems; virtual and augmented reality technologies; training process; model; educational content.

Введение. В условиях высокого темпа технологизации, развития техники и средств связи, существующие традиционные, пассивные формы обучения не обеспечивают формирование требуемых компетенций военных связистов. Организация учебного процесса на основе индивидуальной образовательной траектории позволит синхронизировать уровень подготовки и качество знаний выпускников Военной академии связи с требованиями Главного управления Связи Вооруженных Сил Российской Федерации по эксплуатации действующей и перспективной техники связи и автоматизации, с подготовкой военных специалистов «на опережение». Предлагаемые современные образовательные технологии носят универсальный характер, что свидетельствует о возможности ее реализации в системе боевой подготовки специалистов и подразделений связи Вооруженных Сил Российской Федерации.

Существующий на сегодняшний день подход к обучению специалистов, работающих на сложном оборудовании, основан на традиционных методиках, использующих логическую последовательность связанных текстовых, графических и мультимедийных материалов. В свою очередь, специфика проведения обучения на реальных эксплуатируемых комплексах связи, которые имеют высокую стоимость, обуславливается рисками возможных аварий, нештатных ситуаций или поломками дорогостоящего оборудования.

Для повышения эффективности подготовки специалистов сложных технических комплексов предлагается использовать современные тренажерно-обучающие системы (ТОС) в основу которых положены технологии виртуальной и дополненной реальности.

Активное использование ТОС позволит: синхронизировать уровень знаний, умений и навыков обучающихся к эксплуатации технически сложного оборудования, подготовку специалистов «на опережение».

Заключение. Применение современных образовательных технологий виртуальной и дополненной реальности позволят обеспечить повышение целенаправленности, активности, самостоятельности, степени индивидуализации, уровня осознанности учебной работы, объективности контроля и самоконтроля за деятельностью обучающихся. При этом расширится спектр реализуемых при проведении учебных занятий принципов обучения. В результате повысится эффективность процесса обучения, качество подготовки военных специалистов.

СПИСОК ЛИТЕРАТУРЫ

1. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые сетевые технологии в системах военного назначения. Учебник. Под редакцией профессора И.Б.Саенко. – СПб.: ВАС, 2010. 520 с.
2. Еремеев А.П., Куриленко И.Е. Применение технологии виртуализации в образовательном процессе // Материалы VIII международной научно-технической конференции Новые информационные технологии и менеджмент качества (NIT&QM'2011) – М.:ООО "Арт-Флэш", 2011. - С.120-123.
3. Куриленко И.Е., Еремеев А.П. Модернизация образовательного процесса с помощью современных сетевых технологий и виртуализации ресурсов // Труды международной научно-методической конференции Информатизация инженерного образования - ИНФОРИНО-2012 (Москва, 10-11 апреля 2012 г.) – М.: Издательский дом МЭИ, 2012. - С.43-46.
4. Бойкова А.В. Использование информационных технологий в образовательном процессе военного вуза //Интернет-журнал «Мир науки» 2017, Том 5, номер 6. С. 2-3.
5. Раецкая О.В. Информационная среда современного военного вуза // Интернет-журнал «Мир науки» 2017, Том 5, номер 5. С.2-4.
6. Самойлов Василий Дмитриевич. Совершенствование системы высшего образования офицеров Вооруженных Сил Российской Федерации [Электронный ресурс]: Дис. д-ра пед. наук: 13.00.01.-М.: РГБ, 2003 (Из фондов Российской Государственной библиотеки).

УДК 004

ДВУХФАЗНАЯ МОДЕЛЬ МНОЖЕСТВЕННОГО ДОСТУПА К ИНФОКОММУНИКАЦИОННЫМ РЕСУРСАМ

Верзун Наталья Аркадьевна, Колбанёв Михаил Олегович, Романова Анна Александровна,
Цехановский Владислав Владимирович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru, vvcehanovsky@mail.ru

Аннотация. Предлагается протокол регулируемого множественного доступа к коммуникационным ресурсам на участке последней мили – сенсорной сети интернета вещей. Протокол доступа учитывает особенности киберфизических систем: неоднородность поддерживаемых приложений, сверхплотность сетей, необходимость экономии ресурсов компонентов сетей. Предусматривается использование двухфазной модели обслуживания потоков неоднородных данных от умных вещей. Разработана математическая модель, позволяющая оценивать качество передачи в сети доступа на последней миле.

Ключевые слова: киберфизическая система; интернет вещей; эфирная сеть; множественный доступ; двухфазная модель доступа; вероятностно-временные характеристики.

TWO-PHASE MODEL OF MULTIPLE ACCESS TO INFOCOMMUNICATION RESOURCES

Verzun Natalia, Kolbanev Mikhail, Romanova Anna, Cehanovsky Vladislav
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru, vvcehanovsky@mail.ru

Abstract. A Protocol for controlled multiple access to communication resources on the last mile section of the Internet of things sensor network is proposed. The access Protocol takes into account the features of cyberphysical systems: heterogeneity of supported applications, super-density of networks, and the need to save resources of network components. It is planned to use a two-phase model for servicing flows of heterogeneous data from smart things. A mathematical model has been developed that allows evaluating the quality of transmission in the access network at the last mile.

Keywords: cyberphysical system; Internet of things; ethereal network; multiple access; two-phase access model; probability-time characteristics.

Инфраструктурная база приложений интернета вещей – эфирные сенсорные сети [1]. Их применение в целях создания киберфизических систем поддержки хозяйственной деятельности, требует учитывать следующие особенности:

– автономность питания умных вещей и, соответственно, ограниченность их энергоресурсов и необходимость их экономии;

– большое число умных вещей и образование так называемых сверхплотных сетей, для которых актуальной задачей становится рациональное распределение ограниченных ресурсов (имеющихся каналов передачи) между большим числом источников данных;

– число умных вещей, обеспечивающих покрытие пространства информационной решеткой и собирающих однотипную информацию об окружающей их среде, как правило, избыточно (зачастую сенсоры собирают и передают дублирующиеся данные). Поэтому, частичная потеря данных, передаваемых группой однотипных сенсоров, существенным образом не скажется на адекватности оценки ситуации в целом;

– разнообразие поддерживаемых приложений интернета вещей. Приложения могут существенно отличаться по требованиям к скорости, качеству и надежности передачи данных, необходимым для их полноценного функционирования. Например, в медицине: показания датчиков измерения температуры тела пациента можно передавать гораздо реже, чем показания датчиков измерения частоты его пульса.

Совокупность вышеперечисленных особенностей ведет к увеличению нагрузки на сети последней мили: дефицит доступного частотного ресурса эфирной сети приводит к возникновению ситуаций перегрузки и невозможности полноценного обслуживания всех умных вещей. Поэтому одна из актуальных задач в сфере инфокоммуникаций – разработка новых протоколов доступа к инфокоммуникационным ресурсам, которые бы учитывали особенности современных сетей на последней миле, поддерживающих работу киберфизических систем [2–4].

Для минимизации негативного воздействия перегрузок на функционирование инфраструктуры киберфизической системы необходимо:

– при организации сбора данных с сенсоров на последней миле, предусматривать механизмы отсеивания (или отбрасывания) части поступающего трафика.

– учитывать гетерогенный характер поддерживаемых приложений интернета вещей (например, чувствительность приложений к задержкам передачи).

В докладе предлагается модель регулируемого двухфазного доступа к ресурсам эфирной сети на последней миле и рассматривается сценарий доступа, которые предполагают гибкое деление общего ресурса сети – каналов передачи между умными вещами различных типов.

Передача поступающих от умных вещей блоков данных осуществляется в две фазы:

I-я фаза – регулирование объема поступающего на обслуживание трафика. Предлагается два варианта организации I-й фазы:

1 вариант – режим обслуживания с потерями, т.е. в случае, когда поступает заявка на передачу блока данных, а свободных каналов соответствующего типа нет, то заявка на обслуживание отбрасывается;

2 вариант – режим обслуживания с ожиданием т.е. в случае, когда поступает заявка на передачу блока данных, а свободных каналов соответствующего типа нет, то заявка ставится в очередь и ждет освобождения канала для передачи.

II-я фаза – передача блоков данных в соответствии с регулируемым синхронно-временным методом множественного доступах [5], в котором предусмотрено регулирование доступа умных вещей к каналу передачи: чем строже требования к допустимому времени задержки блока данных по сети, предъявляемые приложением интернета вещей, тем чаще умные вещи, поддерживающие работу данного приложения, получают право на передачу и тем меньше интервал однократной передачи блока данных для умных вещей такого типа.

Разработана математическая модель, позволяющая оценивать качество передачи в сети доступа на последней миле. Получены выражения для расчета вероятностно-временных характеристик процесса передачи различных типов данных: среднее времени и вероятности своевременной доставки блоков данных, формируемых умными вещами, и информационной скорости реального времени. Проведен численный расчет и анализ влияния параметров регулируемого множественного доступа на вероятностно-временные характеристики процесса передачи в сети.

Описанный подход к организации доступа умных вещей к сетевым ресурсам позволит регулировать объем передаваемого трафика для устранения ситуаций перегрузок, а также обеспечивать требуемое качество передачи для различных видов приложений интернета вещей.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н. А., Колбанев М. О., Омельян А. В. Сетевая архитектура цифровой экономики. СПб.: Изд-во СПбГЭУ. 2018. 156 с.
2. Верзун Н. А., Колбанев М. О., Цехановский В. В. Принципы построения и характеристики цифровых сетей нового поколения. СПб.: Изд-во СПбГЭТУ «ЛЭТИ» . 2017. 212 с.
3. Verzun N., Kolbanev M., Vorobeva D. Model of a Centralized Strategy for Selecting the Last Mile Access Network \\ Proceedings of the 11th Majorov International Conference on Software Engineering and Computer Systems, Saint Petersburg, Russia, December 22-13, 2019. http://ceur-ws.org/Vol-2590/paper10.pdf
4. Verzun N., Kolbanev M., Shamin A.The Architecture of the Access Protocols of the Global Infocommunication Resources Computers 2020, 9, 49; https://doi.org/10.3390/computers9020049 .
5. Верзун Н. А., Колбанёв М. О., Омельян А. В. Регулируемый множественный доступ в беспроводной сети умных вещей // Омский науч. вестн. Сер. Информатика, вычислительная техника и управление. 2016. № 4 (148). – С. 147–151.

УДК 004.942

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК И ЗАЩИТА ОТ НИХ НА ОСНОВЕ ВЫЯВЛЕНИЯ ОТКЛОНЕНИЙ В ЭВРИСТИКАХ ТРАФИКА СВЕРХВЫСОКИХ ОБЪЕМОВ: АНАЛИЗ СОВРЕМЕННЫХ ИННОВАЦИОННЫХ РЕШЕНИЙ

Виткова Лидия Андреевна, Паращук Игорь Борисович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия ВО, 39, Санкт-Петербург, 194064, Россия,
e-mails: vitkova@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Проведен анализ и сравнение современных инновационных решений по выявлению отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них. В качестве критериев для сравнения методов и технических решений учитывался комплекс характеристик эффективности как отдельных решений по сбору, предобработке, хранению, сигнатурному анализу, анализу на базе биоинспирированных подходов, машинному обучению и аналитическому моделированию, так и комплексных решений и тенденций по построению систем выявления отклонений в эвристиках трафика сверхвысоких объемов в целом.

Ключевые слова: сетевая атака, инновационное решение, трафик, аномалия, большие данные, устройство, способ, патентный поиск.

DETECTION OF NETWORK ATTACKS AND PROTECTION AGAINST THEM ON THE BASIS OF IDENTIFICATION OF DEVIATIONS IN HEURISMS OF TRAFFIC OF EXTRA VOLUME: ANALYSIS OF MODERN INNOVATIVE SOLUTIONS

Vitkova Lydia, Parashchuk Igor
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)
39, 14-th Linia, VI, St. Petersburg, 199178, Russia
e-mails: vitkova@comsec.spb.ru, shchuk@rambler.ru

Abstract. The analysis and comparison of modern innovative solutions to identify deviations in the heuristics of ultra-high volume traffic to detect network attacks and protect against them. As criteria for comparing methods and technical solutions, a set of performance characteristics was taken into account as individual solutions for the collection, pre-processing, storage, signature analysis, analysis based on bio-inspired approaches, machine learning and analytical modeling, as well as integrated solutions and trends in constructing deviation detection systems in heuristics of ultra-high volume traffic in general.

Keywords: network attack, innovative solution, traffic, anomaly, big data, device, method, patent search.

Введение. Основным начальным этапом любого современного научно-технического телекоммуникационного либо иного проекта является анализ современных инновационных решений в данной конкретной области. Важным элементом этого этапа является, так называемый, патентный поиск. Анализ существующих работ и современных инновационных решений в целом, и патентный поиск, в частности, проводятся с целью проверки чистоты результатов научно-исследовательской работы, корректности и уникальности полученных результатов, а также имеет важное научное, правовое и этическое значение. С учетом современного развития систем защиты информации продолжает оставаться актуальной проблема разработки методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них. В рамках реализации этапов решения данной научно-технической проблемы предполагается сформулировать и решить задачи, недостаточно исследованные с точки зрения получения фундаментальных теоретических и практических результатов в области обнаружения сетевых атак и защиты от них в условиях трафика сверхвысокого объема. Эти задачи включаю разработку математических методов, моделей и алгоритмов: сбора и предобработки сетевого трафика сверхвысокого объема; хранения сетевого трафика сверхвысокого объема; сигнатурного анализа трафика высокого объема; биоинспирированных методов, моделей и алгоритмов выявления отклонений в эвристиках трафика сверхвысоких объемов, обнаружения сетевых атак и защиты от них; математических методов, моделей и алгоритмов аналитического моделирования и машинного обучения, направленных на выявление отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них.

Для решения нашей задачи – разработки методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них, ключевыми словами и выражениями являются: большие данные; сигнатурный анализ данных; хранение больших массивов данных; сбор, предобработка, агрегация, нормализация и анализ больших массивов данных; выявление отклонений (аномалий) в трафике; обнаружение сетевых атак на основе биоинспирированных подходов, машинного обучения и аналитического моделирования, а также защита от сетевых атак.

С учетом того факта, что в Патентном законе Российской Федерации не признается патентоспособность научных теорий, математических методов, правил и методов интеллектуальной и хозяйственной деятельности, компьютерных программ, и решений, заключающихся только в представлении информации [1], проводится

анализ существующих инновационных решений в патентных базах данных Федеральной службы по интеллектуальной собственности, базах по патентам и товарным знакам Российской Федерации (Роспатент), Бюро по патентам и товарным знакам США [2], Европейского патентного бюро (EPO) [3, 4], Всемирной организации интеллектуальной собственности [5], и других источниках, содержащих патентную и инновационную информацию [6-8]. В частности, примерами, аналогами методов и технических решений среди инновационных подходов и патентов США могут служить свидетельства, выданные патентными бюро этой страны в области агрегации, нормализации, анализа и визуализации данных, мониторинга и управления безопасностью сетей [2]:

Многофункциональная система анализаторов угроз и способ ее использования. Способ определения уровня угрозы по выборке, включающий: предоставление массива с несколькими анализаторами, работающего на сервере, содержащего статический анализатор сигнатур, множество динамических анализаторов, арбитр, по меньшей мере, один процесс постобработки и процесс нормализации; анализ образца с помощью статического анализатора для проведения статического анализа; проверка статического анализа арбитром для определения того, какой из множества динамических анализаторов использовать для анализа образца; динамический анализ выборки одним из множества динамических анализаторов угроз (патент US 20180046799 A1, 2019 г.). Способ обнаружения угроз безопасности на основе указания в больших данных доступа ко вновь зарегистрированных доменам. Доменные имена определяются для каждого вычислительного события в наборе, каждое событие детализирует запросы или публикации веб-страниц. Определяется количество событий или обращений, связанных с каждым доменным именем в течение определенного периода времени (патент US 20130318603 A1, 2014 г.). Особого внимания в рамках разработки методов и устройств анализа эвристик трафика представляет способ обнаружения аномалий полнотекстового исполняемого кода. Обнаружение аномалий исполняемого кода включает в себя обнаружение активируемых пользователем элементов управления исполняемого кода, подлежащего тестированию, генерирование первого тестового кода на основе обнаруженных активируемых пользователем элементов управления и генерирование второго тестового кода на основе сценария для исполняемого кода, чтобы воспроизвести аномалию (патент US 20170206155 A1, 2019 г.).

Интересны некоторые методы и технические решения, зарегистрированные Европейским патентным бюро, например [3, 4]: Метод обнаружения аномалий сетевого трафика на основе алгоритма переменного направления множителей (патент CN107404471A, 2017 г.); Система обнаружения вторжений в реальном времени для платформы, применяющей большие данные. Система разделена на три уровня, а именно: уровень сбора информации, рабочий уровень и уровень отображения. Уровень сбора информации содержит модуль мониторинга и две сборки, которые находятся на связи друг с другом. Рабочий уровень содержит базовый модуль признаков, модуль анализа в реальном времени и модуль анализа тенденций. Слой отображения содержит модуль сигнализации и унифицированный модуль выписки. С помощью системы анализа вторжений в режиме реального времени обнаружение вторжений, мониторинг в реальном времени, активное обнаружение, активное управление защитой и связью осуществляются в режиме реального времени (патент CN103561018A, 2014 г.).

Отдельного внимания заслуживают отечественные инновационные решения в рамках разработки методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них [5-8]: Система и способ для обработки и анализа больших объемов данных (патент РФ № RU 2669716 C1, 2018 г.); Способ обнаружения сетевых атак на основе анализа временной структуры трафика (патент РФ № RU 2680756 C1, 2019 г.); Способ обнаружения аномалий в трафике магистральных сетей Интернет на основе мультифрактального эвристического анализа (патент РФ № RU 2696296 C1, 2018 г.).

Заключение. Таким образом, проведен анализ и сравнение современных инновационных решений по выявлению отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них. В качестве критериев для сравнения методов и технических решений учитывался комплекс характеристик эффективности как отдельных решений по сбору, предобработке, хранению, сигнатурному анализу, анализу на базе биоинспирированных подходов, машинному обучению и аналитическому моделированию, так и комплексных решений и тенденций по построению систем выявления отклонений в эвристиках трафика сверхвысоких объемов в целом. Использование результатов проведенного анализа позволит устранить неопределенность подходов к решению задач обнаружения сетевых атак и защиты от них, позволит, в конечном итоге, повысить правовую чистоту итогов научно-исследовательской работы, корректность и уникальность полученных результатов.

Исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

СПИСОК ЛИТЕРАТУРЫ

1. Патентный закон РФ // Электронный источник: http://www.legal-support.ru/information/laws/intellect/patent-law.html.
2. Бюро по патентам и товарным знакам США // Электронный источник: http://www.uspto.gov.
3. Европейское патентное бюро // Электронный источник: http://ep.espacenet. com/
4. European Patent Office // Электронный источник – https://ru.espacenet.com/?locale=ru_RU
5. Google. Поиск по патентам. https://www.google.com/?tbm=pts&gws_rd=ssl.
6. Методика патентного поиска: http://it4b.icsti.su/itb/ps/ps_all.html.
7. Государственная публичная научно-техническая библиотека России (ГПНТБ России): http://www.gpntb.ru/.
8. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам Российской Федерации // Электронный источник: http://www1.fips.ru.

УДК 025.2.004; 621.311.23: 629.12

К ВОПРОСУ ОЦЕНКИ КАЧЕСТВА ЛВС ОРГАНИЗАЦИИ

Гурьев Сергей Николаевич, Яковлев Андрей Анатольевич, Аксенов Сергей Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: sguryev@mail.ru, jaki@ru.ru

Аннотация. В работе сформулированы особенности оценки качества локальной вычислительной сети организации, представлены показатели качества. Сформулированы возможности повышения производительности ЛВС. Предлагаемый подход основан на том, что задача оценки качества всегда связана с определением показателей качества, выбор которых зависит от поставленных целей. Накопленный опыт исследований вычислительных систем, показывает, что из всех показателей качества в большинстве случаев основными являются показатели производительности и надежности.

Ключевые слова: качество, оценка, локальная вычислительная сеть, организация.

ON THE ISSUE OF EVALUATING THE QUALITY OF THE ORGANIZATION'S LAN

Guryev Sergey, Yakovlev Andrey, Aksenov Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: sguryev@mail.ru, jaki@ru.ru

Abstract. In this paper, the features of assessing the quality of the organization's local computer network are formulated, and quality indicators are presented. The possibilities of improving LAN performance are formulated. The proposed approach is based on the fact that the task of quality assessment is always associated with the definition of quality indicators, the choice of which depends on the goals set. The accumulated experience of computer systems research shows that performance and reliability indicators are the main indicators of all quality indicators in most cases.

Keywords: quality, evaluation, local computer network, organization.

Введение. В настоящее время экспертами и представителями бизнеса считается, что самым эффективным способом создания информационной среды является построение ЛВС организации. На данный момент наиболее востребованной технологией является Ethernet – технология передачи данных посредством кабеля, а также современные беспородные технологии (Wi-Fi, WiMAX). Единое информационное пространство организации необходимо для совместного использования разделяемых ресурсов, а также для успешного выполнения организацией своих основных функции.

ЛВС представляет собой вычислительную сеть, охватывающую небольшую территорию и использующая ориентированные на эту территорию средства и методы передачи данных. В обобщенной структуре ЛВС выделяют автоматизированные рабочие места, серверное оборудование и коммутационное оборудование. В зависимости от того, как ЛВС организована и как управляется ее можно отнести к локальной, городской, распределенной. Управляет ЛВС и ее сегментами – сетевой администратор [1].

Значительное увеличение масштабов внедрения ПЭВМ в ЛВС организации расширило области их применения, что привело к существенному росту ассигнований выделяемых на автоматизацию процессов управления в организации.

Основная доля этих ассигнований приходится на центральный элемент любой ЛВС – серверную (серверную группу). Поэтому вполне закономерным является стремление руководства организации минимизировать стоимость этих серверов, обеспечив при этом заданный уровень требований к ЛВС организации в целом. В тоже время, задача минимизации стоимости не может быть решена однозначно, ибо качество, а, следовательно, и стоимость вычислительных систем зависят от большого количества различных факторов. Для снижения степени риска от неверно принятых решений при создании (модернизации) ЛВС необходимо развивать методы их всестороннего исследования.

Среди задач исследования выделяют два класса, составляющих полную группу. Это задачи анализа и задачи синтеза. Постановка задачи анализа требует задания в качестве исходных данных структуры системы и характеристик ее элементов. Решение задачи состоит в нахождении характеристик исследуемой ЛВС организации [2].

Оценка качества ЛВС организации, как по структуре, так и по алгоритмам функционирования относится к сложным системам.

Задачи оценки качества отличаются высокими ресурсо и трудоемкостью.

Процесс исследования зачастую носит интерактивный характер и требует исследования как формальными, так и эвристическими методами решения.

Проведение исследований должны быть инициированы заинтересованной стороной – заказчиком. Только после этого к процессу оценки качества подключается исполнитель. В задачу заказчика входит подготовка задания на исследование, в задачу исполнителя – проведение собственно исследования. Задание на исследование оформляется заказчиком в виде постановки задачи, которая включает три основные составляющие:цель, условия, стратегию.

Главная цель оценки качества может состоять в определении способа создания (построения) или совершенствования ЛВС организации [6].

Задача оценки качества всегда связаны с определением и исследованием показателей качества, выбор которых зависит от поставленных целей. В состав этих показателей качества сети входят важные технические характеристики, которые могут быть оценены и выражены количественными значениями измеряемых или вычисляемых величин таких как: производительность, пропускная способность, надежность, достоверность информации, безопасность информации [3].

Накопленный опыт исследований вычислительных систем, показывает, что из всех показателей качества локальных вычислительных сетей в большинстве случаев основными являются показатели производительности и надежности.

Надежность ЛВС определяется следующими характеристиками: готовностью или коэффициентом готовности, который означает долю времени, в течении которого система может быть использована. Вероятностью доставки пакета узлу назначения без искажений (вероятность потери пакета, вероятность искажения отдельного бита передаваемых данных, отношение потерянных пакетов к доставленным) и другими.

Производительность ЛВС обеспечивает возможность распараллеливания работ (выполняемых процессов) между несколькими элементами сети. Для оценки производительности ЛВС применяют следующие характеристики: время реакции, пропускную способность, задержка передачи и вариация задержки передачи.

Действительно, уменьшение времени решения задачи имеет своим следствием уменьшение его отношения к средней наработке на отказ. В результате возрастает вероятность успешного, своевременного решения задачи. С другой стороны, большая производительность может быть допустить многократное решение задачи или ее части в случае возникновения сбоя, сохраняя при этом время получения результатов в заданных пределах. Кроме того, запас производительности позволяет повысить интенсивность проведения тестового контроля, тем самым увеличивая вероятность выявления потенциальных отказов.

Повышение производительности связано с уменьшением времени, требуемого на подготовительные операции, т.е. с повышением готовности ЛВС к выполнению поставленных задач. Производительность считается одним из важнейших показателей для оценки качества ЛВС организации. Производительность используется не только для оценки качества ЛВС организации, но и более частных процессов.

Производительность зависит от скорости передачи кадров по сети и скорости обработки этих кадров коммутационными устройствами, передающими кадры между своими портами. Скорость передачи кадров по сети зависит от используемых протоколов физического и канального уровней, а также применяемого коммутационного оборудования, позволяющего осуществлять параллельную обработку нескольких кадров. Современные коммутаторы имеют возможность предоставлять каждой станции или сегменту, подключенному к его портам, выделенную пропускную способность протокола [4,5].

Оценку производительности сети использующих случайный метод доступа к среде передачи осуществят как для реальных режимов работы сетей, так и для идеальных случаев — при отсутствии коллизий и при передаче непрерывного потока пакетов, разделенных только межпакетным интервалом.

Чтобы оценить основные параметры ЛВС, необходимо для начала на основе конкретной существующей ЛВС произвести аналитическое моделирование и дать оценку параметрам данной сети. Затем, повторить оценку тех же параметров на практике, работая с сетью, чтобы сравнить полученные результаты для доказательства адекватности математической модели.

Использование программного обеспечения для оценки качества сети позволит произвести ряд экспериментов, результатом которых будет возможно зафиксировать параметры локальной сети, например, такие как: реальная пропускная способность (скорость передачи трафика, в зависимости от загрузки сети), время передачи пакета по сети, время нахождения пакета в устройстве (задержка передачи), доля потерянных пакетов, время реакции и другие.

Заключение. Таким образом, решение задачи оценки качества ЛВС организации сводится к сбору исходных данных и обработке информации по производительности основных элементов сети и представление результатов решения в виде удобном для анализа и выработке решения руководством организации.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 24402-88 Телеобработка данных и вычислительные сети. Термины и определения.
2. Военно-технические основы построения и математическое моделирование перспективных средств и комплексов автоматизации. А.Ю. Иванов, С.П. Полковников, Г.Б. Ходасевич. – СПб.: ВАС, 1997г. – 419с.
3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.:, 2017 – 992с.
4. Олифер В.Г., Олифер Н.А. "Базовые технологии локальных сетей." [Электронный ресурс] СПб.: Питер, 2006г - Режим доступа: http://citforum.ru/nets/protocols2/index.shtml
5. Вычислительные системы, сети и телекоммуникации: учебник. В 2 ч. Ч. 2. Сети и телекоммуникации / В. П. Галас; Владимирский государственный университет А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2017. − 284 с.
6. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь.

УДК 004.942

РАССМОТРЕНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Дементьев Владислав Евгеньевич, Киреев Сергей Хаирбекович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: gamlet8806@rambler.ru, dem-vlad@rambler.ru

Аннотация. В статье рассматривается ряд методов обеспечения устойчивости информационно-телекоммуникационных сетей. Описаны основные вопросы при решении задач по обеспечению устойчивости информационно-телекоммуникационных сетей. Проанализирована практическая значимость методов в описанной области применения.

Ключевые слова: информационно-телекоммуникационная сеть; устойчивость; адаптивность; алгоритм; протокол; топология сети.

THE CONSIDERATION OF METHODS FOR ENSURING THE STABILITY OF INFORMATION TELECOMMUNICATION

Dementyev Vladislav, Kireev Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: gamlet8806@rambler.ru, dem-vlad@rambler.ru

Abstract. The article discusses a number of methods to ensure the stability of information telecommunication military networks. It describes the main issues in solving problems of ensuring the stability of information telecommunication. The features of each of the presented methods and their practical significance in the field of application are analyzed in this article.

Keywords: information telecommunication network; stability; adaptability; algorithm; protocol; network topology.

Введение. В условиях стремительной информатизации общества особую актуальность приобретает обеспечение устойчивости информационно-телекоммуникационных сетей (ИТКС). Под устойчивостью связи, согласно ГОСТ 5311-2008 [1], понимается способность системы связи (СС) выполнять свои функции при выходе из строя части ее элементов в результате воздействия деструктивных факторов (ДФ).

Далее рассмотрим некоторые методы обеспечения устойчивости ИТКС. Одним из решений является формирование резервных путей на основе алгоритма Дейкстры [2]. Анализ исследований в области устойчивости маршрутизации показал, что основным направлением модификации алгоритмов поиска кратчайших является совершенствование представления и формата исходных данных за счет учета в метрике ребер факторов определяющих те или иные свойства реальной сети.

Одним из методов обеспечения устойчивости ИТКС является адаптация параметров сигнализации в протоколе маршрутизации с установлением соединений при воздействии на сеть ДФ [3]. Решение задачи адаптации параметров сигнализации в протоколе маршрутизации с установлением соединений основано на использовании методов теории надежности и теории Марковских процессов.

Рассмотрим метод обеспечения устойчивости ИТКС за счет использования ее топологической избыточности [4]. В основу метода положено эффективное управление топологическим ресурсом сети, а именно – использование для маршрутизации трафика топологических структур с высокой избыточностью, а также маневра маршрутами передачи трафика в составе сети.

Рассмотрим обеспечение устойчивости ИТКС со стороны информационной безопасности. Для построения системы защиты от сетевых угроз предлагается использовать искусственные нейронные сети (ИНС), поскольку они имеют способность к самообучению на нормальном и анормальном сетевом трафике. ИНС могут участвовать в составлении профилей (осуществляя кластеризацию многомерных данных), анализировать весь сетевой трафик, контролировать последовательности вводимых пользователем команд, переходы состояний и пр. [5,6].

Заключение. Выполненный анализ методов обеспечения устойчивости информационно-телекоммуникационных сетей показал, что данные методы несут практическую значимость и их применение (возможно сочетания рассмотренных методов) целесообразно при решении задач по обеспечению устойчивости ИТКС.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 5311-2008, с. 2-7.
2. Цветков К.Ю., Макаренко С.И., Михайлов Р.Л. Формирование резервных путей на основе алгоритма Дейкстры, в целях повышения устойчивости информационно-телекоммуникационных сетей // Информационные каналы и среды. 2014, № 2. С. 72-83.
3. Макаренко С.И., Михайлов Р.Л. Адаптация параметров сигнализации в протоколе маршрутизации с установлением соединений при воздействии на сеть дестабилизирующих факторов // Системы управления, связи и безопасности. 2015, № 1. С. 98-138.
4. Макаренко С.И. Метод обеспечения устойчивости телекоммуникационной сети за счет использования ее топологической избыточности // Системы управления, связи и безопасности. 2018, № 3. С. 14-27.
5. Абрамов Н.С., Фраленко В.П. Нейросетевая система защиты информации вычислительных комплексов // Программные системы: теория и приложения. 2017 [Электронный ресурс]. URL:.http://psta.psiras.ru/read/psta2017 (дата обращения: 15.07.2020).
6. Михайличенко, Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных // Системы управления, связи и безопасности. 2019. № 1. С.54-66.

УДК 519.673

ПРОГНОЗИРОВАНИЕ РАБОЧИХ ХАРАКТЕРИСТИК РАДИОЛИНИЙ ДЛЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ КВ-ДИАПАЗОНА

Дорогов Александр Юрьевич
ПАО «Информационные телекоммуникационные технологии («Интелтех»)
Кантемировская ул., 8, Санкт-Петербург, 197342, Россия
e-mail: vaksa2006@yandex.ru

Аннотация. Рассмотрен моделирующий комплекс для радиосетей КВ-диапазона. Программная модель соответствует рекомендации МСЭ-R P.533-13 Международного Союза Электросвязи (ITU). Приведено описание моделей для режимов «Точка-точка» и «Зона». Комплекс позволяет прогнозировать характеристики радиолиний и зонового радио-покрытия в зависимости от географических координат, времени, месяца, солнечной активности и выбранных системных параметров.

Ключевые слова: ионосфера; радиолиния; радиозона; радиосеть; применимые частоты, отношение сигнал/шум.

PREDICTION OF RADIO CIRCUITS PERFORMANCE CHARACTERISTICS FOR HF DATA TRANSMISSION NETWORKS

Dorogov Alexandr
JSC «INTELTECH»
8 Kantemirovskay St, St. Petersburg, 197342, Russia
e-mail: vaksa2006@yandex.ru

Abstract. The modeling complex for HF-circuits is considered. The software model corespondes with ITU-R recommendation P. 533-13 of the International Telecommunication Union (ITU). The description of models the "Point-to-point" and "Zone"modes is given. The complex allows to predict the characteristics of radio circuits and zonal radio coverage depending on geographical coordinates, time, month, solar activity and selected system parameters.

Keywords: ionosphere; radio line; radiozone; radio network; applicable frequencies, signal-to-noise ratio.

Для КВ-диапазона определяющим фактором распространения радиоволн является наличие околоземной ионосферы. Структура и свойства ионосферы сильно изменяются с высотой. Процессы, протекающие в ионосфере тесно связаны с волновым и корпускулярным излучением Солнца, с процессами в магнитосфере и вариациями магнитного поля Земли, с движением верхней атмосферы и т.д. Этим обусловлена сильная изменчивость свойств ионосферы во времени (в зависимости от времени суток, времени года, циклов солнечной активности), а также в зависимости от высоты, географической широты и долготы.

Сложность и постоянная изменчивость структуры ионосферы, наличие множества факторов оказывающих влияние на распространения радиоволн в такой среде, сложная топология сетей связи приводят к необходимости компьютерного прогнозирования передачи данных в сетях КВ-диапазона.

Международным Союзом Электросвязи (ITU) разработана математическая модель для прогнозирования рабочих характеристик ВЧ-линий. Модель оформлена в виде рекомендации МСЭ-R P.533-13 (07/2015) [2] и программных средств на языке Fortran [3] для ОС Windows. Модель позволяет производить расчёт характеристик КВ-радиолиний с дистанцией до 9000 км (в режиме «Точка-точка») и радиозон покрытия (в режиме «Зона»). Программные средства доступны в виде исполняемых программ моделирующего комплекса и исходных кодов отдельных подпрограмм. В состав комплекса входит база данных антенн и редактор для изменения их характеристик.

Следует отметить, что исходные коды написаны на языке Fortran старой версии и поэтому требуют адаптации к современным компиляторам. В новом варианте программный и пользовательский интерфейсы были реализованы средствами программной среды Матлаб. Новый моделирующий комплекс использует структуру директориев исходного комплекса и полностью совместим с ним по форматам хранения данных.

Программная модель «точка-точка» предназначена для прогнозирования характеристик радиолинии между приёмником и передатчиком. Для сетевой поддержки реализован режим расчёта характеристик для набора радиолиний. Исходными данными программы являются: координаты размещения приёмника и передатчика; характеристики приёмной и передающей антенны; мощность передатчика; время (1-24 час); месяц (1-12); год; расчётные частоты (до 10); солнечная активность. Расчёт характеристик выполняется по всем частотам, по всем месяцам для каждого часа суток. Солнечная активность определяется числом солнечных пятен и устанавливается по номеру года из хранимого файла данных.

Программная модель «Зона» предназначена для прогнозирования распространения сигнала в радиозоне. Зона задается относительно выбранного центра зоны в градусах или в километрах по направлениям «на Восток», «на Запад», «на Север», «на Юг». Отдельно указывает место размещения передатчика, мощность передатчика и характеристики передающей антенны.

СПИСОК ЛИТЕРАТУРЫ

1. Побережский Е.С. Характеристики типичных коротковолновых трасс. Техника средств связи. Серия Техника радиосвязи 1978г. Выпуск 9. стр. 88-92.
2. Рекомендация МСЭ-R P.533-13 (07/2015) Метод для прогнозирования рабочих характеристик ВЧ-линий. Серия P. Распространение радиоволн.
3. Institute for Telecommunication Sciences / Resources / Radio Propagation Software / High Frequency / REC533 Propagation Model, https://www.its.bldrdoc.gov/resources.

УДК 355/359.07

ТРЕБОВАНИЯ К ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ ПЕРЕДАЧИ ДАННЫХ ПРИ ПРИМЕНЕНИИ СЕТЕОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ УСЛУГ

Емельянов Максим Владимирович, Ивлев Виктор Алексеевич, Лебедев Игорь Вячеславович, Сазонов Виктор Викторович

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: zawita@mail.ru, vmktor-sazonov@yandex.ru

Аннотация. На современном этапе актуально говорить о применении сетеориентированных информационных услуг в системах управления специального назначения для уменьшения времени на обработку и актуализацию информации необходимой должностному лицу органов управления для принятия решения. В тоже время их применение трактует необходимость определения требований к пропускной способности сети передачи данных специального назначения. Возможности по пропускной способности сети передачи данных специального назначения ограничены, как следствие этого накладываются ограничения на функционал сетеориентриванных информационных услуг. На основе анализа ограничений пропускной способности сети передачи данных специального назначения предложены рекомендации должностным лицам органов управления по использованию сетеориентированных информационных услуг.

Ключевые слова: сетецентризм, сетеориентированные информационные услуги, система управления специального назначения, сети передачи данных специального назначения, пропускная способность.

DATA NETWORK BANDWIDTH REQUIREMENTS FOR NETWORK ORIENTED INFORMATION SERVICES

Emelyanov Maksim, Ivlev Victor, Lebedev Igor, Sazonov Victor

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: zawita@mail.ru, vmktor-sazonov@yandex.ru

Abstract. At the present stage, it is relevant to talk about the use of networked information services in special-purpose management systems in order to reduce the time for processing and updating the information necessary for the official of the management bodies to make a decision. At the same time, their application interprets the need to determine the requirements for the bandwidth of a special-purpose data network. The capacity of a special purpose data network is limited, as a result of which restrictions are imposed on the functionality of network-oriented information services. Based on the analysis of the bandwidth limitations of the special purpose data network, recommendations are offered to officials of management bodies on the use of network-oriented information services.

Keywords: network centrism, network-oriented information services, special-purpose control system, special-purpose data transmission networks, bandwidth.

Введение. Достижения информационно-технической революции были использованы для создания высокоточного оружия, информационных систем и средств специального назначения, прорывных исследований в военной радиоэлектронике. Именно ее достижения являются той основой, на которой строится вся система вооружения современной армии. В центре понимания концепции сетецентрической войны находится информационное превосходство. Завоевание его одной из сторон ведет к значительному преимуществу. Информационное превосходство в контексте сетецентрического подхода означает способность иметь наиболее полную, правильно сформулированную информацию о противнике и возможном характере его действий. [1-3]

В целях сокращения времени на сбор, обобщение и обработку информации требуется обеспечить единое информационное взаимодействие пунктов управления, разнесенных на значительном удалении друг от друга. Решение данной задачи возможно с помощью создания единой информационной инфраструктуры на основе имеющейся телекоммуникационной сети (сети связи). В результате все пункты управления различного типа и предназначения, функциональные элементы, должностные лица и большое многообразие автоматизированных систем, будут объединены в полноценную информационную сеть и предоставлять услуги по сбору, хранению, распространению и управлению информацией в реальном масштабе времени [4].

С учетом особенностей использования сетеориентированных информационных услуг в системах управления специального назначения следует, что алгоритм обработки информации приобретает следующий вид: «актуализация информации» - «обработка информации» без учета требований к территориальному положению должностного лица в любое время по запросу с учетом наличия соответствующих прав [5].

Заключение. В статье рассматриваются актуальные проблемы совершенствования систем управления специального назначения, возникновение понятия сетецентризма и его развитие, реализация принципа сетецентризма с помощью применения сетеориентированных информационных услуг и особенности их применения в системах управления специального назначения на современном этапе.

СПИСОК ЛИТЕРАТУРЫ

1. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с.

2. Сетевая и сетецентричная война: определения, общие и отличительные черты. В.А. Нагорный В.И. Сальников
3. ГОСТ 7.0-99. Информационно-библиотечная деятельность, библиография. Термины и определения.
4. Трушин В.В. О сущности взаимодействия войск в операции (бою) / Военная мысль. - 2007. - № 4. - С. 16-18.
5. Легков К.Е. Применение сетеориентированных информационных услуг при проведении специальных операций / Сборник трудов военно-научной конференции ВКА им.А.Ф.Можайского. - 2013. - С.16-21.

УДК 004.052.32

ОЦЕНКА ТЕХНИЧЕСКОЙ ГОТОВНОСТИ СИСТЕМ ДОКУМЕНТАЛЬНОГО ОБМЕНА

Емельянов Максим Владимирович, Ивлев Виктор Алексеевич,
Кожевников Владимир Геннадьевич, Сазонов Виктор Викторович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: maxemelja@mail.ru, zawita@mail.ru, vla34912100@yandex.ru, vmktor-sazonov@yandex.ru

Аннотация. Известно, что оценка технической готовности систем документального обмена комплексов средств автоматизации специального назначения определяется коэффициентом исправности отдельных объектов и интегральным коэффициентом исправности систем документального обмена. Данные коэффициенты устанавливаются посредством анализа функционирования систем документального обмена в различных режимах эксплуатации, определяемые решаемыми специальными задачами.

Ключевые слова: техническая готовность комплексов средств автоматизации специального назначения, система характеристик технической готовности, методика расчетов коэффициентов технической готовности.

ASSESSMENT OF THE TECHNICAL READINESS OF DOCUMENT EXCHANGE SYSTEMS

Emelyanov Maksim, Ivlev Victor, Kozhevnikov Vladimir, Sazonov Victor
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: maxemelja@mail.ru, zawita@mail.ru, vla34912100@yandex.ru, vmktor-sazonov@yandex.ru

Abstract. It is known that the assessment of the technical readiness of document exchange systems for special-purpose automation systems is determined by the health factor of individual objects and the integral health factor of document exchange systems. These coefficients are established by analyzing the functioning of document exchange systems in various operating modes, determined by special tasks to be solved.

Keywords: technical readiness of complexes of automation equipment for special purposes, system of technical readiness characteristics, methodology for calculating technical readiness coefficients.

Введение. Для оценки эксплуатационно-технических характеристик продукции специального назначения существует довольно большое количество показателей. При этом, для определения оценки технической готовности систем документального обмена комплексов средств автоматизации специального назначения (далее – СДО КСА СН) следует использовать комплексный показатель, включающий в себя множество коэффициентов, в том числе коэффициент технической готовности [1].

Техническая готовность СДО КСА СН на этапе эксплуатации определяется системой характеристик, а именно: коэффициентом исправности отдельных объектов СДО КСА СН и интегральным коэффициентом исправности СДО КСА СН (в целом) [2].

Исходными данными для оценки показателей исправности являются журналы дежурных смен, обслуживающих СДО КСА СН, где зафиксированы и нужным образом классифицированы критические (то есть приводящие к переходу технических и программных средств в неработоспособное состояние) состояния, а также время, потребовавшееся для их устранения. Необходимость расчета данной характеристики вызвана тем, что отказ одного или более КСА СН не приводит к прекращению функционирования системы документального обмена, а всего лишь снижает характеристики оперативности доведения сообщений и связность объектов.

Исходными данными для вычисления интегрального коэффициента исправности будут являться значения коэффициентов исправности и значимости каждого из объектов, полученные с использованием методики расчета коэффициента исправности СДО КСА СН, а также сведения по абонентской емкости объектов (числа абонентов, которые обслуживаются данным КСА СН). Исходя из вышесказанного, оценивая техническую готовность СДО КСА СН, необходимо учитывать совокупность технических, программных и эксплуатационных факторов, влияющих на ее работоспособность и, как следствие, рассчитывать и принимать во внимание выше обозначенные коэффициенты, влияющие на общую оценку.

Необходимо помнить, что техническая готовность - это величина, изменяющаяся во времени, учитывая которую и выполняя необходимый перечень мероприятий по поддержанию ее в заданных условиях, а также повышению ее коэффициента – мы получим надежную, отказоустойчивую, своевременную и достоверную СДО КСА СН для решения задач по предназначению [3-5].

Заключение. В докладе рассматривается вариант оценки технической готовности СДО КСА СН, при различных коэффициентах значимости (выбранного исходя из принятых приоритетов информационного обмена) и исправности (выбранного исходя из условий эксплуатации).

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34003-90. Автоматизированные системы. Термины и определения.
2. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Уч. пособие. СПб.: ВАС, 2015. 304с. [2, с.57-93].
3. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые информационные технологии в системах управления военного назначения. Учебник/Под редакцией И.Б. Саенко. СПб.: ВАС, 2010. -520с. [4, с.16-36].
4. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи: монография / В. Г. Иванов. – СПб: ПОЛИТЕХ-ПРЕСС, 2018. – 214 с.
5. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. - Финансы и статистика, Инфра-М, 2008.

УДК 004.942

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРИМЕНЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Емельянов Максим Владимирович, Ивлев Виктор Алексеевич, Хмелевской Валерий Павлович, Кожевников Владимир Геннадьевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного

Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

e-mails: maxemelja@mail.ru, zawita@mail.ru, h02v08p@rambler.ru,vla34912100@yandex.ru

Аннотация. Известно, что основу применения сложных систем специального назначения составляет тщательное прогнозирование и планирование действий по развертыванию и эксплуатационному обслуживанию элементов и подсистем, которое, в свою очередь, включает в себя ряд этапов деятельности должностных лиц, направленных на выработку наиболее рационального решения, реализующего целевое предназначение по выполнению поставленных задач обеспечения эффективного управления подчиненными объектами.

Ключевые слова: структура системы связи специального назначения, функциональный подход, структурный подход.

METHODOLOGICAL FOUNDATIONS OF THE USE OF TELECOMMUNICATION NETWORKS

Emelyanov Maksim, Ivlev Victor, Hmelevskoy Valeriy, Kozhevnikov Vladimir

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: maxemelja@mail.ru, zawita@mail.ru, h02v08p@rambler.ru,vla34912100@yandex.ru

Abstract. It is known that the basis for the use of complex special-purpose systems is careful forecasting and planning of actions for the deployment and operational maintenance of elements and subsystems. Which in turn Includes a number of officials aimed at developing the most rational solution that realizes the intended purpose for fulfilling the intended purpose tasks of ensuring effective management of subordinate objects.

Keywords: structure of a special-purpose communication system, functional approach, structural approach.

Введение. Любая сложная организационно-техническая система, характеризующаяся большим количеством взаимосвязанных и взаимодействующих элементов, сложностью выполняемых функций направленных на достижение заданной цели функционирования, возможностью ее разбиения на подсистемы, цели функционирования которых подчинены общей цели, наличием управления, разветвленной информационной сетью интенсивных потоков информации, взаимодействием с внешней средой, требует наличия различных ресурсов, персонала и функционирует в определенных условиях окружающей среды. В ходе функционирования (применения по назначению специальных систем) система осуществляет обмен, в результате которого за приобретаемую для потребляющей системы пользу (полезный или целевой эффект) расплачивается некоторым количеством ресурсов, персонала, особенно в условиях агрессивного воздействия окружающей среды [1-3].

Под применением сложных систем связи специального назначения понимается организованное использование сил и средств для выполнения поставленных задач по обеспечению управления подчиненными объектами.

Рассмотрим основные понятия системного подхода к построению сложных систем связи специального назначения. Под "системой" в данном случае понимается "целое", состоящее из объектов, взаимосвязь и взаимодействие которых порождают новые (системные) качества, не присущие никакому объекту в отдельности, ни их арифметической сумме. Объекты, входящие в систему, называются элементами системы (если в дальнейшем они рассматриваются как неделимые части) или подсистемами (если в дальнейшем сами рассматриваются как системы). В общем случае системы специального назначения можно рассматривать с точки зрения структурного и функционального предназначения.

Под структурой системы связи специального назначения понимается строение, устройство системы, определяемое составом основных подсистем и элементов связи, их взаимосвязью и взаиморасположением. Предназначение системы заключается в эффективной реализации или процесса, в интересах которого создается система связи специального назначения.

Функционирование системы и ее элементов (подсистем) тесно взаимосвязаны, нет структур без функций, как и функций без структур. Когда изучаются структура и функции системы в их единстве, то реализуется структурно-

функциональный подход. Однако на практике иногда приходится изучать сначала только функции или структуры системы. Первый подход получил название функционального (процессорного), а второй − структурного подхода.

Функциональный подход рассматривает виды работ, последовательность их выполняется в системы для достижения желаемого результата по развертыванию системы (подсистемы). При этом учитывается динамика развития (перестроения) систем связи специального назначения в ходе подготовки и проведения особо важных мероприятий [4].

Структурный подход рассматривает состав системы, подсистемы и их взаимосвязи, описывается статика системы специального назначения.

Первый подход более пригоден при конструировании, создании новых систем. В этом случае сначала определяют функции и процессы, которые надо выполнять, а затем подбирают структуры, способные это обеспечить. Структурный подход более применим при рассмотрении анализа и изучении действующих систем. Здесь проще начинать с выявления подсистем или элементов, а затем определить процессы и их взаимосвязи.

Основными частями системы при функциональном подходе будут являться исходные данные, процесс применения и его конечная цель − обеспечение специальными объектами. При этом процесс функционирования системы должен обязательно рассматриваться во взаимодействии с внешней средой. Во взаимодействии с внешней средой система выступает как нечто единое, целое, ввиду того, что связи подсистем (элементов) данной системы значительно устойчивее, чем связи этой системы или ее отдельных подсистем (элементов) с внешней средой.

Основными частями системы при структурном подходе являются подсистемы (элементы) и связи между ними.

Состояние системы − понятие, характеризующее систему в данный момент. Оно может быть описано совокупностью качественных или количественных характеристик.

Для изучения применения систем специального назначения и улучшения их характеристик используются методы анализа и синтеза этих систем. Анализ системы предусматривает декомпозицию или разбиение ее на подсистемы 1, 2, n-го порядка. В процессе анализа применения систем при структурном подходе выделяются подсистемы разных уровней (экипажи, команды) и определяются какие подсистемы данного уровня и их совокупности образуют систему более высокого порядка.

В результате анализа системы при структурном подходе получается более или менее декомпозированная структура системы, способная выполнять поставленные задачи по обеспечению управления специальными объектами.

Учет основных внешних влияющих факторов и возможность анализа базовых структур применения сложных систем специального назначения дают возможность синтезировать новую систему с лучшими показателями.

Следовательно, такой интегральный подход характеризует те механизмы, которые обеспечивают целостность системы, объединяют отдельные подпроцессы в системы процессов, отдельные элементы и подсистемы в развертываемые структуры. Кроме того, системы должны включать в себя материальные и другие ресурсы, объединенные в единое целое для выполнения заданной целевой функции по выполнению поставленных задач.

Первоочередной функцией применения систем специального назначения является прогнозирование и планирование, так как она в той или иной степени поглощает все остальные функции, которые также реализуются в виде планов. Следовательно, планирование является основополагающей функцией применения систем специального назначения, так как определяет цели функционирования системы и способы их достижения. Начальной стадией планирования является прогнозирование, сущность которого состоит в научно обоснованном предвидении развития системы и динамики воздействия внешних влияющих факторов. Прогнозы носят вероятностный характер. Они, в отличие от планов, не строго детерминированы и не являются директивными. Однако, сформированные на основе современных научных методов прогнозы являются достаточно надежной базой планирования [3-6].

Таким образом, основу применения сложных систем специального назначения составляет тщательное прогнозирование и планирование действий по развертыванию и эксплуатационному обслуживанию ее элементов и подсистем, которое, в свою очередь, включает в себя ряд этапов деятельности должностных лиц, направленных на выработку наиболее рационального решения, реализующего целевое предназначение по выполнению поставленных задач обеспечения эффективного управления подчиненными объектами.

Заключение. В докладе рассматриваются подходы и этапы применения сложных систем специального назначения, которые носят циклический характер и могут составлять единый цикл на выполнение важных операций. При планировании применения на последующие операции или при резком изменении условий обстановки и последующем решении вышестоящего руководства, весь цикл выполнения работ по применению повторяется в соответствии с изменившимися внешними влияющими факторами.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34003-90. Автоматизированные системы. Термины и определения.
2. Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Уч. пособие. СПб.: ВАС, 2015. 304с. [2, с.57-93].
3. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые информационные технологии в системах управления военного назначения. Учебник/Под редакцией И.Б. Саенко. СПб.: ВАС, 2010. -520с. [4, с.16-36].
4. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи: монография / В. Г. Иванов. – СПб: ПОЛИТЕХ-ПРЕСС, 2018. – 214 с.
5. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации. - Финансы и статистика, Инфра-М, 2008.
6. Михайличенко, Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных // Системы управления, связи и безопасности. 2019. № 1. С.54-66.

УДК 004.942

ПЕРЕНОС ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОТЕЧЕСТВЕННУЮ АППАРАТНО-ПРОГРАММНУЮ ПЛАТФОРМУ

Зибров Иван Александрович, Кий Андрей Вячеславович, Аксенов Сергей Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: zibrovivan@mail.ru, kiyarmy@rambler.ru

Аннотация. В статье рассматривается вариант переноса программного обеспечения на отечественную аппаратно-программную платформу. Описаны основные проблемы при переносе прикладного программного обеспечения на новую аппаратно-программную платформу. Проанализированы особенности аппаратно-программной платформы как среды переноса программного обеспечения, в результате чего предложен перечень возможных методов портирования.

Ключевые слова: программное обеспечение; импортозамещение; операционная система; дистрибутив.

TRANSFER TO DOMESTIC HARDWARE AND SOFTWARE PLATFORM

Zibrov Ivan, Kij Andrej, Aksenov Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: zibrovivan@mail.ru, kiyarmy@rambler.ru

Abstract. The possibility of replacing foreign-made programs with Russian ones registered in the Unified register of Russian programs is considered. It is noted that when switching to Russian software, problems arise due to the lack of standardization of the main binary interfaces and commands of various distributions. A list of possible porting methods is proposed.

Keywords: software; import substitution; operating system; distribution.

Введение. В связи с развёрнутой в России политикой импортозамещения, коснувшейся и сферы информационных технологий, обозначен ряд проблем, которые необходимо решить в ближайшем будущем. Необходимо провести анализ существующих прикладных систем на предмет совместимости с выбранными импортонезависимыми операционными системами (ОС), общесистемными сервисами (такими, как служба каталогов и система защиты информации от НСД и др.), системой управления базами данных и другими базовыми технологиями. Для приложений, которые сами на ОС не запускаются, необходимо сделать выбор, обоснование и реализацию механизмов работы таких прикладных систем. К числу основных механизмов такого рода относятся: эмуляция, виртуализация различных типов (локальная, удаленная, контейнерная), терминальный доступ и др.[1].

Исходными данными для работ по подготовке процесса являются: старая (исходная) базовая версия программного продукта; системные документы; предложения о модификациях и отчеты о дефектах. Для обеспечения эффективной реализации процесса сопровождения сопроводителю следует разработать и документально оформить стратегию проведения сопровождения, один из ключевых факторов в применении и развитии программных средств [2].

При реализации этой деятельности сопроводитель должен: разработать планы и процедуры сопровождения; установить процедуры рассмотрения предложений о модификации и отчетов о дефектах; применить управление конфигурацией.

До осуществления переноса (внесения изменений в систему и программные средства) сопроводитель должен: проанализировать возможные изменения с точки зрения их влияния на деятельность организации, существующую систему и взаимосвязанные с ней системы; разработать и документально оформить рекомендуемые альтернативные решения по внесению корректировок и согласовать принятое решение по внесению изменений с заказчиком.

Для плавного перехода к новой базовой версии программного продукта должна быть обеспечена параллельная эксплуатация прежнего и нового программных продуктов. Всё, связанное с прежней версией программного средства: документы разработки, журналы регистрации и программы должно быть помещено в архивы. Данные, использованные или связанные со снятым с эксплуатации программным продуктом, следует сохранять доступными для аудиторской проверки [3].

Заключение. В целом, для качественного решения задачи, переноса ППО на отечественную АПП должен опираться на требования государственных и международных стандартов в области автоматизированных систем и жизненного цикла программных средств, при этом особое внимание необходимо уделять предварительному анализу условий переноса, учету наиболее значимых факторов, влияющих на результаты переноса и оценке качества ППО после завершения переноса на новую АПП, что позволит учесть риски переноса и избежать неэффективных материальных и временных затрат.

СПИСОК ЛИТЕРАТУРЫ

1. Написание переносимых программ [Электронный ресурс]. URL: http://givi.olnd.ru/wclr/15_portable.html (дата обращения 02.10.2019г.)
2. ГОСТ Р ISO/МЭК 14764 – 2002. Информационная технология. Сопровождение программных средств. Госстандарт России. Москва. 2002. -32 с.
3. ГОСТ Р ISO/МЭК 12207 – 2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. Москва. Стандартинформ - 2011. -105 с.

УДК 621.391 (075.8)

МЕХАНИЗМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К ДАННЫМ В СУБД В СРЕДЕ ОПЕРАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SE

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио» (Филиал ФГУП НИИР-ЛОНИИР)
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Проведен анализ механизмов разграничения доступа, реализованных в защищенной СУБД PostgreSQL в среде операционной системы специального назначения «Astra Linux SE». Рассмотрены средства управления мандатными и дискреционными правами разграничения доступа в СУБД PostgreSQL. Проанализированы аспекты администрирования баз данных в операционной системы специального назначения «Astra Linux SE».

Ключевые слова: операционная система специального назначения, система управления базами данных, мандатная модель разграничения доступа, дискреционная модель разграничения доступа.

MECHANISMS OF DIFFERENTIATION OF ACCESS IN DBMS IN OPERATING SYSTEM OF A SPECIAL PURPOSE «ASTRA LINUX SE»

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr[2]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] Radio Research & Development Institute «Leningrad Branch of Radio Research & Development Institute» (Branch NIIR-LONIIR)
4 Bolshoi Smolenskiy Av, St. Petersburg, 192029, Russia
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The analysis of access control mechanisms implemented in the DBMS PostgreSQL in operating system of a special purpose «Astra Linux SE» is carried out. The tools for mandatory credential and discretionary rights of access control in the PostgreSQL are considered. The aspects of database administration in operating system of a special purpose «Astra Linux SE» are analyzed.

Keywords: operating system of a special purpose, database management system, mandatory model of differentiation of access, discretionary model of differentiation of access.

Введение. Система управления базами данных (СУБД) PostgreSQL предназначена для создания и управления реляционными базами данных (БД) и предоставляет многопользовательский доступ к расположенным в них данным. В качестве защищенной СУБД в составе операционной системы специального назначения (ОС СН) «Astra Linux SE Смоленск 1.6» используется СУБД PostgreSQL версии 9.6, доработанная в соответствии с требованием интеграции с ОС СН в части мандатного управления доступом к информации. СУБД содержит реализацию мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками [1]. Данная ДП-модель содержит все аспекты дискреционного, мандатного и ролевого управления доступом с учетом безопасности информационных потоков.

СУБД PostgreSQL обеспечивает поддержку модуля безопасности PARSEC ОС СН «Astra Linux SE», который реализует разграничение доступа на основе дискреционной и мандатной политик разграничения доступа [2,3]. Благодаря такой поддержке в рамках инфологической и физической моделей данных возможно разграничение доступа на уровне как схемы данных, так и таблиц базы данных (включая отдельные записи или группы записей), а также SQL-функций обработки этих записей.

Поддержка дискреционного разграничения доступа осуществляется для следующих объектов БД: схемы, таблицы, столбцы и функции. Мандатное разграничение доступа поддерживается для схем, таблиц, записей и функций.

В основе мандатного разграничения доступа лежит управление доступом к защищенным ресурсам БД на основе иерархических и неиерархических меток доступа [4,5]. Это позволяет реализовать многоуровневую защиту с обеспечением разграничения доступа пользователей к защищаемым ресурсам БД и управление потоками информации. В качестве иерархических и неиерархических меток доступа при использовании СУБД в ОС СН «Astra Linux SE» используются метки конфиденциальности или метки безопасности ОС СН. СУБД PostgreSQL не имеет собственного механизма назначения, хранения и модификации меток пользователей и использует для этого механизмы ОС СН. Кроме того, дополнительно к мандатной метке конфиденциальности вводится понятие объектов-контейнеров (объектов, которые могут содержать другие объекты). Для задания способа доступа к объектам внутри контейнеров используется мандатный признак CCR (Conteiner Clearance Required). В случае, когда он установлен, доступ к контейнеру и его содержимому определяется его мандатной меткой конфиденциальности, в противном случае доступ к содержимому разрешен без учета уровня конфиденциальности контейнера. Также накладывается ограничения на мандатную метку конфиденциальности

объекта: метка объекта не может превышать метку контейнера, в котором он содержится. Таким образом, для назначения меток данных сначала должны быть заданы максимальные метки соответствующих объектов, например, таблицы, схемы, табличного пространства и БД.

В качестве главного контейнера выбрано табличное пространство pg_global, которое создается одно на кластер БД. Таким образом, кластер является совокупностью ролей, БД и табличных пространств.

Применение мандатных прав доступа осуществляется на уровне доступа к объектам БД и на уровне доступа непосредственно к данным (на уровне записей).

Проверка мандатных прав доступа к объектам осуществляется одновременно с проверкой дискреционных прав доступа к ним, после разбора и построения плана запроса, непосредственно перед его выполнением, когда определены все необходимые для проверки данные и проверяемые объекты. Таким образом, доступ предоставляется только при одновременном санкционировании его дискреционными правами разграничения доступа (ПРД).

Проверка мандатных прав доступа к записям таблиц осуществляется в процессе выполнения запроса при последовательном или индексном сканировании данных.

Для администратора БД предусмотрены системные привилегии игнорирования мандатного управления доступом. Только таким образом можно производить регламентные работы с БД (например, восстановление резервной копии), т.к. это требует установки меток данных, сохраненных ранее.

Для управления дискреционными и мандатными ПРД в ОС СН «Astra Linux SE» используются следующие графические утилиты:

– pgAdmin3 («Средство администрирования СУБД PostgreSQL»);
– fly-admin-smc («Управление политикой безопасности») – управление протоколированием, привилегиями и мандатными атрибутами пользователей, работа с пользователями и группами.

Для управления мандатными ПРД в режиме командной строки используются следующие утилиты:

– pdp-ulbls – управление допустимыми мандатными уровнями и категориями пользователей ОС СН;
– userlev – изменение БД мандатных уровней;
– usercat – изменение БД мандатных категорий.

Для управления дискреционными правами в режиме командной строки используются утилиты:

– chown – изменение владельца и/или группы согласно заданным атрибутам;
– chmod – изменение прав доступа указанного объекта.

Администрирование БД в СУБД PostgreSQL является достаточно ресурсоемким. Так для назначения мандатных меток объектам СУБД PostgreSQL необходимо запустить утилиту «pgAdmin3», а для назначения мандатных атрибутов субъектам (пользователям) необходимо запустить «fly-admin-smc». При этом в случае необходимости более детальной настройки политики разграничения доступа или проверки корректности работы СУБД необходимо запустить утилиту «psql» - интерактивный терминал PostgreSQL. В результате, администратор обеспечения безопасности информации имеет высокую вероятность совершения ошибки.

Кроме того, требуется многократное повторения рутинных операций, таких как:

– назначение мандатных атрибутов пользователю;
– назначение мандатных меток каждому объекту СУБД, к которому имеет доступ пользователь (БД, таблицам, записям в таблицах, столбцам в таблицах, каждой ячейке таблицы);
– настройка доступа пользователя ко всем объектам СУБД.

Заключение. Защищенная СУБД PostgreSQL в среде ОС СН «Astra Linux SE» реализует все аспекты дискреционного и мандатного управления доступом с учетом безопасности информационных потоков. В СУБД возможно разграничение доступа на уровне как схемы данных, так и таблиц базы данных (включая отдельные записи или группы записей), а также SQL-функций обработки этих записей. Решением проблем администрирования БД является разработка нового программного обеспечения, которое позволит объединить функциональные возможности таких утилит, как «pgAdmin3», «fly-admin-smc» и «psql» при назначении мандатных и дискреционных атрибутов объектам и субъектам СУБД PostgreSQL в составе ОС СН «Astra Linux SE».

СПИСОК ЛИТЕРАТУРЫ

1. П.В. Буренин, П.Н. Девянин и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие. Под редакцией доктора технических наук П.Н. Девянина. М.: Горячая линия – Телеком, 2018. 311 с.
2. Гринь Д.В., Ильина О.Б., Купчиненко О.П., Скоропад А.В.. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: Сб. тр. СПб.: СПОИСУ, 2017. Вып.4. С. 76-78.
3. Ильина О.Б., Купчиненко О.П., Скоропад А.В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. / Под ред. С.В. Бачевского. СПб.: СПбГУТ, 2018. Т.2. С 356-360.
4. Михайличенко, Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных // Системы управления, связи и безопасности. 2019. № 1. С.54-66.
5. Маликов, А.В., Авраменко, В.С., Саенко, И.Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы, 2019, № 6. С.32–42.

УДК 004.3

АНАЛИЗ СОДЕРЖАНИЯ МЕРОПРИЯТИЙ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ АСУ

Ковбасюк Александр Васильевич, Логинов Вячеслав Алексеевич, Масалов Александр Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: rcpus1@mail.ru, loginov64@rambler.ru, masalov.84@mail.ru

Аннотация. Проведен анализ содержания мероприятий технического обеспечения автоматизированных систем управления. Техническое обеспечение осуществляется в целях поддержания автоматизированной системы управления в исправном состоянии. Требования к техническому обеспечению должны гарантировать, что при их выполнении будет полностью обеспечиваться заданная эффективность реализации других видов обеспечения и автоматизированной системе в целом.

Ключевые слова: техническое обеспечение; автоматизированные системы управления; средства автоматизации.

ANALYSIS OF THE CONTENT OF TECHNICAL SUPPORT MEASURES FOR AUTOMATED CONTROL SYSTEMS

Kovbasuk Alexandr, Loginov Vyacheslav, Masalov Alexandr
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: rcpus1@mail.ru, loginov64@rambler.ru, masalov.84@mail.ru

Abstract. The analysis of the content of technical support measures for automated control systems is carried out. Technical support of automated control systems is carried out in order to maintain them in good condition. Requirements for technical support should ensure that their implementation will fully ensure the specified efficiency of implementation of other types of software and the automated system as a whole.

Keywords: technical support; automated control system; automation tool.

Введение. Система, автоматизирующая процессы или функции управления называется автоматизированной системой управления (АСУ). Назначение конкретной автоматизированной системы определяется в зависимости от автоматизируемых процессов и функций органа управления, в интересах которого создается такая система, ее функционального предназначения, а также от характера объекта управления.

Любое управления, как правило, реализует следующие информационные процессы:

- сбор и регистрация;
- обработка;
- хранение;
- передача информации и др.

Для реализации каждого такого процесса используется необходимый состав специальных технически средств, входящий в состав технического обеспечения (ТО).

Техническое обеспечение (ТО) - комплекс технических средств, применяемых для функционирования автоматизированной системы управления (ГОСТ 24003-84). Комплекс технических средств предназначен для автоматизированной реализации информационного процесса.

Техническое обеспечение связи и АСУ осуществляется в целях поддержания их в исправном состоянии. В состав технического обеспечения входит: своевременное снабжение средствами и оборудованием, эксплуатационно-расходными материалами, восстановление их расхода и потерь, содержание техники и ЗИП в комплекте и в исправности; проведение регламентов, обслуживание и контроль состояния техники в установленные сроки; организацию эксплуатации и ремонта поврежденной (неисправной) техники; организацию управления силами и средствами технического обеспечения.

В состав ТО входит также различное оборудование, обеспечивающее функционирование технических средств в составе АСУ в соответствии с их предназначением.

Выбор технических средств определяется сложностью задач, решаемых системой управления, содержанием информационного процесса, требованиями к организации информационного процесса.

Комплекс технических средств как материальная основа автоматизации является наименее гибким видом обеспечения. Поэтому при создании средств ТО главными задачами являются: выбор целесообразного состава технических средств; обеспечение взаимодействия различных технических средств; организация эффективного использования технических средств.

При выборе технических средств необходимо учитывать следующие принципы применения оборудования: соответствия производительности технических средств комплекса автоматизации решаемым на нем задачам (в противном случае эффективность использования комплекса и АСУ, в целом, может снизиться); совместимости технических средств; агрегируемости технических средств (возможности создания комплексов из различных компонентов); максимального использования производительности каждого технического средства.

Первичность предназначения АСУ и состава других видов обеспечения по отношению к техническим средствам можно показать на примере рассмотрения требуемых свойств базового вычислительного комплекса в случае применения его в трех различных по назначению системах:

– в системе (подсистеме) сбора, хранения и передачи командной информации требуются расширенные средства каналов обмена, аппаратная поддержка безопасности и отказоустойчивости;

– в информационно-расчетной системе (подсистеме) - расширенные средства работы с внешними средствами хранения информации, возможность применения специализированных процессоров для работы с базами данных;

– в системе сбора и обработки информации - расширенные средства специализированной обработки, увеличенные ресурсы памяти.

Приведенные принципы позволяют сформулировать возможный порядок обоснования требований к ТО, согласованный с методиками выполнения подобных работ для других видов обеспечения.

Во-первых, проведение информационного обследования органа управления, подлежащего автоматизации, включающего определение:

– основных задач, решаемых в ходе функционирования системы;

– характера решаемых задач;

– определение текущего уровня применения средств автоматизации;

– характеристики связей взаимодействия;

– характеристик (периодичность, формы, объём) внутренних, входных и выходных документов;

– применяемых и перспективных средств общего и специального математического, а также информационного обеспечения;

– требований к отдельным подсистемам с обоснованными показателями;

– концептуальных моделей основных информационных процессов.

В результате выполнения указанных пунктов осуществляется обоснование средств технического обеспечения, состав показателей, эффективность АСУ в целом, (производительность, надежность, пропускные способности каналов обмена или номенклатура оборудования).

Во-вторых, построение на основе анализа перспективных разработок и знаний возможностей производства усеченного дерева вариантов структур технических средств АСУ.

В-третьих, обоснованный выбор основных качественных и количественных показателей, характеризующих эффективность (качество) технических средств.

В-четвертых, определение требований к показателям эффективности исходя из назначения и задач, решаемых системой.

В-пятых, разработка (на базе модели основных информационных процессов) математических моделей, связывающих структуру системы для каждого из выбранных вариантов с основными и частными техническими показателями эффективности.

В-шестых, выполнение экспертной оценки дерева перебора одним из выбранных методов.

Для повышения качества обеспечения технического обеспечения системы выполнить тестирование прототипов комплексов технических средств с использованием инструментальных тестовых пакетов и макетов, предлагаемых к применению информационных и расчетных задач.

При формировании требований к техническим средствам должны быть определены режимы их функционирования и использования (например, многозадачность и однопользовательность).

Основные требования к техническому обеспечению со стороны других видов обеспечения сводятся к ресурсам производительности, памяти, системы ввода-вывода и периферийных устройств.

Технические средства современных автоматизированных систем управления представлены прежде всего управляющими системами, состоящими из совокупности вычислительных комплексов повышенной надежности, пультов управления и периферийных приборов, связанных в единое целое посредством каналов ввода-вывода.

Требования к техническому обеспечению должны гарантировать, что при их выполнении будет полностью обеспечиваться заданная эффективность реализации других видов обеспечения и автоматизированной системе в целом. К основным группам требований, предъявляемых к техническому обеспечению, можно отнести следующие:

– наличие достаточного уровня ресурсов производительности, основной и внешней памяти;

– необходимые номенклатура и качество периферийных средств.

Опыт создания систем автоматизации позволяет сформировать ряд принципов разработки технического обеспечения АСУ.

Заключение. Требования к техническим средствам уточняются по мере перехода от замысла на систему до конечного предъявления технического задания на нее. Приведенные принципы позволяют сформулировать возможный порядок обоснования требований к техническому обеспечению, согласованный с методиками выполнения работ для других видов обеспечения. Перспективными направлениями в развитии технических средств автоматизации управления являются дальнейшая их интеграция со средствами телекоммуникации в составе единых подсистем и обеспечение

СПИСОК ЛИТЕРАТУРЫ

1. Чихачев А.В., Третьяков С.М., Бурлаков А.А. и др. Техническое обеспечение связи и автоматизации. Учебник. – СПб.: ВАС, 2017. 152 - 302 стр.
2. ГОСТ 24.003-84 «Единая система стандартов автоматизированных систем управления».
3. В.Ф. Шпак Основы автоматизации управления. Ч.1, стр. 126-145. Петродворец, ВМИРЭ, 1998 г.
4. Н.Ф. Директоров и др. Автоматизация управления и связь в ВМФ. С. 114-118. СПб. Элмор, 2001.г.
5. С.М. Доценко и др. Единое информационно-функциональное пространство ВМФ: от идеи до реализации. Стр. 221-268. СПб., НИКА, 2003 г.

УДК 025.2.004; 621.311.23: 629.12

МОНИТОРИНГ ЭЛЕКТРОННЫХ БИБЛИОТЕК: БАЗОВЫЕ ПОНЯТИЯ, ЦЕЛИ, ПРИНЦИПЫ И НАПРАВЛЕНИЯ РАЗВИТИЯ

Крюкова Елена Сергеевна, Михайличенко Николай Валерьевич, Паращук Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mails: e.kkrukovaa69@yandex.ru, 23esn2008@rambler.ru, shchuk@rambler.ru

Аннотация. Рассмотрены особенности и перспективы построения электронных библиотек, предпринята попытка сформулировать ключевые концептуальные основы оптимального адаптивного мониторинга их состояния (качества). Сформулирована сущность и введены квалиметрические понятия мониторинга электронных библиотек, описаны этапы концептуальной модели оптимального адаптивного мониторинга объектов такого класса, рассмотрены цели и задачи мониторинга. Предложен комплекс принципов оптимального адаптивного мониторинга электронных библиотек, что создает предпосылки для синтеза алгоритмов оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния (качества) таких систем в целях снижения затрат ресурсов системы управления, повышения оперативности и достоверности (точности) принятия решений по управлению электронными библиотеками в различных условиях обстановки.

Ключевые слова: электронная библиотека, мониторинг, состояние, качество, анализ, наблюдение, оценивание, прогнозирование.

MONITORING OF ELECTRONIC LIBRARIES: BASIC CONCEPTS, GOALS, PRINCIPLES AND DIRECTIONS OF DEVELOPMENT

Kryukova Elena, Mikhaylichenko Nikolay, Parashchuk Igor
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mails: e.kkrukovaa69@yandex.ru, 23esn2008@rambler.ru, shchuk@rambler.ru

Abstract. The features and prospects of building electronic libraries are examined, an attempt is made to formulate the key conceptual foundations of optimal adaptive monitoring of their condition (quality). The essence is formulated and qualimetric concepts of monitoring electronic libraries are introduced, the stages of the conceptual model of optimal adaptive monitoring of objects of this class are described, the goals and objectives of monitoring are considered. A set of principles is proposed for optimal adaptive monitoring of electronic libraries, which creates the prerequisites for the synthesis of algorithms for optimal and adaptive monitoring, assessment and prediction of the state (quality) of such systems in order to reduce the cost of resources of the control system, increase the efficiency and reliability (accuracy) of decision making on managing digital libraries in different environments.

Keywords: electronic library, monitoring, condition, quality, analysis, observation, evaluation, forecasting.

Введение. В информационно-телекоммуникационную среду, в информационное пространство все активнее внедряются электронные библиотеки, призванные, в конечном итоге, оттеснить на второй план традиционные библиотеки в области образования и научно-исследовательской деятельности. Данный процесс обусловлен общемировым эволюционным развитием информационно-телекоммуникационной инфраструктуры, закономерен и необратим. Ярким примером современных электронных библиотек (ЭБ), библиотек нового цифрового поколения, является единая ЭБ образовательных и научно-исследовательских организаций Министерства обороны РФ в рамках проекта «Электронный вуз» [1]. Данная ЭБ, как и любая иная, представляет собой емкую и мощную информационную систему для обеспечения поиска и управляемого доступа по информационно-телекоммуникационным сетям к электронным документам без индивидуального носителя, профессиональным базам данных, информационным справочным и поисковым системам, а также иным информационным ресурсам. Она построена на различных технологиях и рассчитана на предоставление широкого спектра услуг.

Анализ теоретических положений и результатов практического использования мониторинга в различных сферах деятельности, анализ современного состояния информационного обеспечения управления ЭБ, современных требований и тенденций технической эволюции инфотелекоммуникационных систем и управления ими, а также широкое использование «де факто» рассматриваемого понятия, позволяют нам сформулировать свой взгляд на сущность мониторинга ЭБ, как типовых компонент информационно-телекоммуникационной среды. Мониторинг ЭБ – единый комплекс систематических целенаправленных мероприятий (организационных, технологических и технических), основанный на непрерывном либо периодическом (регулярном) наблюдении за состоянием ЭБ (сбор, хранение, обработка и анализ информации о состоянии), качественном и количественном оценивании состояния (качества) и прогнозировании изменений состояния (качества) ЭБ под влиянием конструктивных или деструктивных факторов. Итак, мониторинг ЭБ должен включать ряд последовательных операций: 1) наблюдение (контроль) за состоянием ЭБ, состоянием ее элементов и за факторами, воздействующими на них; 2) текущее комплексное оценивание состояния (качества) ЭБ и ее элементов; 3) прогнозирование возможных изменений состояния (параметров, показателей качества (ПК)) ЭБ и ее элементов.

Качество ЭБ – свойство или совокупность свойств данного объекта, обуславливающих его соответствие назначению [2, 3]. Наблюдение – комплексный целенаправленный процесс восприятия (сбора, хранения, обработки

и анализа) информации о состоянии ЭБ и факторов, воздействующих на нее. Оценивание – процесс принятия решения о состоянии (качестве) ЭБ, процедура получения качественных и количественных оценок состояния (оценочных значений ПК) ЭБ. Прогнозирование – процесс разработки прогноза, исследования конкретных перспектив изменения состояния (качества) ЭБ в различных ожидаемых условиях эксплуатации. Выработка вероятностного суждения о возможных изменениях состояния (параметров, ПК) ЭБ.

Ключевым направлением развития мониторинга ЭБ как типовых компонент информационно-телекоммуникационной среды, является, на наш взгляд, создание системы оптимального адаптивного мониторинга. При этом под адаптивностью мониторинга будем понимать способность осуществлять целенаправленное приспособление (согласование) характеристик свойств поведения данного процесса к сложным условиям, имеющая целью оптимизацию параметров мониторинга ЭБ. Адаптация осуществляется в интересах получения оптимальной (необходимой и достаточной) информации о состоянии (качестве) ЭБ, соответствующей (адекватной) сложившейся ситуации. Оптимальный мониторинг ЭБ – мониторинг объекта такого типа, при котором траектория достижения цели данного процесса в пространстве ситуаций является самой предпочтительной в смысле принятого критерия. Опираясь на рассмотренные понятия, можно сформулировать базовые понятия концептуальной модели оптимального адаптивного мониторинга ЭБ [4].

Основополагающей целью оптимального адаптивного мониторинга (ОАМ) ЭБ является информационно-аналитическое обеспечение системы управления (СУ) ЭБ, адекватное целям функционирования и управления ею и учитывающее влияние внешних и внутренних, конструктивных и деструктивных факторов. Для реализации указанной цели осуществляются процедуры ОАМ ЭБ, решающие следующие основные задачи: наблюдение – оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) условиям эксплуатации получение (выявление, регистрация и накопление) требуемой на данный момент информации о фактическом состоянии ЭБ; оценивание – оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) текущим требованиям СУ получение оценок состояния (качества) ЭБ; прогнозирование – оптимизируемое по состоятельности, достоверности и точности, а также соответствующее (подстраивающееся к) текущим требованиям СУ получение прогностических оценок состояния (качества) ЭБ.

Иными словами, выполняется ряд взаимосвязанных задач – на основании полученной в результате наблюдения информации решается задача принятия информационного решения о годности или негодности конкретной ЭБ для выполнения определенных функций в данный момент времени и в данных условиях. В случае, если принимается решение о негодности ЭБ, то возникает задача идентификации и локализации неисправностей и отказов, включая коллизии, связанные с нарушениями безопасности информации в ЭБ [5].

Необходимым условием эффективного анализа и синтеза алгоритмов оптимального адаптивного мониторинга ЭБ является использование принципов системного подхода. Опираясь на основные принципы системного подхода, сформулируем базовые принципы и рекомендации, определяющие научную и практическую стороны реализации процесса оптимального адаптивного мониторинга ЭБ. К принципам ОАМ ЭБ можно отнести: принцип единства (двойственности) ОАМ; принцип множественности моделей; принцип цели (целевой ориентации, целенаправленности) ОАМ ЭБ; принцип преемственности информационно-аналитических методов мониторинга; принцип информационно-аналитического единства, требующий использования стандартных единых расчетно-аналитических подходов к реализации мониторинга ЭБ; принцип адаптивности мониторинга ЭБ; принцип регулярности мониторинга ЭБ; принцип постоянства мониторинга ЭБ; принцип активности мониторинга ЭБ; принцип комплексности (целостности, всесторонности, интегративности) мониторинга ЭБ; принцип преемственности результатов (историзма) мониторинга ЭБ, а также принцип пригодности результатов ОАМ ЭБ для практического использования в интересах управления структурой, параметрами и режимами функционирования ЭБ.

Заключение. Таким образом, рассмотрены особенности и перспективы построения электронных библиотек, предпринята попытка сформулировать ключевые концептуальные основы оптимального адаптивного мониторинга их состояния (качества). Сформулирована сущность и введены квалиметрические понятия мониторинга электронных библиотек, описаны этапы концептуальной модели оптимального адаптивного мониторинга объектов такого класса, рассмотрены цели и задачи мониторинга. Предложен комплекс принципов оптимального адаптивного мониторинга электронных библиотек, что создает предпосылки для синтеза алгоритмов оптимального и адаптивного наблюдения, оценивания и прогнозирования состояния (качества) таких систем в целях снижения затрат ресурсов системы управления, повышения оперативности и достоверности (точности) принятия решений по управлению электронными библиотеками в различных условиях обстановки.

СПИСОК ЛИТЕРАТУРЫ

1. Электронная библиотека Министерства обороны Российской Федерации (2019) [Электронный ресурс] – Режим доступа: http://mil.ru/departament_informashion_system/activity/ellib.htm, свободный. – Загл. с экрана.
2. Петухов Г.Б. Основы теории эффективности целенаправленных процессов. Ч.1. – М.: МО СССР, 1989. – 660 с.
3. Евланов Л.Г. Контроль динамических систем. –М.: Наука, 1979. – 432 с.
4. Паращук И.Б. Вариант классификации процедур мониторинга в интересах синтеза систем контроля качества телекоммуникационных сетей // Приборы и Системы: Управление, Контроль, Диагностика. №5, 2003. С. 64-67.
5. Авраменко В.С., Маликов А.В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // Региональная информатика и информационная безопасность. Выпуск 4. . – СПб.: СПОИСУ, 2017. – 533 с., С. 24-26.

УДК 004.942

ИНФОРМАЦИОННЫЕ СИСТЕМЫ В ИНТЕРЕСАХ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМ ОБЕСПЕЧЕНИЕМ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Кузнецов Евгений Михайлович, Лебедев Игорь Вячеславович, Масалов Александр Александрович, Пантюхин Олег Игоревич

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: kuznetsov52em@yandex.ru, liv03081979@gmail.ru, masalov.84@mail.ru, p_oleg99@mail.ru

Аннотация. Рассмотрена актуальность создания информационных систем в целях поддержки управления техническим обеспечением телекоммуникационных сетей специального назначения и предложена концепция их развития. Проведен анализ существующих информационных платформ. Рассмотрены основные проблемные вопросы при переходе от существующей системы управления техническим обеспечением телекоммуникационных сетей специального назначения к автоматизированной информационной системе.

Ключевые слова: информационные системы, управление техническим обеспечением.

APPLICATION OF INFORMATION SYSTEMS FOR MANAGEMENT OF TECHNICAL SUPPORT OF TELECOMMUNICATION NETWORKS

Kuznetsov Evgeny, Lebedev Igor, Masalov Alexsandr, Pantyukhin Oleg

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: kuznetsov52em@yandex.ru, liv03081979@gmail.ru, masalov.84@mail.ru, p_oleg99@mail.ru

Abstract. The relevance of creating information systems to support the management of technical support for special-purpose telecommunications networks is considered and the concept of their development is proposed. The analysis of existing information platforms is carried out. The main problematic issues in the transition from the existing management system for technical support of special purpose telecommunications networks to an automated information system are considered.

Keywords: information systems, technical support management**.**

Введение. В настоящее время ускоренными темпами идет переоснащение телекоммуникационных сетей специального назначения (ТССН) на перспективные средства, эксплуатация которых во многом зависит от состояния системы технического обеспечения (ТО). На эту систему возложены функции по поддержанию максимально возможной обеспеченности множества территориально распределенных организаций (предприятий) работоспособным (исправным), готовым к применению по назначению телекоммуникационным оборудованием [1].

Если автоматизированное управление сетями закладывается производителями телекоммуникационных средств, то автоматизации мероприятий технического обеспечения ТССН уделяется недостаточное внимание. Под автоматизацией в большинстве случаев понимается оснащение руководителей и должностных лиц, ответственных за техническое обеспечение, вычислительными средствами с общим программным обеспечением, что не позволяет в полной мере реализовать на практике информационную поддержку в системе управления технического обеспечения ТССН на всех уровнях иерархии.

Эффективное управление системой ТО ТССН, в свою очередь, зависит от достоверности сведений, поступающих с нижних уровней иерархии и точности принятия решений на основе их обработки. Основные слагаемые успешной практической реализации информационных систем для ТССН можно сформулировать, как применение концепции «от «А» до «Я»: от автоматизированного сбора, автоматической обработки информации до подготовки предложений в решение на организацию, планирование и управление системой с автоматизация всех нетворческих процессов (сбор, обработка и передача информации; производство расчетов, моделирование, поддержка принятия решений; оформление и размножение различных документов и т.д.).

С точки зрения системного подхода, все предприятия весьма похожи друг на друга. В структуру каждого из них входят многочисленные подразделения, непосредственно осуществляющие тот или иной вид деятельности. Такой взгляд позволяет сформулировать общие принципы построения корпоративных информационных систем (далее - КИС), т.е. информационных систем в масштабе всего предприятия [2]. Не являются исключением и структурные подразделения силовых ведомств.

К сожалению единого подхода, в создании КИС нет, хотя и существуют типовые решения, например, платформа «1С: ERP: Управление предприятием» от российского производителя, предназначенная для построения комплексных информационных систем управления деятельностью многопрофильных предприятий с учетом лучших мировых и отечественных практик автоматизации крупного и среднего бизнеса. Однако в компании 1С отталкиваются от собственного опыта в условиях российской действительности, что в конечном итоге и заставляет вместе с программным продуктом покупать и 1С программиста, после чего адаптировать, дорабатывать и оптимизировать. Учитывая опыт специалистов, занимающихся внедрением ERP, большая часть компаний, использующих 1С занимаются доработкой системы на всем сроке её эксплуатации. Что, впрочем, верно и для западных систем (Microsoft Dynamics NAV, SAP Business One) [3]. С финансовой точки зрения это сопоставимо, а

возможно даже и экономически менее выгодно, чем разработка новой информационной системы, которая будет изначально удовлетворять всем возложенным на нее требованиям предъявляемым управлением техническим обеспечением ТССН.

В целях «безболезненного» перехода от существующей системы управления к автоматизированной целесообразно при проектировании применить принцип создания «Как есть» с последующей оптимизацией до «Как должно быть» и максимальной автоматизацией процессов сбора и обработки информации.

Поскольку данные составляют основу деятельности любой организации и являются наиболее стабильной её составляющей (функции и структура организации меняются гораздо чаще), то при построении ведомственных информационных систем наиболее адекватным решаемым задачам является подход к проектированию, основанный на данных [2]. Такой подход обеспечивает наилучшее архитектурное решение при разбиении системы на приложения, а также простоту и согласованность при интеграции приложений.

Модульная структура построения информационной системы управления технического обеспечения ТССН может состоять из подсистем, объединённых в функциональные группы: формирования данных об изделиях, предоставления элементарных сведений, формирования запросов и отчётов. Данное построение сможет обеспечить изменение практически любых разделов при сохранении целостности информационной системы управления техническим обеспечением ТССН.

Также при создании информационной системы технического обеспечения специального назначения необходимо добиться выделения элементарных (неделимых) параметров (атрибутов), однозначно определяющих характеристики и свойства, как конкретного изделия, так и системы в целом; реализации различных запросов с возможностью совершать среднесрочные и долгосрочные прогнозы; обеспечение устойчивого функционирования и развития информационной системы.

Исходя из главной функции технического обеспечения ТССН делаем вывод, что единицей измерения эффективного функционирования системы является образец техники и его техническое состояние, а процент обеспеченности и процент работоспособной (исправной) техникой - характеристиками системы. Таким образом актуализация данных, направленная на выполнение главной функции системы (о количестве работоспособной техники), происходит на нижнем уровне иерархии, при этом многие процессы сбора данных возможно автоматизировать (например, сведения о наработке изделия в режиме реального времени).

Проведенных анализ документов, циркулирующих в системе технического обеспечения ТССН, позволяет классифицировать их на следующее виды: финансовые (бухгалтерские); документы по учету эксплуатации технических и программных средств; планирующие документы по техническому обеспечению ТССН; руководящие, технические и справочные документы; отчетные и другие документы.

Построив модель информационных потоков в системе управления технического обеспечения ТССН можно сделать вывод, что наибольшее количество связей имеют два объекта: «Паспорт-формуляр на изделие» и «Донесение», на которые и приходится весь основной поток данных об изделии. При этом следует учесть, что информация в них дополняет друг друга. Таким образом, если иметь доступ к обоим источникам возможно получение более полной информации об изделии. Следует отметить, что основной поток данных является статичным и вводится в информационную систему при вводе изделий в эксплуатацию. К ним относятся учетные сведения об изделии, требования руководящих и эксплуатационных документов.

Практически все сведения об изделии, вводятся в базу данных информационной системы уже на процессе ввода его в эксплуатацию. Наибольшей динамикой изменения обладают сведения по наработке и текущему состоянию образца ТССН, получаемые от оперативно-технических служб подразделений, непосредственно эксплуатирующих телекоммуникационное оборудование. Очевидно, что в дальнейшем сбор и первичную обработку указанных данных целесообразно производить в автоматическом (автоматизированном) режиме.

Требования руководящих документов обладают низкой динамикой изменения их обновление должно осуществляться централизовано вместе с обновлениями специального программного обеспечения. При этом, однако, необходимо учесть, что существующие классификаторы и номенклаторы оборудования телекоммуникационных систем не могут в полной мере обеспечить однозначное идентификацию изделий в существующих учетных и отчетных документах, так как перечень используемого оборудования, в следствии его поступательного развития, периодически подвергается изменению. Введение кодирования образцов техники связи и АСУ позволит, не только однозначно классифицировать каждый, а также заложить перспективу на расширение номенклатуры, минимизировать объем обрабатываемой информации и значительно упростить разработку сводных отчетов по различным признакам.

Заключение. Таким образом, несмотря на определенные недостатки существующей системы управления ТО ТССН, стоит отметить, что при определенном уровне автоматизации и незначительном изменении алгоритмов сбора и обработки сведений, она должна стать основой для проектируемой «инфокоммуникационной» системы с расширенными возможностями. Глубокий экспертный анализ задаст основные направления её развития с учетом современных тенденций, обеспечивая преемственность развития и облегчение внедрения её в существующую систему.

СПИСОК ЛИТЕРАТУРЫ

1. Чихачев А.В., Третьяков С.М., Бурлаков А.А. и др. Техническое обеспечение связи и автоматизации. – СПб.: ВАС, 2017. 302 стр.
2. Погонин В.А., Схиртладзе А.Г. Интегрированные системы проектирования и управления. Корпоративные информационные системы: Учеб. пособие. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. 144 с.
3. Сравнение ERP - обзор преимуществ и недостатков SAP BUSINESS ONE, MICROSOFT DYNAMICS NAV и 1С ERP 2.0 [Электронный ресурс]. URL: http://mindcore.ru/bez-rubriki/sravnenie-erp-obzor-preimushhestv-i-nedostatkov.html (дата обращения: 10.06.2020).

УДК 004.942

ЭКСПЕРТНЫЕ СИСТЕМЫ ДЛЯ АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И ТЕХНОЛОГИЙ, ИХ ЗАДАЧИ И ОСОБЕННОСТИ

Малофеев Валерий Александрович, Паращук Игорь Борисович, Пронин Антон Александрович, Саяркин Леонид Андреевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: valeron12.1366@gmail.com, shchuk@rambler.ru, sayarkin95@mail.ru

Аннотация. Рассмотрены задачи и особенности экспертных систем для анализа кибербезопасности телекоммуникационных сетей и технологий. Проанализированы основные возможные этапы жизненного цикла экспертных систем в интересах оценки уровня кибербезопасности и проектирования систем кибербезопасности. Экспертных систем, позволяющих устранить противоречие между субъективным характером принятия экспертного решения и формирования экспертной оценки по результатам рассмотрения материалов (исходных данных) и ростом степени автоматизации процесса анализа уровня кибербезопасности сетей и технологий телекоммуникаций.

Ключевые слова: кибербезопасность, экспертная система, анализ, проектирование, телекоммуникационная сеть, технология, решение, информация.

EXPERT SYSTEMS FOR ANALYSIS OF THE CYBER SECURITY OF TELECOMMUNICATION NETWORKS AND TECHNOLOGIES, THEIR TASKS AND FEATURES

Malofeev Valery, Parashchuk Igor, Pronin Anton, Sayarkin Leonid
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: valeron12.1366@gmail.com, shchuk@rambler.ru, sayarkin95@mail.ru

Abstract. The tasks and features of expert systems for the analysis of cyber-security of telecommunication networks and technologies are considered. The main possible stages of the life cycle of expert systems are analyzed in the interests of assessing the level of cyber-security and designing cyber-security systems. Expert systems that allow eliminating the contradiction between the subjective nature of making an expert decision and forming an expert assessment based on the results of consideration of materials (initial data) and the increasing degree of automation of the process of analyzing the level of cyber-security of networks and telecommunication technologies.

Keywords: cyber-security, expert system, analysis, design, telecommunication network, technology, solution, information**.**

Введение. Важной особенностью современного этапа научно-технического прогресса является стремительное развитие систем кибербезопасности (КБ) телекоммуникационных сетей и технологий (ТКСиТ). При этом под кибербезопасностью понимается раздел информационной безопасности, в рамках которого изучают процессы формирования, функционирования и эволюции киберобъектов ТКСиТ, для выявления источников киберопасности, образующихся при этом, определение их характеристик, а также их классификацию и формирование нормативных документов, выполнение которых должно гарантировать защиту киберобъектов ТКСиТ от всех выявленных и изученных источников киберопасности [1].

Большинство современных систем КБ (СКБ) ТКСиТ являются сложными управляемыми системами, разработка которых требует постоянного анализа тенденций их развития, направлений совершенствования технологий их построения. Похожие задачи стоят и перед специалистами, осуществляющими экспертизу качества технических решений, принимаемых в ходе анализа КБ, проектирования и построения СКБ ТКСиТ. В отличие от процесса разработки СКБ ТКСиТ, реализация которого требует принятия технических решений по всему перечню решаемых задач проектирования различными специалистами (группами специалистов), процесс экспертной деятельности должен быть направлен на формирование экспертных оценок, основанных на анализе некоторых обобщенных показателей качества проектируемой системы, характеризующих стратегические технические решения (технические решения, определяющие облик системы кибербезопасности в целом) и осуществляется сравнительно небольшой группой специалистов. Таким образом, организация экспертной деятельности представляет собой вполне самостоятельную задачу, решаемую в ходе анализа КБ и проектирования СКБ ТКСиТ. Методы, направленные на снижения организационных сложностей коллективной работы (анкетирование, интервью, анкетирование с участием интервьюера) и снижение степени субъективности экспертных оценок (парные сравнения, масштабирования, ранжирования, свертки) как правило, не используются.

С целью повышения эффективности экспертной деятельности, в настоящее время разработан целый ряд экспертных систем (ЭС) для различных сфер деятельности [2-4]. Понимая под знаниями взаимоувязанную совокупность данных полученных в ходе практической деятельности и учитывающих профессиональный опыт специалистов в конкретной области, а так же используя результаты анализа множества определений ЭС, разрабатываемых для различных сфер деятельности, сформулируем понятие ЭС применительно к анализу КБ и проекту СКБ ТКСиТ. Функциональная структура ЭС в интересах анализа КБ и проектирования СКБ ТКСиТ включает следующие элементы: эксперт (группа экспертов) – пользователь (ей); интерфейс эксперта-

пользователя; база знаний о КБ и СКБ (БЗСИБ); интеллектуальный редактор БЗСИБ; инженер по знаниям; эксперт-донор.

Современные ЭС представляют собой сложные программные комплексы, аккумулирующие знания специалистов в конкретных предметных областях и распространяющих этот опыт для консультирования менее квалифицированных пользователей. Исходя из этого, рассмотрим основные возможные этапы жизненного цикла ЭС анализа КБ и проектирования СКБ ТКСиТ. Действительно, в области анализа КБ, разработки и экспертной оценки СКБ ТКСиТ трудно представить себе такую ситуацию, когда применение математических методов обоснования технических решений или реализация методов моделирования для оценки оптимальности принятого решения были бы лишними. Все этапы жизненного цикла ЭС в интересах анализа КБ и проектирования СКБ ТКСиТ можно разделить на ряд относительно независимых этапов: разработка технического задания (ТЗ); подготовка к проектированию; разработка прототипа; доработка; оценка; стыковка; поддержание в актуальном состоянии. Таким образом, несомненно, что одним из эффективных подходов к оптимизации анализа КБ и создания систем КБ телекоммуникационных сетей и технологий является подход, основанный на построении экспертных систем, реализующих, наряду со структурированием экспертных знаний, современные достижения теорий вероятности, нечетких множеств, массового обслуживания, математической статистики, теории игр и опирающихся на данные, поступающие из действующих систем-аналогов, на данные имитационного моделирования.

Суть подхода заключается в формировании экспертных показателей качества (ЭПК), отражающих уровень КБ и существенные свойства СКБ ТКСиТ, формировании оптимальных (не избыточных) экспертных систем показателей качества (ЭСПК), соответствующих физическому, канальному и сетевому уровню кибербезопасности ТКСиТ, на основе моделей и алгоритмов, соответствующих характеру и степени априорной неопределенности того или иного этапа функционирования данной системы. Очевидно, что реализовать предложенные модели и методы в ходе организации экспертной деятельности в интересах анализа кибербезопасности ТКСиТ возможно только на основе разработки специальных экспертных систем [4].

Принимая во внимание относительно невысокие требования к временным параметрам процесса обновления знаний и принятия решения в ходе организации экспертной деятельности, а также учитывая непрерывное параллельное развитие вычислительной техники и технологий хранилищ данных, такие ЭС можно классифицировать как квазидинамические ЭС с возможностью их организации на основе локальных вычислительных сетей. По степени интеграции программного обеспечения ЭС такого класса могут быть определены как гибридные, функционирующие как интеллектуальная надстройка над пакетами прикладных программ реализующих структурные и функциональные модели анализа КБ ТКСиТ. Разработка специальной интегрированной среды для реализации ЭСПК выглядит более затратной и менее гибкой.

Основу знаний, содержащихся в специальной ЭС должны, на наш взгляд, составлять знания: содержащиеся в памяти эксперта-донора; полученные в результате моделирования процессов изменения ЭПК КБ ТКСиТ; полученные в результате анализа данных, поступающих из системы-аналога; содержащиеся на материальных носителях (компакт диски, специальная литература и т.д.). В настоящее время разработаны десятки моделей (языков) представления знаний для различных предметных областей. Все многообразие моделей можно разбить на две большие группы – модульные и сетевые. Поскольку модульные модели оперируют совокупностью не связанных элементов знаний и предназначены для интерпретации только поверхностных знаний в специальной ЭС такого класса должны быть реализованы сетевые языки представления знаний. Высокая степень абстрагирования предметной области ограничивает применение формально-логических моделей в прикладных ЭС, но для организации экспертной деятельности при анализе КБ ТКСиТ реализация формально-логических моделей в специальных ЭС может оказаться весьма продуктивной. Также весьма продуктивными, на наш взгляд, могут оказаться модели ЭС для анализа КБ, основанные на искусственных нейронных сетях [5].

Заключение. Таким образом, рассмотрены задачи и особенности экспертных систем для анализа кибербезопасности телекоммуникационных сетей и технологий. Проанализированы основные возможные этапы жизненного цикла экспертных систем в интересах оценки уровня кибербезопасности и проектирования систем кибербезопасности. Экспертных систем, позволяющих устранить противоречие между субъективным характером принятия экспертного решения (формирования экспертной оценки) по результатам рассмотрения материалов (исходных данных) и ростом степени автоматизации процесса анализа уровня кибербезопасности сетей и технологий телекоммуникаций.

СПИСОК ЛИТЕРАТУРЫ

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. №5(8). 2014. С. 39-42.
2. Гаськова Д.А., Массель А.Г. Разработка экспертной системы для анализа угроз кибербезопасности в энергетических системах // Информационные и математические технологии в науке и управлении. №1. 2016. С.113-122.
3. Созинова Е.Н. применение экспертных систем для анализа и оценки информационной безопасности // Молодой ученый. №10. 2011. С. 64-66.
4. Ненадович Д.М., Паращук И.Б., Лещенко А.С. Особенности экспертных систем в интересах анализа информационной безопасности телекоммуникационных сетей // V-я Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». Материалы конференции. – СПб.: СПОИСУ, 2007. С. 114-115.
5. Авраменко В.С., Маликов А.В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // Региональная информатика и информационная безопасность. Выпуск 4. . – СПб.: СПОИСУ, 2017. – 533 с., С. 24-26.

УДК 004.942

ПЛАНИРОВАНИЕ ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИИ КОМПЛЕКСОВ СРЕДСТВ АВТОМАТИЗАЦИИ

Масалов Александр Александрович, Кузнецов Евгений Михайлович, Ковбасюк Александр Васильевич, Лебедев Игорь Вячеславович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: masalov.84@mail.ru, edelritter@mail.ru, liv03081979@gmail.ru

Аннотация. Рассмотрена необходимость автоматизации планирования технической эксплуатацией комплексов средств автоматизации с использованием методов, разработанных на основе моделей сетевого планирования и управления.

Ключевые слова: техническое эксплуатация; система сетевого планирования и управления; сетевая модель; программные продукты.

PLANNING OF TECHNICAL OPERATION OF COMPLEXES OF MEANS OF AUTOMATION

Masalov Aleksandr, Kuznetsov Evgeni, Kovbasyuk Aleksandr, Lebedev Igor
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: masalov.84@mail.ru, edelritter@mail.ru, liv03081979@gmail.ru

Abstract. The necessity of planning automation by the technical operation of automation systems using the methods developed on the basis of network planning and management models is considered.

Keywords: technical exploitation; network planning and management system; network model; software products.

Введение. В современных условиях большими темпами идет переоборудование комплексов средств автоматизации специального назначения (КСА СН) на перспективные и современные образцы, успешная и эффективная эксплуатация которых во многом зависит от состояния системы планирования и управления технической эксплуатации. Как известно, целью планирования является четкая регламентация мероприятий эксплуатации с их взаимоувязкой по силам, средствам и времени выполнения. При решении разнообразных технической эксплуатации КСА СН важна предварительная инженерная проработка (прогноз) условий их осуществления, установление временных рамок мероприятий и обеспечения их необходимыми ресурсами. Действительно, невозможно себе представить, например, назначение работ по техническом обслуживанию в ущерб обеспечению действующих связей и подготовки инженерно-технического персонала. С другой стороны, успешное использование техники по назначению возможно лишь при периодическом обслуживании и равномерном расходе ресурса. В свою очередь, качество выполнения технического обслуживания в значительной степени зависит от эффективности мероприятий метрологического обеспечения, качество ремонта определяется своевременной поставкой ЗИП, а эффективность работы ремонтных органов – своевременной поставкой ремфонда и т.д. Рассмотрение цепи мероприятий по поддержанию технической готовности КСА СН приводит к выводу о необходимости взаимоувязки, которая решается целенаправленными действиями должностных лиц по их планированию [1].

В настоящее время одним из основных подходов к процессам автоматизации планирования выступают методы, разработанные на основе моделей сетевого планирования и управления (СПУ). Задачи СПУ решаются в следующей последовательности: построение исходного сетевого графика - расчет параметров исходного сетевого графика - оптимизация сетевого плана по исходному сетевому графику.

С точки зрения оптимизации процессов управления реализация метода сетевого планирования и управления включает два основных этапа: структурное и календарное планирование.

На этапе структурного планирования вначале весь процесс планирования ТЭ КСА СН требуется разбить на четко определенные отдельные операции, составляющие весь процесс, их отношения предшествования (т.е. какая операция должна предшествовать другой) и их длительность. Затем определяются взаимосвязи отдельных операций. На основании этого строится сетевая модель (сетевой график), каждая дуга (стрелка) которой отображает определенную операцию. Таким образом, сетевая модель является графическим представлением взаимосвязи операций процесса ТЭ КСА СН.

Построение сетевой модели на этапе структурного планирования позволит детально проанализировать все операции и внести улучшение в структуру процесса еще до начала его реализации. В дальнейшем сетевая модель будет использоваться для разработки календарного плана выполнения операций, задачи которого играют особо важную роль в управлении проектами. Задачи календарного планирования, как правило, многокритериальны, многоэкстремальны, имеют множество несвязанных решений и поэтому относятся к комбинаторным задачам со сложной алгебраической структурой и дискретными процессами оптимизации, далекими от тех непрерывных процессов и функций [2].

На этапе календарного планирования определяются моменты начала и окончания каждой операции ТЭ КСА СН с указанием ее взаимосвязи с другими операциями. Кроме того, календарный график должен дать возможность выявлять критические операции (с точки зрения времени выполнения исследуемого процесса), которым требуется уделять особое внимание, чтобы закончить исследуемый процесс к назначенному сроку. Что касается некритических операций, то календарный план позволит определить резервы времени, которые можно выгодно использовать при

задержке выполнения этих операций или для эффективного расходования ресурсов. Далее для наглядности представления календарного графика ТЭ КСА СН необходимо построить диаграмму Ганта, которая, является по сути «надстройкой» над сетевой моделью.

Система СПУ позволяет формировать календарный план реализации сложного комплекса работ, определять и мобилизовать резервы времени, предупреждать возможные срывы в ходе работ, осуществлять оперативную корректировку планов. При этом важно учитывать, что данные планирования вышестоящего органа управления являются исходными для планирования подчиненного уровня.

Точно так же содержание и результаты оперативного планирования основываются на данных текущего планирования, которое, в свою очередь, использует данные перспективного планирования.

Сетевая модель для планирования ТЭ КСА СН являются эффективным средством, поскольку позволяет:

– сформировать календарный план реализации сложного проекта;

– определить и мобилизовать резервы времени, материальных, финансовых, информационных, трудовых ресурсов;

– осуществить реализацию принципа "точно в срок" с прогнозированием и предупреждением возможных срывов в ходе реализации проекта;

– повышать эффективность управления при четком распределении ответственности между руководителями разного уровня и исполнителями и необходимом делегировании полномочий;

– оптимальным образом выполнить весь комплекс работ, возлагаемых на систему ТЭ КСА объекта автоматизации;

– скоординировать работу должностных лиц и обеспечить высокую наглядность хода выполнения работ, проводимых в системе управления и планирования мероприятий ТЭ КСА;

– иметь возможность в случае необходимости, перераспределять людские ресурсы между работами.

Как мы видим особенностью методов СПУ является не только моделирование всего комплекса работ, но и выявление тех участков, от которых в наибольшей степени зависит выполнение всего проекта в установленные сроки.

Сегодня на IT-рынке имеются разнообразные программные продукты, реализующие сетевые методы планирования от внушительных профессиональных систем до систем, позволяющих эффективно распорядиться рабочим временем, финансовыми средствами и т.п. Данные программные средства можно разделить по следующим категориям [3]: профессиональные системы планирования; системы планирования среднего класса; системы быстрого планирования; органайзеры (планировщики).

Наиболее известные и широко используемые из них — Microsoft Office Project, OpenPlan, Spider Project. Модели проекта, используемые в них, основаны на методе критического пути и отличаются лишь в деталях. Как правило, овладев одной из этих программ, не составляет труда воспользоваться любой другой [4].

Заключение. В настоящее время должностные лица, ответственные за планирование и контроль мероприятий ТЭ КСА для исполнения документов как правило используют текстовые и графические редакторы, оставляя без внимания программные средства сетевого планирования, что приводит к увеличению сроков планирования и управления мероприятиями ТЭ КСА. Стоит отметить необходимость учитывать тот факт, что использование средств сетевого планирование целесообразно начиная с уровней управления имеющих значительный объем задач, оперирующих распределением ресурсов и обладающих малыми сроками на исполнение документов и их оперативную корректировку.

В тоже время рациональность использования средств сетевого планирования, подтверждена во всем мире и нет сомнений, что вопрос внедрения данных средств и методов с целью оптимизации планирования ТЭ КСА СН только вопрос времени.

СПИСОК ЛИТЕРАТУРЫ

1. Абышко В.Ю., Баринов М.А., Захаров А.А., Чихачев А.В. Техническое обеспечение связи и автоматизации.
2. Учебник. - Спб.: ВАС, 2010. -320с.
3. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении.
4. Учебное пособие для вузов. –М.: Финансы и статистика, 2002.
5. Математические основы управления проектами.
6. Учебное пособие / С.А. Барков, В.И. Воропаев, Г.И. Секлетова [и др.]. – М.: Высш. шк., 2005.
7. Официальный сайт программы Spider Project [Электронный ресурс]. URL: http:// www.spiderproject.com (дата обращения: 6.06.2020).

УДК 025.2.004; 621.311.23: 629.12

ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Михайличенко Антон Валерьевич, Михайличенко Николай Валерьевич, Султанова Ясмина Маратовна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: katjuha777@inbox.ru, 23esn2008@rambler.ru

Аннотация. В работе обоснованы актуальность и объективная необходимость повышения достоверности анализа эффективности функционирования центров обработки данных в интересах обоснованного и оперативного управления структурой, параметрами и режимами работы таких систем. Сформулированы ключевые виды неопределенности, влияющие на принятие решений в задачах оценки эффективности

функционирования центров обработки данных. Предлагаемый подход основан на том, что синтез оптимальной системы показателей, подлежащих наблюдению, оцениванию и прогнозированию, производится с учетом всего объема и номенклатуры услуг, которые должны быть предоставлены пользователю. Вследствие этого повышается достоверность контроля состояния ЦОД и обоснованность принимаемых решений по управлению параметрами и режимами его работы.

Ключевые слова: качество, эффективность, показатель, управление, центр обработки данных.

APPROACH TO EVALUATING THE PERFORMANCE OF DATA CENTERS

Mikhaylichenko Anton, Mikhaylichenko Nikolay, Sultanova Yasmina
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: katjuha777@inbox.ru, 23esn2008@rambler.ru

Abstract. The paper substantiates the relevance and objective need to improve the reliability of the analysis of the effectiveness of data processing centers in the interests of reasonable and operational management of the structure, parameters and modes of operation of such systems. Key types of uncertainty affecting decision-making in the tasks of evaluating the effectiveness of data processing centers are formulated. The proposed approach is based on the fact that the synthesis of the optimal system of indicators to be monitored, evaluated and predicted is made taking into account the entire volume and range of services that should be provided to the user. This increases the reliability of data center status monitoring and the validity of decisions made to manage its parameters and operating modes.

Keywords: quality, efficiency, indicator, management, data center.

Введение. Для достижения своевременности и устойчивости предоставления информационных услуг пользователям необходимо использовать высокопроизводительную ИТ-инфраструктуру. Одним из ключевых элементов высокопроизводительной ИТ-инфраструктуры является центр обработки данных (ЦОД). Центр обработки данных это согласованная по задачам и развернутая на местности взаимосвязанная совокупность программно-аппаратных средств, предназначенных для создания высокопроизводительной и отказоустойчивой инфраструктуры, отвечающей за обработку и хранение информации в интересах пользователей [1].

Анализ современных условий функционирования ЦОД позволяет выделить ряд противоречий между существующим уровнем развития методов и средств хранения и обработки данных (уровнем развития ЦОД), потребностью в обеспечении их высокой результативности с одной стороны, и уровнем развития методик оценивания эффективности ЦОД в интересах управления структурой, параметрами и режимами их функционирования в различных условиях неопределенности, с другой стороны.

Основой методологии построения сложных информационно-технических систем являются методы оценки эффективности их функционирования. Разработке данных методов посвящен ряд исследований [2, 3]. Развитые в этих исследованиях методы анализа эффективности легли в основу существующих частных методик оценки эффективности функционирования сложных информационных систем.

Вместе с тем, дальнейшее их использование для сравнительного анализа существующих систем таких как ЦОД ВН и выработке перспективных направлений их развития становится затруднительным в силу следующих причин.

Во-первых, отсутствие учета разноплановости характеристик ЦОД.

Во-вторых, существующие частные методики не обеспечивают учет противоречий при статистических и параметрических измерениях характеристик ЦОД.

В-третьих, ограничения на ресурсы моделирования и отсутствие статистических данных о параметрах ДЦ не позволяет получить достоверную информацию о значениях ПК.

Таким образом, на сегодняшний день не существует методик, позволяющих проводить в комплексе оценку эффективности функционирования ЦОД с одновременным учетом нечеткости, неполноты и противоречивости информации об его состояниях, тогда как объективно существует целый ряд факторов, вносящих данную неопределенность в условиях их функционирования.

Возникает задача развития существующих моделей оценки эффективности на случай учета особенностей реального процесса функционирования ЦОД ВН, с учетом нечеткости, неполноты и противоречивости информации о его состояниях которую в работе предложено решать с использованием математического аппарата нейро-нечетких сетей.

Сущностью, предлагаемой модифицированной вероятностно-временной модели, является совместное использование известных подходов описания поведения системы в пространстве состояний – например разностных уравнений и нейро-нечетких сетей (ННС). Причем ННС служит также для подготовки исходных данных для моделирования.

Процесс функционирования ННС состоит из ряда этапов:

На первый вход сети подается показатель качества (ПК) функционирования ЦОД, а на второй вход мнения экспертов о корреляционных связях и значениях данного показателя. Затем в первом слое каждому терму входных переменных будут присваиваться степени принадлежностей входных значений ПК, ассоциированных с нейронами. Во втором слое каждый нейрон, образуя посылки нечетких правил, вычисляет уровень истинности правила. В третьем слое производится нормализация уровней истинности каждого правила. В четвертом слое выходы нейронов представляют произведение нормализованных значений уровней истинности на соответствующие выходы правил. В

последнем слое нейрон выходного слоя производит суммирование выходов нейронов предыдущего слоя и вырабатывает решение о предпочтительности включения данного ПК в систему показателей качества.

Таким образом, в соответствии с принятыми этапами комплексной оценки эффективности функционирования ЦОД первым шагом является синтез системы показателей качества процесса функционирования ЦОД.

Главным недостатком [4, 5] существующих подходов является то, что при их использовании не всегда формулируется глобальная система показателей качества. Редко делались попытки математически строго показать, каким образом из нее можно получить множество локальных СПК. Ни один из методов при определении состава СПК не учитывает наличие в комплексе нечеткости, неполноты и противоречивости информации как о ЦОД, так и знания, лица эксплуатирующего ЦОД. Все это снижало степень адекватности и полноты отражения в СПК всех существенных свойств дата центра.

Следующим этапом является разработка математической модели процесса функционирования ЦОД. С целью обеспечения совместного анализа различных по физическому смыслу и по классу случайных процессов, учета неопределенной информации о состояниях ПК, введены унифицированные модели отклонений ПК функционирования ЦОД на базе управляемых цепей Маркова в виде разностных стохастических уравнений, развитых для случая, когда состояния дата центра описаны нечетко, неполно и противоречиво. Ключевым элементом этой новой синтезированной модели – являются элементы МПВ, получаемые по-новому с одновременным, комплексным учетом нечеткой, неполной и противоречивой меры неопределенности о вероятностях перехода параметров (ПК) ЦОД из состояния в состояние.

С учетом особенностей предложенной системы показателей качества, случайного характера изменения большинства ПК, их нечеткого, неполного и противоречивого описания, и возможности решения в рамках выбранного подхода основных проблем комплексной оценки эффективности функционирования ЦОД.

На основе исходных данных и сформулированных требований к пороговым значениям отклонений нечеткого, неполного и противоречивого ПК, на каждом шаге функционирования ЦОД первоначально определяются безусловные по наблюдениям оценочные значения определяется безусловная по другим ПК вероятность выполнения требований к процессу данном шаге. С учетом этого, последовательно определяются условные вероятности для остальных ПК входящих в данную СПК. Затем, аналогично в обратном порядке и для этого же шага функционирования определяются составляющие условных вероятностей выполнения требований к остальным процессам и системам. Имея частные показатели эффективности на данном шаге функционирования ЦОД, формируется текущее значение обобщенного показателя эффективности на этом шаге, используя “свертку” текущих частных показателей эффективности функционирования на основе аппарата условных вероятностей.

Реализация модели СПК ЦОД на основе математического аппарата управляемых цепей Маркова, разностных уравнений сделала целесообразным применение в качестве аппарата текущего оценивания значений ПК методов фильтрации Калмана.

Заключение. Применение разработанной методики позволяет, в соответствии моделью оценки обоснованности, повысить точность принимаемых решений в 1,5 раза. Общий выигрыш в оперативности оценивания по сравнению с применением аппарата искусственных нейронных сетей, нечетких множеств и их совместного последовательного использования составляет до 12%.

СПИСОК ЛИТЕРАТУРЫ

1. Михайличенко Н. В. Сравнительный анализ технологий построения региональных центров обработки данных. // Юбилейная XV-ая Санкт-Петербургская международная конференция «Региональная информатика 2016», – СПб.: СПОИСУ, 2016. – 599 с., С.102-103.
2. Петухов Г.Б. Основы теории эффективности целенаправленных процессов. Ч.1. – М.: МО СССР, 1989. – 660 с.
3. Паращук И.Б. Вариант классификации процедур мониторинга в интересах синтеза систем контроля качества телекоммуникационных сетей // Приборы и Системы: Управление, Контроль, Диагностика. №5, 2003. С. 64-67.
4. Кузнецов В.П. Интервальные статистические модели. – М.: Радио и связь, 1991. 352 с.
5. Крюкова Е.С., Малофеев В.А., Паращук И.Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек // Новые информационные технологии и системы: сборник научных статей XVI Международной научно-технической конференции (г. Пенза, 27–29 ноября 2019 г.). – Пенза: Изд-во ПГУ, 2019. С. 177-180.
6. Маликов, А.В., Авраменко, В.С., Саенко, И.Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы, 2019, № 6. С.32–42.
7. Михайличенко, Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных // Системы управления, связи и безопасности. 2019. № 1. С.54-66.

УДК 025.2.004; 621.311.23: 629.12

ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Михайличенко Антон Валерьевич, Михайличенко Николай Валерьевич, Султанова Ясмина Маратовна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, katjuha777@inbox.ru

Аннотация. В работе проанализированы современные тенденции развития центров обработки данных. Определен широкий спектр услуг, предоставляемых пользователям дата-центров. Сформулированы ключевые виды неопределенности, влияющие на принятие решений в задачах оценки эффективности функционирования центров обработки данных. Предлагаемый подход основан на том, что синтез оптимальной системы показателей,

подлежащих наблюдению, оцениванию и прогнозированию, производится с учетом всего объема и номенклатуры услуг, которые должны быть предоставлены пользователю. Вследствие этого повышается достоверность контроля состояния ЦОД и обоснованность принимаемых решений по управлению параметрами и режимами его работы.

Ключевые слова: качество, эффективность, показатель, управление, центр обработки данных.

APPROACH TO EVALUATING THE PERFORMANCE OF DATA CENTERS

Mikhaylichenko Anton, Mikhaylichenko Nikolay, Sultanova Yasmina
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: 23esn2008@rambler.ru, katjuha777@inbox.ru

Abstract. The paper substantiates the relevance and objective need to improve the reliability of the analysis of the effectiveness of data processing centers in the interests of reasonable and operational management of the structure, parameters and modes of operation of such systems. Key types of uncertainty affecting decision-making in the tasks of evaluating the effectiveness of data processing centers are formulate. The proposed approach is because the synthesis of the optimal system of indicators to be monitored, evaluated and predicted is made taking into account the entire volume and range of services that should be provided to the user. This increases the reliability of data center status monitoring and the validity of decisions made to manage its parameters and operating modes.

Keywords: quality, efficiency, indicator, management, data center.

Введение. Современные дата-центры не очень похожи на мэйнфреймы. Это чудеса вычислительной техники, включающие современные серверы высокой производительности и революционные системы охлаждения. Они также предлагают широкий спектр услуг, предоставляя инфраструктурные ресурсы, которые были бы немыслимы в предыдущие десятилетия.

Центры обработки данных продолжают стимулировать инновации, чтобы предоставить своим клиентам лучшие и часто индивидуальные решения для их сетевых и вычислительных задач. Идя в ногу со временем тенденций, центр обработки данных может помочь компаниям определить какие услуги являются основными для них [1-3].

1. Услуги colocation.

Поскольку стоимость строительства частного центра обработки данных продолжает расти, а универсальность сторонних центров обработки данных расширяется, все больше компаний рассматривают colocation как идеальную услугу для своей ИТ-инфраструктуры. Важно помнить, что сегодняшние центры обработки данных полностью отличаются от старых хранилищ данных предыдущих десятилетий. Современный дата-центр является связующим звеном, предлагая организациям доступ почти ко всем цифровым услугам, которые только можно себе представить.

Colocation-это не только аренда производственных площадей, это также означает использование расширенных возможностей питания и охлаждения центров обработки данных для снижения текущих затрат на инфраструктуру. В большинстве случаев центры обработки данных предоставляют клиентам инструменты для управления и контроля своей инфраструктуры, которые намного превосходят все, что они могли бы позволить себе создать в своем собственном предприятии.

2. Технология виртуализации.

Возможно, самой главной тенденцией развития центров обработки данных за последнее десятилетие был широко распространенный толчок к программно-определяемым инфраструктурам. Вместо того, чтобы просто служить хранилищем данных, программно-определяемый центр обработки данных (SDDC) виртуализирует вычислительную и запоминающую мощности, доступные через свои серверы в виде программного обеспечения, которое затем поставляется в комплекте и продается клиентам в качестве услуги. Этот процесс позволяет нескольким пользователям устанавливать и управлять своими собственными службами на одном физическом сервере. Каждый виртуализированный сервер отделен от других, обеспечивая как конфиденциальность, так и гибкость. Поскольку клиенты приобретают виртуализированные активы в программно-определяемой инфраструктуре, невероятно легко масштабировать их в соответствии со своими потребностями или перемещать их, чтобы воспользоваться преимуществами комплексных услуг центра обработки данных.

Виртуализация серверов и контейнеризация оказали огромное влияние на эффективность работы центров обработки данных. Программно-определяемые инфраструктуры позволяют предприятиям предлагать услуги по низким ценам, а также минимизируют требования к мощности и охлаждению. Серверы высокой плотности, работающие под управлением больших виртуализированных рабочих нагрузок, могут потреблять много электроэнергии и генерировать много тепла, но гораздо эффективнее размещать несколько клиентов на одном сервере высокой плотности, чем на нескольких блоках с более низкой плотностью. Эти средства экономии могут быть переданы клиентам, что позволит им инвестировать в дополнительные услуги за пределами серверного пространства.

3. Гибридные ИТ-услуги.

Облачные вычисления являются одной из наиболее значимых тенденций следующего поколения центров обработки данных. Когда облачные сервисы впервые стали доступны многие компании перенесли все свои мощности в облако. Это хорошо сработало для некоторых из них, другие компании обнаружили, что проблемы безопасности и неожиданные расходы на работу в чисто публичной облачной среде не имеют смысла. Некоторые компании предпочли полностью уйти из облака, перейдя вместо этого в решение для совместного размещения или воспользовавшись программно-определяемой инфраструктурой центра обработки данных для создания частного облака на виртуализированных серверах.

Но некоторые компании все еще нуждаются в услугах публичного облака. Отвечая этой потребности, центры обработки данных разработали гибридную облачную архитектуру и мульти-облачные решения, которые позволяют компаниям использовать преимущества мощности публичных облачных вычислений, в то же время наслаждаясь безопасностью и контролем частной сети. Гибридная облачная архитектура хранит конфиденциальные и ценные данные в частной сети, а также устанавливает соединения с общедоступной облачной службой. Эта архитектура позволяет компаниям защищать и контролировать свои данные, все еще используя их в общедоступной облачной среде.

4. Гипермасштабируемые центры обработки данных.

По мере того как все больше организаций обращаются к облачным вычислительным решениям, спрос на инфраструктуру центров обработки данных, которая их поддерживает, также растет. Гипермасштабируемые объекты значительно больше, чем большинство корпоративных центров обработки данных, иногда вмещающих тысячи и тысячи серверов. Поскольку спрос на облачные и социальные медиа-сервисы не показывает никаких признаков снижения, компании инвестируют в строительство еще большего количества этих массовых объектов.

5. Инновационная технология охлаждения.

Центры обработки данных уже давно полагаются на обычную инфраструктуру кондиционирования воздуха для удовлетворения своих потребностей в охлаждении. Учитывая, что охлаждение отвечает за огромный процент потребления энергии в центре обработки данных, неудивительно, что многие объекты сосредоточились на улучшении своих стратегий охлаждения как способ стать более эффективными. Энергоемкие процессоры, необходимые для питания современных приложений искусственного интеллекта, также генерируют больше тепла, чем может обрабатывать традиционная инфраструктура охлаждения, заставляя центры обработки данных принимать новые подходы для удовлетворения своих потребностей в охлаждении.

6. Искусственный интеллект.

Как искусственный интеллект, так и более специализированные приложения машинного обучения получили широкое распространение в последние годы [4]. Проблема для многих организаций заключается в обеспечении огромного объема вычислительной мощности, необходимой для этих приложений. При использовании сложных адаптивных алгоритмов для решения задач, которые когда-то считались тривиальными, спрос на вычислительную мощность будет продолжать расти.

7. Инновации в технологии хранения данных.

Между падением стоимости твердотельных накопителей (SDDs) и развитием новых технологий, таких как кристаллы памяти, организации инвестируют значительные средства в ресурсы хранения, необходимые для размещения массивного накопления данных, генерируемых по сегодняшним сетям. Только данные социальных сетей вынудили компании пересмотреть свои стратегии больших данных в последние годы, и распространение сетей 5G и устройств IoT, несомненно, произведет еще больше данных, которые нужно где-то хранить.

Заключение. Современные тенденции развития центров обработки данных существенно изменили отрасль. Там, где центры обработки данных когда-то были исключительной заботой крупных компаний, сегодня они предоставляют более мелкие организации с возможностью предоставления продуктов и услуг более эффективно, чем когда-либо прежде. Поскольку технологии центров обработки данных продолжают развиваться, то эти тенденции, безусловно, уступят место еще более современным разработкам.

СПИСОК ЛИТЕРАТУРЫ

1. Михайличенко Н. В. Сравнительный анализ технологий построения региональных центров обработки данных. // Юбилейная XV-ая Санкт-Петербургская международная конференция «Региональная информатика 2016», – СПб.: СПОИСУ, 2016. – 599 с., С.102-103.
2. Паращук И.Б. Вариант классификации процедур мониторинга в интересах синтеза систем контроля качества телекоммуникационных сетей // Приборы и Системы: Управление, Контроль, Диагностика. №5, 2003. С. 64-67.
3. Крюкова Е.С., Малофеев В.А., Паращук И.Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек // Новые информационные технологии и системы: сборник научных статей XVI Международной научно-технической конференции (г. Пенза, 27–29 ноября 2019 г.). – Пенза: Изд-во ПГУ, 2019. С. 177-180.
4. Михайличенко Н.В., Паращук И.Б. Безопасность киберфизических систем типа «умная логистика» для автоматизированного управления снабжением // Наукоемкие технологии в космических исследованиях Земли. 2019. Т.11. №5. С. 32-38.

УДК 621.311.23; 629.12

МОДЕЛЬ СТАЦИОНАРНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Носов Алексей Олегович, Житков Александр Павлович, Сазонов Виктор Викторович, Файзулин Вадим Вячеславович

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mails: 11199111@mail.ru, alexzm55@gmail.com, vmktor-sazonov@yandex.ru, vadim.fsizulin@gmail.com

Аннотация. Разработана имитационная модель стационарной сети передачи данных построенная на объектах комплексного оснащения. Средой имитационного моделирования выбран симулятор сети передачи данных Cisco Packet Tracert позволивший разработать физическую и логическую структуру стационарной сети передачи данных с учётом обоснованных ограничений в условиях функционирования.

Ключевые слова: объект комплексного оснащения, межсетевой экран, маршрутизатор, коммутатор, автоматизированное рабочее место, сервер.

STATIONARY DATA NETWORK MODEL

Alexey Nosov, Alexander Zhitkov, Viktor Sazonov, Vadim Fayzullin

Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mails: 11199111@mail.ru, alexzm55@gmail.com, vmktor-sazonov@yandex.ru, vadim.fsizulin@gmail.com

Abstract. A simulation model of a stationary data transmission network built on objects of complex equipment has been developed. The simulation environment is the Cisco Packet Tracert data network simulator, which allows us to develop the physical and logical structure of a stationary data network, taking into account reasonable restrictions in the operating conditions.

Keywords: complex equipment object, firewall, router, switch, automated workplace, server.

Введение.

В настоящее время существующие методы исследований сетей передачи данных специального назначения (СПД СН) имеют следующие недостатки:

- проведение измерений, а также анализ их результатов занимают продолжительное время;
- необходимо привлекать опытных специалистов (администраторов и операторов);
- невозможность в большинстве случаев проведения экспериментов без нарушения режима эксплуатации.

Одним из наиболее эффективных методов исследования, снижающих вышеуказанные недостатки, является имитационное моделирование, сущность которого заключается в имитации процессов функционирования СПД СН [1-5].

Анализ средств имитационного моделирования показывает, что наиболее удобным средством моделирования СПД СН является Cisco Packet Tracer которое позволяет экспериментировать с поведением сети, настраивая её под поставленные задачи, и создавать сеть с большим числом оборудования.

Разработанная модели стационарной СПД СН построена на распределенной сети доступа, состоящую из пяти объектов комплексного оснащения (ОКО), каждый из которых включает средство доступа к сети оператора связи, коммутатор локальной сети с абонентами открытого сегмента, криптомаршрутизатор с межсетевым экраном, коммутатором и абонентскими средства локальной сети закрытого сегмента.

Таким образом, нам потребовалось: 15 маршрутизаторов (5 маршрутизаторов доступа с 2 интерфейсами FastEthernet каждый; 5 криптомаршрутизаторов с 2 интерфейсами FastEthernet каждый; 5 маршрутизаторов Единой сети электросвязи (ЕСЭ) с 4 интерфейсами GigabitEthernet каждый для связи между собой и 1 интерфейсом FastEthernet для связи с подсетью); 10 коммутаторов (поддерживающие сеть FastEthernet на кабеле типа - витая пара); по 1 сетевой карте на каждую рабочую станцию и сервера (36 сетевых карт стандарта FastEthernet); оптоволоконный кабель в количестве 12 км; витая пара в количестве, необходимом для развертывания СПД СН состоящую из пяти ОКО.

Заключение. В докладе рассматриваются вопросы построения имитационной модели работы СПД СН (на первом этапе разработана обобщенная структура; на втором этапе произведен анализ функционирования составных элементов данной системы и сделаны выводы о степени адекватности разработанной модели).

СПИСОК ЛИТЕРАТУРЫ

1. Иванов В.Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи: Монография/ В.Г. Иванов. – СПб.: ПОЛИТЕХ-ПРЕСС, 2018. – 214с.
2. Инфокоммуникационные системы специального назначения. Учебное пособие / Под ред. С.М. Одоевского. – СПб.: ВАС, 2016. – 456 с.
3. https://www.intuit.ru/studies/courses/3549/791/lecture/29211.
4. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В.Г. Олифер, Н.А. Олифер. СПб.: Питер, 2011. – 943 с.
5. Основы передачи данных: Учебник / Под ред. Проф. И.Б. Паращука. – СПб.: ВАС, 2015 – 216 с.

УДК 623.611

ОПТИМИЗАЦИЯ АЛГОРИТМОВ МНОЖЕСТВЕННОГО ДОСТУПА В САМООРГАНИЗУЮЩЕЙСЯ СЕТИ РАДИОСВЯЗИ ДЕКАМЕТРОВОГО ДИАПАЗОНА

Панин Роман Сергеевич[1], Путилин Алексей Николаевич[2]
[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
[2] ПАО «Информационные телекоммуникационные технологии («Интелтех»)
Кантемировская ул., 8, Санкт-Петербург, 197342, Россия
e-mails: paninrs@yandex.ru, a.n.putilin@yandex.ru

Аннотация. Рассматривается задача оптимизации алгоритма множественного доступа в самоорганизующейся декаметровой радиосети. Основным отличием от традиционных задач является необходимость учёта в этом случае ее анизотропности. Предложен подход к решению задачи параметрического синтеза системы множественного доступа в самоорганизующихся сетях связи.

Ключевые слова: самоорганизующиеся сети связи; множественный доступ; декаметровый диапазон; система передачи данных, пакетная сеть радиосвязи.

OPTIMIZATION OF MULTIPLE ACCESS ALGORITHMS IN A DECAMETER SELF-ORGANIZING RADIO NETWORK

Panin Roman[1], Putilin Alexey[2]
[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
[2] JSC «INTELTECH»
8 Kantemirovskay St, St. Petersburg, 197342, Russia
e-mails: paninrs@yandex.ru, a.n.putilin@yandex.ru

Abstract. The problem of optimizing the multiple access algorithm in a self-organizing decameter radio network is considered. The main difference from traditional problems is the need to take into account its anisotropy in this case. An approach to solving the problem of parametric synthesis of a multiple access system in self-organizing communication networks is proposed.

Keywords: self-organizing communication networks; multiple access; decameter range; data transmission system, packet radio network.

Введение. В настоящее время растет интерес к беспроводным децентрализованным самоорганизующимся сетям связи (ССС или MANET – Mobile Ad hoc Network). Использование на принципах множественного доступа группы выделенных радиоканалов обеспечивает ССС устойчивость к изменениям инфраструктуры сети, устойчивость к изменению помеховой обстановки, простоту и высокую скорость развертывания. Эти преимущества указывают на несомненный интерес данной технологии для систем управления критическими структурами. В настоящее время предложены ряд стандартов для реализации ССС в гигагерцовых диапазонах. Однако ареал покрытия таких сетей не превышает сотен метров. Использование для критических структур требует перехода в диапазоны, обеспечивающие обмен данными на тысячи километров. Этому требованию отвечают диапазоны, находящиеся ниже 30 МГц. Среди них наибольшей информационной ёмкостью обладает декаметровый диапазон.

Однако в отличие от гигагерцовых диапазонов в данном диапазоне наиболее ярко проявляется анизотропия выделяемых для организации сети радиоканалов как по их частоте, так и по направлению передачи. Пригодный для передачи данных в одном направлении радиоканал может оказаться совершенно непригодным для другого направления. Острота данной проблемы снижается при использовании всеми станциями сети сигналов последовательным расширением спектра, то есть систем радиосвязи с псевдослучайным переключением рабочих частот. Вероятность наличия для любого направления связи пригодного радиоканала растет с увеличением числа используемых радиоканалов. С другой стороны, увеличение этого числа выше потребностей ССС, определяемых входной нагрузкой, приводит к нерациональному использованию частотного ресурса, к простою радиоканалов.

Реализация ССС в декаметровом диапазоне невозможна без выбора оптимального числа коллективно используемых ССС радиоканалов, их подбора на основе априорного знания их пригодности по направлениям связи, а также определения оптимальных параметров алгоритма доступа к ним. Данная работа предлагает подход к формулировке данной задачи оптимизации и определению принципов построения математической модели рассматриваемой системы радиосвязи.

Структура сети определяется следующими параметрами. В сети имеется S абонентов (радиостанций). В соответствии со схемой организации связи (СхОС) в сети Dd - направлений передачи данных. Все каналы имеют одинаковую скорость передачи R. Передаваемые пакеты имеют длину Lp. Скорость передачи в пакетах Sp=R/Lp. Пакет передается в одном временном слоте, поэтому время в сети дискретно по слотам передачи. Время слота Ts=1/Sp. Коэффициент связности сети

C=2*Dd/(S(S-1)), 0≤C≤1, где S(S-1)/2 – максимальное количество каналов в сети, когда каждый связан с каждым. Таким образом, множеством параметров описывающих структуру сети определяется как α=(S,Dd,Sp,Lp).

Среда передачи описывается следующими параметрами. В ССС разрешено использование Fc радиоканалов, находящихся в разных участках декаметрового диапазона [1]. Ионосферно-волновой и частотно-диспетчерской службой (ИВ ЧДС) до начала функционирования ССС, априорно определена матрица вероятностей установления соединения в направлении передачи данных d в радиоканале f – P(d,f), где d∈{1,Dd}, f∈{1,Fc}. Из множества FB выбранных частот вследствие воздействия преднамеренных или системных помех может оказаться непригодными для всех информационных направления до Fj радиоканалов [2]. Таким образом, среда передачи описывается множеством параметров δ=(Fc,P,Fj).

Следует определить четыре возможных типа матриц P(d,f).

Тип 1: радиосеть изотропна по направлениям и радиоканалам. P(d,f)=P* для всех d и f. Ситуация типична для работы радиосети с антеннами зенитного излучения (NVIS – Near Vertical Incidence Skywave propagation) на дальность до 300 км на частотах 2...8 МГц или для работы радиосети при отсутствии прогноза по оценке качества радиоканалов: отсутствие службы ИВ ЧДС или отсутствие возможности достоверного прогноза вследствие чрезвычайных условий.

Тип 2: радиосеть изотропна по направлениям и анизотропна по частотам. P(d,f)=P(f) для всех d. Ситуация типична для работы сети из двух групп абонентов, имеющих локальные области расположения в которых они связаны между собой альтернативными каналами: провод, оптоволокно, УКВ и проч. Типичный примеры: взаимодействие двух АСУ, разделенных в пространстве.

Тип 3: радиосеть изотропна по частотам и анизотропна по направлениям. P(d,f)=P(d) для всех f. Это разновидность радиосети типа 1 при наличии сосредоточенных по направлениям помех искусственного или естественного происхождения.

Тип 4: сеть анизотропна по направлениям и частотам. Общий случай. Степень анизотропии существенно влияет на эффективность функционирования сети. Гипотетически возможны варианты фрагментации сети на несколько независимых подсетей или направлений радиосвязи: для различных групп направлений связи все рабочие частоты различны.

Поступающая в сеть нагрузка определяется следующими параметрами. Среднее число пакетов, поступающих в сеть в единицу времени (слот) 0≤Ap≤Dd, нормированное число пакетов 0≤λ≤1, где λ=Ap/Dd. Поток пакетов стохастический без памяти, направление передачи данных в которое поступает пакет выбирается случайно. Закон распределения времени между возникновением пакетов – геометрический. Требуемое время доставки пакета в сети – Td. Требуемая вероятность доставки пакета в сети – Pr. Множеством параметров, описывающих нагрузку в сети определяется как β=(Ap,Am,Td,Pr).

Используется алгоритм множественного доступа с контролем занятости (МДКЗ, см. [3]). Он определяется следующими параметрами. Количество используемых радиоканалов Fb. Из множества возможных радиоканалов FS выбирается подмножество FB. Вероятность использования свободного канала при возникновении заявки на установление соединения Pu. Таким образом, множество параметров алгоритма множественного доступа есть γ=(Fb,FB,Pu). Эти параметры являются предметом оптимизации.

Для оценки эффективности функционирования ССС представляется достаточным использование следующих показателей качества.

1. Вероятность своевременной доставки пакета в направлении за требуемое время Pd(α,β,γ,δ)=Pf(β)*Pc(α,β,γ,δ), где

Pf(β) - вероятность наличия свободного канала при возникновении заявки за требуемое время,

Pc(α,β,γ,δ) - вероятность установления соединения в направлении.

2. Производительность сети Pn(α,β,γ,δ).

В соответствии с методом выбора доминирующего показателя качества наиболее обоснованным представляется выбор производительности сети в качестве показателя эффективности функционирования системы множественного доступа ССС при ограничении на вероятность своевременной доставки пакета:

$$\mathrm{Pn}(\mathrm{Dd},\mathrm{FS},\mathrm{FB}) = \frac{1}{Dd}\max_{0\le\lambda\le 1}\sum_{d=1}^{Dd}\frac{1}{\mathrm{V}(\alpha,\delta)\mathrm{Tm}(\alpha,\beta,\gamma,\delta)},$$ где

Tm(α,β,γ,δ) – среднее время доставки пакета в направлении d на стартовых каналах FB,

V(α,δ) – скорость передачи в направлении d на выбранных частотах.

Задача оптимизации параметров системы множественного доступа ССС (задача синтеза) состоит в определении:

$$\gamma^* = \arg\max_{\gamma\in Y}\mathrm{Pn}(\alpha,\beta,\gamma,\delta)$$ при условии, что Pd(α,β,γ,δ)≥ Pd для всех d.

Заключение. Предложенный подход позволяет построить формализованную модель, направленную на решение задачи параметрического синтеза системы множественного доступа в ССС. Он разделяет группы параметров, описывающих структуру сети, среду передачи, поступающую нагрузку и, собственно, алгоритм множественного доступа. Это позволяет при необходимости выполнить независимую корректировку исходных данных по любой из названных четырех составных частей. Представлена формулировка задач анализа и синтеза рассматриваемой системы связи, которая является методической основой для построения математической модели функционирования и разработки методики оптимизации параметров системы множественного доступа в ССС.

СПИСОК ЛИТЕРАТУРЫ

1. Recommendation ITU-R F.1487 Testing of HF modems with bandwidths of up to about 12 kHz using ionosfpheric cannel simulators, 2000: [Электронный ресурс]. URL: https://www.itu.int
2. Путилин А.Н. Модель взаимодействия линии радиосвязи и станции радиоэлектронного подавления // Доклад на конф. «Региональная информатика 2012», 24-26 октября 2012 г. – СПб.: СПОИСУ, 2012.
3. Бунин С.Г., Войтер А.П. Вычислительные сети с пакетной радиосвязью - Киев: Тэхника, 1989.- 129 с.

УДК 681.324

ПРОЕКТИРОВАНИЕ И МОДЕЛИРОВАНИЕ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Пантюхин Олег Игоревич, Ковалёв Игорь Станиславович, Солодухин Борис Владимирович, Юдин Анатолий Алексеевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: p_oleg99@mail.ru, iskova@mail.ru, boris.soloduxin@yandex.ru, ytol5@mail.ru

Аннотация. В современных системах управления специального назначения разворачиваются сложные системы связи и автоматизации, средствами которых оборудуются пункты управления. При этом центры обработки данных (ЦОД) являются основой системы автоматизации. Именно от качества их функционирования будет зависеть оперативность, надёжность и достоверность принятия решений органами управления.

Ключевые слова: центр обработки данных; проектирование; имитационное моделирование.

DESIGN AND SIMULATION OF SPECIAL-PURPOSE DATA CENTERS

Pantyukhin Oleg, Kovalev Igor, Solodukhin Boris, Yudin Anatoly

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: p_oleg99@mail.ru, iskova@mail.ru, boris.soloduxin@yandex.ru, ytol5@mail.ru

Abstract. In modern special-purpose control systems, complex communication and automation systems are deployed, with the means of which control points are equipped. At the same time, data centers (DC) are the basis of the automation system. It is the quality of their functioning that will determine the efficiency, reliability and reliability of decision-making by management bodies.

Keywords: data center; design; simulation modeling.

Введение. Современные ЦОД являются, в сущности, ядром информационно-телекоммуникационной инфраструктуры сложных организационно-технических систем. Они представляют собой комплекс инженерной инфраструктуры, программных и аппаратных средств, организационных процедур и человеческих ресурсов. Центры предназначены для приёма, хранения, обработки и предоставления данных должностным лицам (ДЛ) сложных организационно-технических систем с требуемым уровнем качества. ЦОД содержат высоконадежное серверное оборудование, системы хранения и передачи данных, программное обеспечение, архитектурно-технические решения, обеспечивающую инженерную инфраструктуру, физическую защиту помещений, комплекс организационных мероприятий, а также систему мониторинга и управления [1]. Потребность в проектировании ЦОД возникает при следующих условиях: значительном росте информационных потоков; увеличении количества потребителей информации; большой удаленности потребителей информации.

К преимуществам ЦОД необходимо отнести: отказоустойчивость и надёжность системы автоматизации; высокий уровень защиты информации; возможность оптимизации информационных процессов; централизованное управление и улучшение контроля; гибкость и масштабируемость системы; снижение стоимости эксплуатации ИТ-структуры.

К основными компонентам ЦОД относятся:

– сетевая инфраструктура или локальная вычислительная сеть (ЛВС), которая объединяет серверы и системы хранения данных ЦОД, обеспечивает внешние подключения к автоматизированным рабочим местам (АРМ) или ЭВМ конечных пользователей;

– инфраструктура хранения, предоставляющая массивы хранения данных (базы данных) ЦОД;

– вычислительные ресурсы, то есть серверы, поддерживающие работу приложений ЦОД. Эти серверы предоставляют ресурсы памяти и место в локальном хранилище, выполняют обработку приложений и обеспечивают их подключение к сети;

– вспомогательные службы.

Проектирование ЦОД, как и проектирование крупных автоматизированных систем управления (АС), предполагает выполнение ряда стадий, содержащих, в свою очередь, набор конкретных задач, нацеленных на создание центров с высоким качеством обслуживания [1]. В нашей стране разработана система стандартов, определяющих содержание, состав исполнителей и порядок выполнения работ на разных этапах проектирования, а также порядок их приёмки. Государственный стандарт ГОСТ 34.601-90, например, содержит нормативные требования к содержанию стадий и задач проектирования автоматизированных систем, предназначенных для

обеспечения различных видов деятельности (управление, проектирование, исследование и т.п.), включая их сочетания. Он предусматривает следующие стадии и задачи проектирования: формирование требований к ЦОД, разработка концепции, техническое задание на создание ЦОД, эскизный и технический проект построения ЦОД, разработка рабочей документации, ввод в действие и сопровождения ЦОД.

При предпроектном обследовании объекта, в рамках которого будет функционировать ЦОД сложной организационно-технической системы, производится: сбор и обработка сведений об этой инфраструктуре (системе), особенностях её функционирования, включая данные о её взаимодействии с внешней средой и другими системами, а также выполнение процедур системного анализа и моделирования, разработка технико-экономического обоснования целесообразности создания ЦОД, выработка общих требований на его разработку и другие работы [1].

Одним из основных свойств и показателей качества функционирования ЦОД является их оперативность, так как именно она комплексно отражает их целевое предназначение и учитывает влияние внутренних и внешних дестабилизирующих факторов. К внутренним относятся конечная надежность средств вычислительной техники (вероятность отказа) и ошибочные действия ДЛ (вероятность ошибки), а к внешним, например, дестабилизирующее влияние вредоносного программного обеспечения [2].

От оперативности и надёжности обработки информации во многих АС зависит построение информационных процессов и уровень оказания услуг потребителям.

Под информационным процессом при решении задач в автоматизированных системах понимается согласованная по месту, времени и целям совокупность подпроцессов подготовки и ввода данных, проверки их на достоверность, классификации, обобщения и группирования, а также хранения поступающей информации, поиска и выдачи данных в форме, необходимой для использования при принятии решений, решении задач различных типов по функциям управления, оформления результатов в виде документов, команд или сигналов, их доведения до взаимодействующих объектов АС [3].

Хранение введённых в АС данных осуществляется при реализации подпроцесса хранения информации. При этом данные размещаются в базе данных, как правило, распределенной, обеспечивая тем самым: надёжность, безизбыточность, целостность и непротиворечивость хранения данных; достоверность и безопасность данных; возможность манипулирования данными (чтение, запись, изменение, удаление).

При проектировании и исследовании автоматизированных систем и комплексов средств автоматизации широко применяется имитационное моделирование с применением ЭВМ [2]. Для повышения эффективности процесса моделирования применяются специализированные средства и языки имитационного моделирования, ориентированные на конкретные объекты исследования. При моделировании АС для расчёта значений вероятностно-временных показателей оперативности и надёжности эти системы сводятся к системам и сетям массового обслуживания (СМО, СеМО). Наиболее приспособленным средствами описания СМО являются такие инструментальные средства, как GPSS-World, AnyLogic.

Целью имитационного моделирования является получение приближённых знаний об объекте, не производя непосредственное измерение значений его параметров. Понятно, что это необходимо только тогда, когда измерение невозможно, или оно стоит дороже проведения имитации. При этом результаты будут определяться случайным характером процессов. По этим данным можно получить достаточно устойчивую статистику. Имитационное моделирование можно рассматривать как разновидность экспериментальных испытаний. На основе результатов анализа информационных потребностей ДЛ АС, сделан выбор в сторону имитационного моделирования и теории массового обслуживания. Основными этапами методики оценки оперативности ЦОД являются [2-5]:

- оценка информационной потребности пользователей при использовании ЦОД;
- разработка модели оценки оперативности;
- собственно, моделирование с учетом воздействия внутренних и внешних дестабилизирующих факторов.

Ядром методики является имитационная модель оценки оперативности, позволяющая определить показатель оперативности обработки сообщений, циркулирующих в АС с ЦОД и сравнить его значения с требуемыми.

Заключение. Большинство компонентов АС имеет сложную структуру и характеризуется многообразием связей между элементами. В качестве компонентов можно привести персональные ЭВМ, автоматизированные рабочие места должностных лиц, центры обработки данных, комплексы средств автоматизации, компьютерные сети (сети передачи данных) и др.

Возвращаясь к примеру, с ЦОД и подключёнными к нему АРМ, можно показать, что пользователи и их АРМ выступают в роли источников потока запросов на выполнение задач (заявок) на серверах баз данных ЦОД. Заявки, поступающие в случайные моменты времени, образуют входной поток заявок. АРМ, каналы передачи данных и сервера ЦОД интерпретируются обслуживающими приборами. Заявки, которые не могут быть приняты к обслуживанию, образуют очередь. Результаты решения задач формируются в выходной поток заявок. Результатом исследования, как правило, выступают временные характеристики процесса пребывания заявки в отдельных СМО и сети в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Бородко А.В., Пантюхин О.И. Анализ содержания типовых стадий и задач проектирования современных центров обработки данных специального назначения // В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды IV межвузовской научно-практической конференции. СПб.: ВАС, 2019. С. 127-131.

2. Борец Д.В., Ковалёв И.С., Малышев В.С., Пантюхин О.И. Оценка оперативности локальной вычислительной сети пункта управления силового ведомства // Информационная безопасность регионов России (ИБРР-2017). Материалы юбилейной X межрегиональной конференции. 1-3 нояб. 2017г. СПОИСУ. – СПб, 2017. С.52-53.
3. Овсянников С.Н., Пантюхин О.И., Хмелевской В.П. Организация информационного процесса в системе автоматизации управления связью. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). Сборник научных статей VI Международная научно-техническая и научно-методическая конференция: сб.науч.ст. в 4-х т. СПб.: СПбГУТ, 2017: т.1. С.502-507.
4. Михайличенко Н. В. Сравнительный анализ технологий построения региональных центров обработки данных. // Юбилейная XV-ая Санкт-Петербургская международная конференция «Региональная информатика 2016», – СПб.: СПОИСУ, 2016. – 599 с., С.102-103.
5. Паращук И.Б. Вариант классификации процедур мониторинга в интересах синтеза систем контроля качества телекоммуникационных сетей // Приборы и Системы: Управление, Контроль, Диагностика. №5, 2003. С. 64-67.

УДК 004.942

ПРОГРАММНЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК: ВОПРОСЫ ТЕХНИКО-ЭКОНОМИЧЕСКОЙ ОЦЕНКИ КОНКУРЕНТНЫХ АНАЛОГОВ, ПОТЕНЦИАЛА РАЗВИТИЯ И ПРИМЕНЕНИЯ

Паращук Игорь Борисович[1], Виткова Лидия Андреевна[2], Малофеев Валерий Александрович[1]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН),
14-я линия ВО, 39, Санкт-Петербург, 194064, Россия,
e-mails: shchuk@rambler.ru, vitkova@comsec.spb.ru, valeron12.1366@gmail.com

Аннотация. Выполнен обзор и анализ современных зарубежных и отечественных программных средств, предназначенных для решения задач выявления сетевых атак. Для решения задачи выявления сетевых атак описан новый программный продукт, сочетающий в себе различные подходы к построению комплексного механизма выявления отклонений в эвристиках трафика сверхвысоких объемов. Произведена оценка трудозатрат на создание коммерческой версии программного продукта, выделены направления и перспективы развития таких средств и основные преимущества от их внедрения в структуру сетевой безопасности организации.

Ключевые слова: технико-экономическая оценка, потенциал, сетевая атака, система обнаружения, защита, программный продукт, отклонения, эвристика, объем трафика, трудозатраты, ресурсы.

SOFTWARE SYSTEMS FOR DETECTING NETWORK ATTACKS: ISSUES OF TECHNICAL AND ECONOMIC EVALUATION OF COMPETITIVE ANALOGUES, POTENTIAL of DEVELOPMENT AND APPLICATION

Parashchuk Igor[1], Vitkova Lydia[2], Malofeev Valery[1]

[1] Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia

[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)
39, 14-th Linia, VI, St. Petersburg, 199178, Russia
e-mails: shchuk@rambler.ru, vitkova@comsec.spb.ru, valeron12.1366@gmail.com

Abstract. A review and analysis of modern foreign and domestic software tools designed to solve the problems of identifying network attacks is performed. To solve the problem of detecting network attacks, a new software product is described that combines various approaches to constructing an integrated mechanism for detecting deviations in heuristics of ultra-high volume traffic. The labor costs for creating a commercial version of the software product are estimated, directions and prospects for the development of such tools and the main advantages from their implementation in the network security structure of the organization are highlighted.

Keywords: technical and economic evaluation, potential, network attack, detection system, protection, software product, deviations, heuristics, traffic volume, labor costs, resources.

Введение. Важным элементом опытно-конструкторских работ является технико-экономическая оценка рыночного потенциала результатов этих изысканий. Особое место сегодня занимают проекты, направленные на разработку эффективных методов обнаружения и защиты от сетевых атак. Проблеме создания программных систем обнаружения и защиты нового поколения, способных предотвратить проведение сетевых атак на ранних стадиях, уделяется сегодня много внимания [1-3]. Создан экспериментальный образец (прототип) программного обеспечения (ПО) для обнаружения сетевых атак и защиты от них на основе выявления отклонений в эвристиках трафика сверхвысоких объемов. С точки зрения технико-экономической оценки рыночного потенциала созданного экспериментального образца (прототипа) ПО необходимо проанализировать характеристики конкурентных аналогов. Среди прямых конкурентов разработанного экспериментального образца (прототипа) ПО для обнаружения сетевых атак, можно выделить некоторые наиболее распространенные зарубежные и отечественные программные продукты, в составе которых решаются подобные задачи. Рассмотрим часть из них.

Система обнаружения атак RealSecure представляет собой комплексное программное обеспечение, разработанное компанией Internet Security Systems (США), которое осуществляет выявление отклонений в эвристиках трафика на основе применения сетевых и системных модулей слежения [4]. Это интеллектуальный

анализатор пакетов с расширенной базой сигнатур атак, который позволяет обнаруживать враждебную деятельность и распознавать атаки на узлы телекоммуникационной и/или вычислительной сети. Программное обеспечение BlackICE и ICEcap производства компании Network ICE (США) – комплекс средств мониторинга сетевого трафика и выдачи предупреждающих сообщений. При этом BlackICE – специализированное приложение-агент, которое предназначено исключительно для выявления злоумышленников [5, 6]. Программный комплекс Intruder Alert [7, 8] корпорации Symantec (США) больше похож на инструментарий для специалистов в области информационной безопасности, поскольку он предоставляет максимальную гибкость в определении стратегий защиты сети. Инструментарий детектирования сетевых атак – программный пакет Centrax производства компании CyberSafe устроен по принципу «все в одном», в его составе есть средства контроля за системой безопасности, мониторинга трафика, выявления атак и выдачи предупреждающих сообщений [9, 10]. Анализатор трафика eTrust Intrusion Detection [11, 12] разработан корпорацией Computer Associates (США), он способен осуществлять функции контроля за информационной безопасностью и функции управления стратегиями защиты, в этом продукте реализованы средства выдачи предупреждений в режиме реального времени, шифрования данных и обнаружения атак. Программный продукт PT Network Attack Discovery (PT NAD) от российской компании Positive Technologies [13] – система глубокого анализа сетевого трафика для выявления атак на периметре и внутри сети. Система ViPNet Personal Firewall [14] от компании ИнфоТеКС – это программный сетевой экран для контроля и управления трафиком рабочих мест и серверов.

Все описанные выше программные системы предоставляют возможность анализа, мониторинга и оценки не очень больших объемов данных, относящихся к обнаружению сетевых атак и защите от них, характеризуются жестко задаваемой структурой для выявления отклонений в трафике. Как правило, такие системы используют упрощенные алгоритмы обработки трафика, базы данных сигнатур атак на основе простых реляционных моделей и не предлагают выбор контрмер для защиты от сетевых атак. В отличие от этих программ, разработана перспективная программная система, объединяющей в себе различные подходы к обнаружению сетевых атак на базе биоинспирированных подходов при выявлении отклонений в эвристиках трафика сверхвысоких объемов, методы аналитического моделирования, машинного обучения, обнаружения сигнатур и обеспечивающая высокую достоверность, оперативность и адаптивность выявления сетевых атак, а также выбор контрмер для защиты от них.

При этом выполняются все основные показатели качества, традиционно предъявляемые к программным продуктам: надежность, практичность, эффективность, сопровождаемость и мобильность. Помимо исследования характеристик конкурентных аналогов и описания собственного программного продукта, в рамках технико-экономическая оценки рыночного потенциала результатов изысканий и проектов проведены оценка трудозатрат на создание этого нового программного продукта, а также анализ технических и научных перспектив его применения и анализ ожидаемых преимуществ его использования. Оценка трудозатрат вычислялась с использованием промежуточной модели COCOMO II (Constructive Cost Model) [15].

Заключение. Таким образом, проведена технико-экономическая оценка потенциала новой программной системы обнаружению сетевых атак и защиты от них, выполнен обзор конкурентных программных средств, предназначенных для решения задач выявления сетевых атак и защиты от них в сетях с высоким объемом трафика. Существует новой программный продукт, сочетающий в себе механизмы выявления отклонений в эвристиках трафика сверхвысоких объемов, обладающий большей оперативностью, гибкостью и требующий меньших вычислительных ресурсов и ресурсов памяти. Произведена оценка трудозатрат на создание коммерческой версии программного продукта, выделены направления и перспективы развития таких средств и основные преимущества от их внедрения в структуру сетевой безопасности организации.

Исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В.С., Маликов А.В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // Региональная информатика и информационная безопасность. Выпуск 4. . – СПб.: СПОИСУ, 2017. – 533 с., С. 24-26.
2. Паращук И.Б., Михайличенко Н.В., Шестаков Е.О. Анализ направлений, методов и средств технического обеспечения комплексной защиты систем хранения данных // IV Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Труды конференции. Том 1. – СПб: ВАС, 2019. С. 333-337.
3. Михайличенко Н.В. Проблемы и перспективы обеспечения безопасности центров обработки данных // Региональная информатика и информационная безопасность. 2017. С. 137-138.
4. Internet Security Systems RealSecure // Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century: Prevention and Detection for the Twenty-First Century. 2005 [Электронный ресурс]. URL: https://flylib.com/books/en/2.352.1/internet_security_systems _realsecure.html (дата обращения: 04.06.2020).
5. Парнелл Т. Программы обнаружения сетевых атак // Network world. 2000. №4 [Электронный ресурс]. URL: https://www.osp.ru/nets/2000/04/141079 (дата обращения: 04.06.2020).
6. BlackICE & ICEcap // NetworkIce.com. 2020 [Электронный ресурс]. URL: https://www.networkice.com/ (дата обращения: 04.06.2020).
7. IBM выбирает программу INTRUDER ALERT корпорации SYMANTEC для защиты клиентов, пользующихся услугами компании по внешнему управлению системами безопасности // Infosecurity.ru. Информационная безопасность бизнеса. 2012 [Электронный ресурс]. URL: http://www.infosecurity.ru/_gazeta/content/020312/pr020218.html (дата обращения: 05.06.2020).
8. Хостовая система выявления атак Symantec Intruder Alert [Электронный ресурс]. URL: http://razgovorodele.ru/ security/safety09/safe-work06.php (дата обращения: 05.06.2020).
9. Системы обнаружения вторжений // Byte. 2001. №10 (39) [Электронный ресурс]. URL: https://www.bytemag.ru/articles/detail.php?ID=6563%27 (дата обращения: 05.06.2020).
10. CyberSafe // Киберсофт [Электронный ресурс]. URL: https://cybersafesoft.com/product.php?id=1 (дата обращения: 05.06.2020).
11. Broadcom // Broadcom. Inc. [Электронный ресурс]. URL: https://www.broadcom.com/ (дата обращения: 05.06.2020).

12. Detection and prevention: 6 intrusion detection systems tested // ZD Net. [Электронный ресурс]. URL: https://www.zdnet.com/article/detection-and-prevention-6-intrusion-detection-systems-tested/ (дата обращения: 05.06.2020).
13. PT Network Attack Discovery // Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/services/ (дата обращения: 05.06.2020).
14. ViPNet Personal Firewall 4 // ИнфоТеКС [Электронный ресурс]. URL: https://infotecs.ru/product/vipnet-personal-firewall.html#docs (дата обращения: 05.06.2020).
15. Тютюнников Н.Н. Оценка затрат на разработку и сопровождение программных средств терминологического фонда по базовому уровню модели COCOMO // Актуальные вопросы экономических наук. 2013. №35. С. 89–94.

УДК 025.2.004; 621.311.23: 629.12

МНОГОПАРАМЕТРИЧЕСКИЕ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ, ДАТА-ЦЕНТРЫ И ЭЛЕКТРОННЫЕ БИБЛИОТЕКИ: СПОСОБ КОНТРОЛЯ ПАРАМЕТРОВ ТЕХНИЧЕСКОГО СОСТОЯНИЯ И АНАЛИЗА КАЧЕСТВА

Паращук Игорь Борисович, Михайличенко Николай Валерьевич, Крюкова Елена Сергеевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shchuk@rambler.ru, 23esn2008@rambler.ru, e.kkrukovaa69@yandex.ru

Аннотация. Рассмотрены особенности и перспективы использования нового способа контроля и анализа многопараметрических систем хранения данных, дата-центров и электронных библиотек, в который заложена новая совокупность существенных признаков и определена новая последовательность действий. Способ обеспечивает повышение уровня достоверности результатов анализа и контроля параметров таких сложных информационно-технических систем в условиях неоднородной исходной информации, получаемой по разным каналам наблюдения, обеспечивает непрерывный анализ параметров системы, показателей (коэффициентов) ее качества и эффективности за интервал времени (получение интервальных оценок), что расширяет область применения технических средств контроля и диагностики параметров сложных управляемых технических систем и устройств, где данный способ будет использован, с учетом внутренних и внешних (конструктивных и деструктивных) воздействий на многопараметрическую систему на определенных временных интервалах.

Ключевые слова: многопараметрическая система, электронная библиотека, способ, состояние, качество, анализ, контроль, оценка, интервальные средние.

MULTIPARAMETRIC DATA STORAGE SYSTEMS, DATA CENTERS AND DIGITAL LIBRARIES: METHOD OF CONTROL THE TECHNICAL CONDITION PARAMETERS AND QUALITY ANALYSIS

Parashchuk Igor, Mikhaylichenko Nikolay, Kryukova Elena
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shchuk@rambler.ru, 23esn2008@rambler.ru, e.kkrukovaa69@yandex.ru

Abstract. Peculiarities and prospects of using a new method for monitoring and analyzing multi-parameter data storage systems, data centers and electronic libraries, which contain a new set of essential features and determine a new sequence of actions, are considered. The method provides an increase in the level of reliability of the results of analysis and control of the parameters of such complex information technology systems under the conditions of heterogeneous initial information obtained through different observation channels, provides a continuous analysis of the system parameters, indicators (coefficients) of its quality and efficiency over a time interval (obtaining interval estimates) that expands the scope of technical means of monitoring and diagnostics of parameters of complex controlled technical systems and devices where this method will be used, taking into account internal and external (structural and destructive) effects on a multi-parameter system at certain time intervals.

Keywords: multi-parameter system, electronic library, method, condition, quality, analysis, control, evaluation, interval averages.

Введение. В современных условиях все большее значение приобретают способы контроля и анализа технического состояния, качества и защищенности сложных многопараметрических информационно-технических систем (МПС), объектов и процессов, реализуемых ими [1-5]. Вместе с тем, существующие методы контроля параметров технического состояния и анализа качества сложных управляемых информационно-технических систем, не всегда соответствуют требованиям современных систем управления.

Например, известен, так называемый, «неразрушающий способ» [3], при реализации которого осуществляют неоднократный контроль сложного технического объекта путем его сканирования при идентичных условиях с определенными временными интервалами между сканированиями. Однако эффективному использованию данного метода для задач контроля и анализа МПС хранения данных (ХД), дата-центров (ДЦ) и электронных библиотек (ЭБ) не способствует большое время, необходимое для контроля технического состояния и качества контролируемого объекта, а также низкая чувствительность к малым отклонениям его параметров. Способ, известный как метод Чернякова-Петрушина [4], основан на представлении технической системы в виде иерархии ее структурных элементов, характеризующихся частными показателями качества и эффективности, и приведении в соответствие каждому элементу нормативных значений, соответствующих этим частным показателям. Но это

способ с ограниченными возможностями, поскольку позволяет осуществлять контроль, диагностику и прогнозирование технического состояния лишь радиоэлектронного оборудования, что является недостаточным для оценки технического состояния, качества и эффективности больших систем, требующих более высокого уровня компьютерного обеспечения с привлечением баз данных, например, МПС ХД, ДЦ и ЭБ. Существует способ контроля МПС [5], основанный на автоматической оценке параметров качества. Однако данный способ имеет недостаток – относительно невысокую достоверность контроля и узкую область применения, ограниченную возможностью идентификации показателей качества в дискретные моменты времени. Этот способ позволяет получать точечные оценки параметров системы, не всегда пригодные для принятия решений по оптимальному управлению МПС и для прогноза динамики их функционирования. В реальных условиях анализ и контроль параметров состояния МПС, таких как системы ХД, ДЦ и ЭБ, происходят не только в условиях неоднородной исходной информации, но и в условиях внутренних и внешних (конструктивных и деструктивных) воздействий на систему на определенных временных интервалах, а для оптимального управления системой в таких условиях интерес представляет не точечный, а интервальный результат, оценочные значения параметров системы за интервал времени. Это подтверждают и известные международные стандарты, апробированные на зарубежных системах [6], где акценты расставлены на вопросах непрерывной оценки качества.

С учетом этого, предлагается способ анализа и контроля МПС, например, таких как системы ХД, ДЦ и ЭБ, в котором дополнительно производится интервальная оценка качества и идентификация технического состояния системы при неполной и неоднородной информации, на основе использования теории интервальных средних [7]. При этом задают временной интервал (t+Δt) на котором будет осуществляться интервальная оценка параметров МПС (этот интервал может быть от одной до 10 минут). Затем, на множестве всех идентифицированных параметров технического состояния, путем анализа статистики за время (t+Δt) мгновенных значений параметров системы, определяют показатели (коэффициенты) качества каждого состояния $\mu(S_i)$ на временном интервале (t+Δt). На основе статистического анализа измеряемых параметров (наблюдения на интервале (t+Δt)) элементов МПС и с использованием методов теории интервальных средних находят нижний и верхний средние уровни качества элементов МПС на интервале времени (t+Δt) [7-9]. Вычисляют точное нижнее $\underline{E}(t+\Delta t)$ и верхнее $\overline{E}(t+\Delta t)$ значение среднего уровня эффективности МПС, наблюдаемого на интервале времени (t+Δt), путем решения задачи линейного программирования на основе средних значений идентифицированных параметров системы. В итоге, определяются интервальные оценки обобщенного показателя (коэффициента) качества и обобщенного показателя эффективности МПС типа систем ХД, ДЦ и ЭБ, с учетом результатов интервального анализа параметров этой системы.

Предложенный способ работает следующим образом. Производится контроль многопараметрических систем, включающий в себя процедуры оценки в реальном масштабе времени и накопления (записи) данных о значениях параметров системы на интервале времени (t+Δt). Затем осуществляется выбор с помощью коммутатора измеряемых параметров, измеряют величины этих параметров на интервале времени (t+Δt) с помощью n различных специальных датчиков, преобразуют величины параметров в соответствующие цифровые данные с помощью различных специальных преобразователей, регистрируют цифровые данные в запоминающем устройстве накопителя базы данных и анализируют их в вычислителе интервальных средних, получая интервальный результат контроля, оценочные значения за интервал времени.

Заключение. Таким образом, рассмотрены особенности и перспективы использования способа контроля и анализа многопараметрических систем ХД, дата-центров и ЭБ, в который заложена новая совокупность существенных признаков и определена новая последовательность действий. Этот способ обеспечивает повышение уровня достоверности результатов анализа и контроля параметров таких сложных информационно-технических систем в условиях неоднородной исходной информации, получаемой по разным каналам наблюдения, обеспечивает непрерывный анализ параметров системы, показателей (коэффициентов) ее качества и эффективности за интервал времени (получение интервальных оценок), что расширяет область применения технических средств контроля и диагностики, где данный способ будет использован, с учетом внутренних и внешних (конструктивных и деструктивных) воздействий на многопараметрическую систему на определенных временных интервалах.

СПИСОК ЛИТЕРАТУРЫ

1. Бушуев С.Н., Авраменко В.С., Копчак Я.М., Козленко А.В. Методологические аспекты оценки качества управления связью // Вопросы радиоэлектроники. 2013. Т. 3. №1. С. 49-53.
2. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-практической конференции. Т. 4., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2019. С. 19-24.
3. Патент РФ №2184373 «Способ неразрушающего контроля изделий», МПК G01N 29/04, опубликован 27.06.2002, Бюл. №18.
4. Патент РФ №2210112 «Унифицированный способ Чернякова/Петрушина для оценки эффективности больших систем», МПК G06F 17/00, опубликован 10.08.2003, Бюл. № 22.
5. Патент РФ №2427875 «Способ контроля и анализа многопараметрических систем», МПК G05B 21/00, G06F 17/40, опубликован 27.08.2011, Бюл. №24.
6. ISO/IEC 15288:2008. Systems and software engineering – System life cycle processes. (пересмотрен ISO/IEC/IEEE 15288:2015) [Электронный ресурс]. URL: https://www.iso.org/ru/standard/463711.html (дата обращения: 13.06.2020).
7. Гуров С.В., Уткин Л.В. Надежность систем при неполной информации. – СПб.: Любавич, 1999, 160 с.
8. Кузнецов В.П. Интервальные статистические модели. – М.: Радио и связь, 1991. 352 с.
9. Крюкова Е.С., Малофеев В.А., Паращук И.Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек // Новые информационные технологии и системы: сборник научных статей XVI Международной научно-технической конференции (г. Пенза, 27–29 ноября 2019 г.). – Пенза: Изд-во ПГУ, 2019. С. 177-180.

УДК 004.942

СОВМЕСТНОЕ УПРАВЛЕНИЕ МАРШРУТИЗАЦИЕЙ И КАНАЛЬНОЙ СТРУКТУРОЙ МОБИЛЬНОЙ ПАКЕТНОЙ СЕТИ РАДИОСВЯЗИ НА ОСНОВЕ ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ ИНФОРМАЦИОННЫХ ПОТОКОВ В РЕШЕНИИ ЗАДАЧИ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ СРЕДСТВ СВЯЗИ И АСУ

Попов Андрей Иванович, Макарова Ульяна Витальевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: AdPopovAI@yandex, ulyana.umrihina@yandex.ru

Аннотация. В настоящее время, в условиях, когда сеть передачи данных активно развивается, вопрос технического обеспечения связи и автоматизированных систем управления (АСУ) является значимым и требует достаточного внимания при проектировании и строительстве новых сетей передачи данных (СПД) и систем хранения данных, и развитии и усовершенствовании старых. В данной статье рассмотрены основные направления совершенствования телекоммуникационных технологий, также методы и задачи маршрутизации, предложенные для применения в пакетных мобильных СПД, их классификации. Представлена методика формализованной постановки и решения задачи оптимального совместного управления маршрутизацией и канальной структурой пакетной радиосети, основанного на оптимизации распределения информационных потоков по маршрутам сети в рамках ограничений.

Ключевые слова: пакетные сети передачи данных, маршрутизация, телекоммуникационные технологии.

JOINT CONTROL OF ROUTING AND CHANNEL STRUCTURE OF MOBILE PACKET RADIO COMMUNICATION NETWORK BASED ON OPTIMIZATION OF DISTRIBUTION OF INFORMATION FLOWS IN SOLVING TASK OF TECHNICAL SUPPORT OF COMMUNICATION FACILITIES AND ACS

Popov Andry, Makarova Uliana
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: AdPopovAI@yandex, ulyana.umrihina@yandex.ru

Abstract. At present, as the data network is actively evolving, the issue of communications technology and automated control systems (ACS) is significant and requires sufficient attention in the design and construction of new data networks (SDNs) and storage systems, and the development and improvement of old ones. This article discusses the main areas of improvement of telecommunication technologies, as well as the routing methods and tasks proposed for application in packet mobile SDNs, their classification. The method of formalized setting and solving the problem of optimal joint control of routing and channel structure of a packet radio network based on optimization of distribution of information flows along network routes within limits is presented.

Keywords: packet data networks, routing, telecommunication technologies.

Введение. В настоящее время, в условиях, когда сеть передачи данных постоянно совершенствуется вопрос технического обеспечения связи и АСУ является значимым и требует достаточного внимания при проектировании и строительстве новых сетей передачи данных (СПД) и систем хранения данных [1], и развитии и усовершенствовании старых. В свою очередь продолжается перевод существующих систем радиосвязи на цифровые методы передачи информации, пакетную передачу речи и данных, особое внимание необходимо уделять развитию пакетных радиосетей, как более перспективного направления по сравнению с традиционными. В основе их лежит принцип коммутации пакетов применительно к системе радиосвязи с подвижными объектами.

На сегодняшний день развитие телекоммуникационных технологий идет по двум основным направлениям: увеличение производительности оборудования за счет использования новой элементной базы, и разработка новых алгоритмов целью достижения ими новых качеств.

Пакетные радиосети вышли на качественно новый уровень своего развития, для которого характерно резкое возрастание количества взаимодействующих узлов, интенсивность обмена данными, активное использование мультимедиа-технологий в системе управления, повышение требования к оперативности доставки информации. Сильная территориальная разобщенность таких сетей с одной стороны, и динамический характер параметров и топологий с другой, подразумевает создание и использование качественно новых подходов к управлению передачей данных в системе управления пакетной радиосети.

Одной из важнейших проблем, требующих решения, является создание эффективных алгоритмов маршрутизации, обеспечивающих поиск необходимых маршрутов с учетом динамики и топологии пакетной радиосети.

Все методы маршрутизации, предложенные для применения в пакетных мобильных сетях передачи данных, можно классифицировать по следующим признакам [5]:

- по способу построения и поддержания маршрутов: таблично-ориентированные (далее табличные), зондовые и гибридные;
- по числу получателей: однопользовательские, групповые и “волновые”;

– по количеству и типу параметров в метрике выбора маршрута: однопараметрические и многопараметрические; энергосберегающие, с заданным качеством обслуживания и др.
– по количеству маршрутов: однопутевые и многопутевые;
– по типу маршрутов: симметричные и асимметричные.
– по наличию оборудования позиционирования: координатные и некоординатные;
– по организации сети: иерархические и неиерархические (одноуровневые);
– по принятию решений по маршрутизации: пассивные и активные (интеллектуальные).

Задачей метода маршрутизации является создание, хранение и поддержание маршрута(ов) передачи между отправителем и адресатом заданного качества (обычно кратчайшего). Кратчайший маршрут определяется как функция минимальной стоимости маршрута, определяемая как сумма стоимостей всех каналов маршрута. При этом методы маршрутизации должны [5,6]:

– соответствовать особенностям МР;
– удовлетворять ряду обязательных (опционных) требований.

Например, ТР1 – децентрализованное функционирование (обязательно); ТР2 – быстрая сходимость и отсутствие зацикливания маршрутов (обязательно); ТР3 – минимальная загрузка сети служебной информацией (выступает целевой функцией); ТР4 – получение маршрута по мере необходимости (режим ≪молчания≫ сети); ТР5 – обеспечение нескольких маршрутов доставки информации к адресату; ТР6 – обеспечение маршрутов заданного качества (по производительности, задержки и др.); ТР7 – поддержка однонаправленных каналов; ТР8 – минимизация расходуемой мощности узлов, оснащенных батареями; ТР9 – безопасность процессов маршрутизации и другие.

Исторически сложившийся подход к решению данной проблемы основан на алгоритмах, созданных для выбора оптимальных путей в графах с фиксированной структурой, где динамическая топология сети не является исходным положением, а каждый случай ее изменения рассматривается как смена режима функционирования, топологии и нагрузки.

Рассмотрим задачу совместного управления маршрутизацией пакетов в мобильной пакетной сети радиосвязи с автоматически управляемыми режимами функционирования радиосредств. Обычно при построении таких сетей на каналообразующие средства возлагаются задачи создания канальной структуры, в рамках которой обеспечивалась бы эффективная передача данных, в том числе с управлением маршрутизацией при различных нагрузках в информационных направлениях сети [2-6].

Основным отличием постановок задач от традиционных задач и методик (см., например, [2-6]) является учет возможности назначения (переназначения) маршрутов, которые могут быть реализованы при работе радиосредств в различных режимах, определяющих на сетевом уровне системы передачи данных, как корреспондирующее направление передачи данных, так и техническую скорость обмена информацией. Принципы построения пакетных сетей радиосвязи такого типа описаны в [5-6]. В настоящей работе представлена методика формализованной постановки и решения задачи оптимального совместного управления маршрутизацией и канальной структурой пакетной радиосети, основанного на оптимизации распределения информационных потоков по маршрутам сети в рамках ограничений.

Задача оптимального управления сводится к задаче оптимизации величин, определяющих интенсивности информационных потоков на маршрутах.

Выводы**.** Предложенная методика может использоваться для постановки и решения задачи построения оптимального алгоритма маршрутизации пакетов данных, реализация которого в ИС обеспечивает максимальную вероятность своевременной доставки сообщений. В рамках рассмотренной модели могут представляться сети, фрагментами которых являются пакетные радиосети, а также другие системы связи, ресурс которых ограничен не только пропускной способностью линий связи, но и пропускной способностью отдельных элементов.

Разработанный алгоритм оптимизации распределения информационных потоков обеспечивает нахождение ε-оптимальной сетевой структуры с требуемой для практики точностью и оперативностью, позволяющей его использовать для выработки решений по управлению маршрутизацией в ИС в реальном времени. Постановка задачи, методика решения и алгоритм оптимизации легко адаптируются к другим вариантам задания оптимизируемого функционала.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М., Путилин А.Н. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных // Журнал «Радиотехнические и телекоммуникационные системы», март 2019, стр. 46-56
2. Паращук И. Б .,Чуднов А. М Методика комплексной маршрутизации в неоднородной сети передачи данных военного назначения // Журнал «Известия Российской академии ракетных и артиллерийских наук», Спец. выпуск за 2019 г., стр.60-64
3. Паращук И. Б., Михайличенко Н.В. Эффективность современных центров обработки данных. Перспективные направления развития отечественных информационных технологий: материалы III межрегиональной научно-практической конференции. Научный редактор Б.В. Соколов, 2017. С.24-26.
4. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений // Радиотехнические и телекоммуникационные системы. 2017, №2, с.41-49.
5. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
6. Путилин А. Н. Алгоритм управления режимами обмена данными в самоорганизующейся сети декаметровой радиосвязи. // Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция, 1-3 ноября 2017 г. Санкт-Петербург. 2017, с. 106-107.

УДК 004

ИНФОРМАЦИОННАЯ СИСТЕМА УЧЁТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Ренсков Андрей Анатольевич, Ренсков Дмитрий Андреевич, Халенёв Александр Юрьевич, Сотская Дарья Ивановна

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: andreyrenskov@gmail.com, dmitryirenskov@gmail.com, a.khalenev@yandex.ru, darya.sotskaya@bk.ru

Аннотация. В данной работе рассмотрены сущность, содержание разработанной информационной системы учета программного обеспечения, предназначенная для автоматизации процесса учета, поиска ПО и формирования других запросов. Приведены технологии и средства разработки данной информационной системы. Представлено описание интерфейса ИС, показывающее простоту и удобность использованием данной информационной системы учета ПО в военном образовательном учреждении. В данной работе были учтены условия для ее функционирования в масштабах военного образовательного учреждения.

Ключевые слова: программное обеспечение, информационная система, учёт ПО, запросы, сервер, веб-приложение.

SOFTWARE ACCOUNTING INFORMATION SYSTEM IN EDUCATIONAL INSTITUTION

Renskov Andrey, Renskov Dmitry, Khalenev Alexandr, Sotskaya Darya

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: andreyrenskov@gmail.com, dmitryirenskov@gmail.com, a.khalenev@yandex.ru, darya.sotskaya@bk.ru

Abstract. This paper considers the essence and content of the developed information system of software accounting, designed to automate the accounting process, search for the source of other queries. The article describes th technologies and tools for developing this information system. The description of the is interface shows the simplicity and convenience of using this information system for software accounting in a military educational institution. This work took into account the conditions for it is functioning in the scale of a military educational institution.

Keywords: software, information system, software accounting queries, server, web application.

Введение. На факультетах высших учебных заведений готовят большое многообразие специалистов по различным специальностям. Как нельзя остро стоит задача создания информационной системы учета программного обеспечения, предназначенная для автоматизации процесса учета, поиска ПО и формирования других запросов.

В качестве основного подхода обучения принята концепция 3-х этапной подготовки [1]:

На первом этапе осуществляется теоретическая подготовка. В ходе изучения теоретического материала активно используются электронные образовательные ресурсы.

На втором этапе формируются первичные навыки в эксплуатации средств связи и автоматизации при выполнении учебных задач на тренажерных средствах. В основном это программные средства, имитирующие работу реальных средств связи и автоматизации, общее количество, которых достигает более двухсот.

На третьем этапе формируются навыки в эксплуатации средств связи и автоматизации при выполнении учебных задач на реальных средствах связи и автоматизации.

Это показывает, что особенностью образовательной деятельности является ее информатизация, что характерно для всех образовательных организаций России. Реализуется информатизация посредством информационной образовательной среды.

Согласно ФГОС важным условием реализации основной образовательной программы, является наличие в вузе ИОС, включающей в себя:

- комплекс информационных образовательных ресурсов;
- цифровые образовательные ресурсы;
- средства информационных и телекоммуникационных технологий;
- систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде.

На сегодняшний день в образовательных учреждениях разработано более тысячи программных продуктов, ориентированных на обучение. Это и электронные учебники, электронные версии учебных пособий, системы тестирования, виртуальные туры, компьютерные тренажеры и т.д.

Таким образом, разработка информационной системы учета программного обеспечения для высшего учебного заведения с учетом современных условий является актуальной.

Основным принципом образовательной организации является реализация единых подходов в профессиональной деятельности, в том числе и реализация единых требований к информационной системе учета программного обеспечения.

Разрабатывая информационную систему для деятельности факультетов было необходимым учесть условия для ее функционирования в высшем учебном заведении. Так информационная система должна быть адаптирована к условиям функционирования в интересах всех факультетов образовательного учреждения. Информационная система

учета программного обеспечения факультета образовательного учреждения предназначена для автоматизации процесса учета, поиска ПО и формирования других запросов.

Разработана база данных и веб-приложение, позволяющее формировать запросы на обработку данных. Веб-приложение в настоящее время является очень популярным решением во многих областях.

В качестве базовых технологий и средств разработки информационной системы использованы язык гипертекстовой разметки – HTML, язык создания сценариев на стороне клиента – JavaScript, язык создания сценариев, исполняющихся на стороне веб-сервера – PHP и система управления базами данных MySQL.

Информационная система учета построена с использованием веб-приложении качестве промежуточного уровня, основанного на технологии "клиент-сервер", архитектура расширяется до трехуровневой.

На нижнем уровне на компьютерах пользователей расположены приложения клиентов, выделенные для выполнения функций и логики представлений, обеспечивающие программный интерфейс для вызова приложения на среднем уровне. Приложение нижнего уровня называют «тонким» или «облегченным» клиентом. В качестве клиента может выступать обычный web-браузер [2-4].

На среднем уровне расположен сервер приложений, на котором выполняется прикладная логика, и с которого логика обработки данных выполняет операции с базой данных, т.е. этот уровень обеспечивает обмен данными между пользователями и базами данных. Сервер приложений размещается в узле сети доступно всем клиентам.

На третьем, верхнем, уровне расположен удаленный специализированный сервер базы данных, принимающий информацию от сервера приложений. Сервер баз данных выделен для услуг обработки данных и файловых операций.

Кратко можно следующим образом описать работу СУБД с трехзвенной архитектурой клиент-сервер. СУБД и база данных в виде набора файлов находится на жестком диске специально выделенного компьютера (сервера сети). На специально выделенном сервере приложений располагается программное обеспечение (бизнес-логика). На каждом клиентском компьютере установлен так называемый «тонкий» клиент — клиентское приложение, реализующее интерфейс пользователя. Клиент инициирует обращение к программному обеспечению, расположенному на сервере приложений. Сервер приложений формирует запросы к БД на языке SQL, т.е. по сети от сервера приложений к серверу БД передается лишь текст запроса. Результат выполнения запроса копируется на сервер приложений, который возвращает результат в клиентское приложение (пользователю). Приложение отображает результат выполнения запросов.

При такой архитектуре клиентский уровень занимает браузер, на уровне сервера находится сервер БД, а на промежуточном уровне размещаются веб-сервер и модули расширения сервера. Модуль расширения сервера выступает преобразователем протоколов между клиент-серверным приложением.

Защита информации, размещенной на страницах веб-приложения, а также в базе данных обеспечивается двумя уровнями безопасности: уровень безопасности СУБД MySQL и уровень безопасности, реализуемый непосредственно на уровне веб-приложения.

Гибкая система безопасности и аутентификации сервера баз данных позволяет решить большинство проблем безопасности БД «Учета ПО факультета образовательного учреждения».

Были разработаны функциональная схема информационной системы учета ПО, обобщенный алгоритм работы информационной системы учета ПО, инфологическая, логическая и физическая модель данных информационной системы учета ПО факультета военного учебного учреждения

Главная страница информационной системы учета программного обеспечения состоит из «шапки» сайта, пользовательского меню, строки поиска и таблицы с краткой характеристикой зарегистрированного ПО.

Меню состоит из ссылок, по которым осуществляются переходы между разделами веб-приложения. В состав меню входят: Главная; Администрирование; Карта регистрации; Сведения о ПО.

Ниже пользовательского меню располагается строка быстрого контекстного поиска программного обеспечения.

Основную часть экранной формы занимает таблица с краткой характеристикой зарегистрированного ПО и набором фильтров для оптимизации поиска необходимого ПО.

По номеру регистрации с помощью ссылки осуществляется переход на страницу «Сведения о ПО».

Заключение. Таким образом, была разработана и реализована информационная система учета программного обеспечения учебного учреждения, для которой была создана база данных ведения информации о регистрируемом программном обеспечении.

Информационная система учета программного обеспечения предназначена для хранения информации о программных продуктах, используемых при ведении и обеспечении образовательной деятельности факультета образовательного учреждения

Был соблюден принцип образовательной организации: реализация единых подходов в профессиональной деятельности, в том числе и реализация единых требований к информационной системе учета программного обеспечения. Были учтены условия для ее функционирования в масштабах образовательного учреждения.

СПИСОК ЛИТЕРАТУРЫ

1. Министерство связи и массовых коммуникаций Российской Федерации. Приказ №226 от 31.05.2016 г. «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных.»
2. Артеменко Ю.Н. MySQL. Справочник по языку.-М:Вильямс,20011-535с.
3. Мазуркевич А., Еловой Д. PHP: Настольная книга программиста- М.:Новое знание, 2012 – 479с.
4. PHP – License. Официальный сайт компании. Интернет: http://www.php.net

УДК 621. 391

ЗАЩИТА ОТ ПОМЕХ И ПОМЕХОУСТОЙЧИВОСТЬ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ПО КОРОТКОВОЛНОВЫМ ЛИНИЯМ СВЯЗИ

Савищенко Николай Васильевич, Синюк Александр Демьянович, Остроумов Олег Александрович, Остроумов Максим Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: snikaspb@mail.ru, eentrop@rambler.ru, oleg-26stav@mail.ru

Аннотация. Рассматривается методика оценки помехоустойчивости приема многопозиционных сигналов в линиях радиосвязи декаметрового диапазона частот. Получены точные выражения расчета вероятности ошибки в канале связи в условиях замираний Райса и Релея.

Ключевые слова: замирания, разнесенный прием, вероятность ошибки, многопозиционные сигналы, помехоустойчивость.

INTERFERENCE PROTECTION AND NOISE IMMUNITY WHILE INFORMATION TRANSMITTING AT SHORT-WAVE COMMUNICATION LINES

Savishenko Nikolay, Sinuk Aleksander, Ostroumov Oleg, Osnroumov Maksim
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: snikaspb@mail.ru, eentrop@rambler.ru, oleg-26stav@mail.ru

Abstract. Noise immunity evaluation technique of receiving multi-position signals in radio lines of the decameter frequency range is considered. The exact expressions of the error probability calculation in the communication channel under the conditions Rice and Rayleigh fading are obtained.

Keywords: fading, diversity, error probability, multi-position signals, noise immunity.

Введение. Как известно на надежность связи при передаче информации в любом диапазоне частот существенное влияние оказывают помехи. Помехи могут иметь различную природу. Они могут быть искусственными, естественными и т.д. Наибольшее влияние оказывают помехи, похожие на сигналы, которые используются для передачи полезной информации. Наличие естественных помех при передаче информации по коротковолновым линиям связи также пагубно влияет на качество связи. В ионосферных каналах радиосвязи, из-за неоднородности ионосферы возникают замирания, и присутствует эффект многолучевости, из-за переотражения радиоволны от различных слоев ионосферы и неоднородностей в них.

Основная часть. Повышение помехоустойчивости и помехозащищённости линий радиосвязи, а также совершенствование математического аппарата их оценки помехоустойчивости, исходя из требований к системам связи, является актуальным. Существует много способов борьбы с помехами и замираниями [1]. Одним из наиболее эффективных и часто используемых является метод разнесенного приема. В системах с разнесенным приемом обеспечивается параллельная передача одной и той же информации по нескольким ветвям разнесения. Выделяют шесть видов разнесения: по пространству, по времени и частоте, по углу прихода лучей, по поляризации и по отдельным лучам при многолучевом распространении [2-4].

Существующие методики оценки помехоустойчивости систем с разнесенным приемом, представленные в [2,4], не учитывают позиционность передаваемых многомерных сигналов и влияние помехи подобной, сигналу.

В работе предлагается методика оценки помехоустойчивости декаметрового канала радиосвязи в условиях разнесенного приема многопозиционных сигналов КАМ-*M* и ФМ-*M* для канала с аддитивным белым гауссовским шумом и замираниями Райса и Релея. Отличие данной методики от уже существующих [1] заключается в расчете средней вероятности символьной (битовой) ошибки по точным выражениям, учитывающим позиционность многомерных многопозиционных сигналов.

Заключение. Использование пространственного разнесенного приема всегда дает выигрыш по помехоустойчивости. При пространственном разнесенном приеме выбор количества ветвей может производиться в зависимости от тех требований, которые предъявляются к системе связи. При использовании временного (частотного, когда информация на каждой частоте излучается своим передатчиком) разнесенного приема с увеличением количества ветвей разнесения для фиксированной мощности сигнала величина вероятности ошибки стремится к значению вероятности ошибки в канале с аддитивным белым гауссовским шумом. При частотном разнесенном приеме, реализованном на одном передатчике, с увеличение количества ветвей разнесения значение вероятности ошибки в канале связи уменьшается до определенного минимального значения. При дальнейшем увеличении количества ветвей разнесения качество связи ухудшается.

В случае если канал связи неоднородный, то при сдвоенном пространственном разнесенном приеме величина энергетических потерь, связанная с тем, что в разных ветвях отношение сигнал/шум различное, практически не зависит от позиционности используемых сигналов.

СПИСОК ЛИТЕРАТУРЫ

1. Игнатов В. В., Сахнин А. А. Развед- и помехозащищённость систем и средств военной связи. – СПб.: ВУС, 2001. 212 с.
2. Кловский Д. Д. Передача дискретных сообщений по радиоканалам. – М.: Радио и связь, 1982. 362 с.
3. Савищенко Н. В. Специальные интегральные функции, применяемые в теории связи:монография. — СПб.: Военная академия связи, 2012. — 560 с.
4. Андронов И. С., Финк Л. М. Передача дискретных сообщений по параллельным каналам. – М.: Сов.радио, 1971. 408 с.

УДК 621. 391.3

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПЭМИН НА ОСНОВЕ МЕТОДА ЭФФЕКТИВНОГО НЕРАВНОМЕРНОГО КОДИРОВАНИЯ ПРЕФИКСНЫМИ КОДАМИ

Синюк Александр Демьянович, Остроумов Олег Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий, пр., 3, Санкт-Петербург, 194064, Россия
e-mails: eentrop@rambler.ru, oleg-26stav@mail.ru

Аннотация. Рассматривается метод зашиты информации от утечки по каналу ПЭМИН. В его основе заложена оценка трудоемкости нарушителя по восстановлению блока сообщения из его образа с ошибками сжатого методом эффективного неравномерного кодирования префиксными кодами на выходе канала утечки. Определяется общая постановка задачи. Приводятся некоторые стратегии нарушителя по получению исходного сообщения на входе канала утечки. Предлагаются меры по увеличению трудоемкости нарушителя с использованием псевдослучайных вставок. Определяются направления исследований. Полученные результаты развивают и углубляют известные исследования защиты информации от утечки по ПЭМИН и могут быть полезны специалистам в области построения подсистем защиты информации телекоммуникационных систем.

Ключевые слова: защита информации, легальные пользователи; нарушитель; канал утечки; побочный канал электромагнитных излучений и наводок; метод эффективного неравномерного кодирования префиксными кодами.

INFORMATION PROTECTION FROM PEMINS LEACKAGE BASED ON THE METHOD OF EFFECTIVE UNIFORM CODING WITH PREFIX CODES

Sinuk Aleksander, Ostroumov Oleg
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny,
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: eentrop@rambler.ru, oleg-26stav@mail.ru

Abstract. The information protection method from leakage through the spurious electromagnetic emissions and interference channel is considered. It is based on the assessment of the intruder complexity to restore the message block from its image with errors compressed by the method of effective uneven coding with prefix codes at the leak channel output. The problem general statement is determined. Some intruder strategies for receiving the initial message at the leak channel input are given. Measures are proposed to increase the complexity of the intruder using pseudo-random inserts. Research areas are identified. The obtained results develop and deepen the information protection well-known studies against leakage through spurious electromagnetic emissions and interference and they may be useful to specialists in the field of building information protection subsystems of telecommunication systems.

Keywords: information protection, legal users; intruder; leak channel; side channel of electromagnetic radiation and interference; method of efficient non-uniform coding with prefix codes.

Введение. В современное время обеспечение защиты информации является сложной, многогранной проблемой, решение которой требует разработки и реализации ряда технических, правовых, организационных и других мер. Общепринятой мерой защиты содержания информации считается использование криптографических методов [1]. Однако применение последних не полностью решает задачу обеспечения конфиденциальности передаваемой информации в телекоммуникационных системах. Это связано с тем, что при достаточно сложном построении современных систем связи остаются отрезки тракта передачи-приема информации, по которым она циркулирует в открытом виде. Этот факт создает угрозу формирования канала утечки информации по так называемым побочным каналам электромагнитных излучений и наводок (ПЭМИН) [2].

В работах [1-4] представлен ряд методов защиты от ПЭМИН к которым можно отнести: применение экранов и обработка информации в экранированных помещениях; применение генераторов шума; использование специальных фильтров; использование волоконно-оптических кабелей; реализация способов кодового зашумления и шифрования по известному ключу и др. Приведенные методы используют различную природу воздействия на ПЭМИН и имеют недостатки, ограничивающие область их применения. Это определяет необходимость поиска новых способов защиты предаваемой информации от ПЭМИН.

Предлагается метод зашиты информации от утечки по каналам ПЭМИН на основе методов эффективного кодирования неравномерными префиксными кодами [5, 6]. К данному классу кодов можно отнести коды Хафмена, Шеннона-Фано и др. Особенностью выбранной группы кодов является, то, что все кодовые комбинации (КК) имеют разную длину, разделение которых осуществляется таким выбором комбинаций, когда начало каждой из них будет уникальным. В ходе декодирования выделение кодовой комбинации осуществляется по неповторяющемуся сочетанию символов начала КК. Эти методы используются преимущественно для кодирования текстовых сообщений, данных телеметрии и любых цифровых данных, когда недопустима потеря, либо искажение даже одного элемента сообщения. Эти обстоятельства составляют базис предлагаемого метода.

Рассмотрим следующую постановку задачи. Необходимо передать сообщение между легальными пользователями A и B, осуществляя обмен данными между ними по каналам, которые доступны по каналам утечки по ПЭМИН нарушителю E. Требуется обеспечить передачу сообщения с высокой защищенностью для легальных пользователей и обеспечить

наперед заданный высокий уровень трудоемкости поиска сообщения для *E*. Пользователь *A* связан с пользователем *B* по идеальному основному каналу связи (т.е. каналу связи без ошибок) [3, 4]. Нарушитель *E* на выходе канала утечки по ПЭМИН перехватывает всю передаваемую информацию, которая передается по основному каналу. Описание канала утечки можно представить моделью дискретного симметричного канала связи [4]. Предполагается, что вероятность ошибки на бит канала утечки отлична от нуля.

Пусть у легального пользователя *A* имеется некоторый текст T длиной *t* бит, который необходимо передать получателю *B*. Перед передачей текст сжимается компрессором посредством выбранного метода эффективного неравномерного кодирования префиксными кодами (ЭКНПК). Сжатый блок C (образ) передается по основному каналу. Легальный пользователь *B* преобразует принятый блок C в декомпрессоре по методу ЭКНПК и получает переданный текст T.

Рассмотрим ситуацию у нарушителя. Последний на выходе канала утечки получает сообщение (образ) C*. Исходя из того, что вероятность ошибки в канале утечки отлична от нуля, нарушитель получает искаженный ошибками блок (образ) сжатого текста C*. Известно, что методы ЭКНПК обладают большой чувствительностью к ошибкам, т.к. изменение в образе даже одного бита может привести к искажению всего принятого сообщения. Возникающие ошибки искажают принятые комбинации (образы) и существенно затрудняют корректное разделение последних между собой, что в совокупности с общим искажением комбинации существенно затрудняет правильное декодирование ее нарушителем.

Предположим, что множество текстов T включает некоторое подмножество допустимых текстов *W* (если, например, если передается текстовая информация, то естественно считать, что допустимым множеством являются буквы соответствующего языка, цифры и знаки препинания). Пусть допустимые тексты равномерно распределены на множестве всех возможных текстов T и вероятность того, что случайно выбранный текст, принадлежит множеству *W* отлична от нуля. У нарушителя имеется возможность отбрасывать бессмысленные тексты. Предположим, что выбранный метод ЭКНПК обладает большим коэффициентом размножения ошибок (изменение одного бита в комбинации влечет за собой изменение большого числа битов в открытого (восстановленного) текста).

В этих условиях для нарушителя возможна следующая стратегия получения открытого текста T: перебрать, восстанавливая некоторое количество сжатых текстов C*, учитывая, что при этом в сжатых блоках могут иметь место ошибки. Затем, выделить среди полученных текстов T* допустимые тексты и объединяя, несколько таких текстов, с использованием статистических закономерностей, можно получить с некоторой вероятностью передаваемое сообщение. Нарушитель имеет возможность выполнить следующие виды атак:

1. Поиск всех возможных комбинаций искаженных битов в блоке;
2. Составление библиотеки образцов блоков исходных сообщений и соответствующих им сжатых образов сообщений (СОС);
3. Выявление СОС, перехваченных без ошибок.

Однако, при больших размерах блоков информации практически невозможно заранее создать и хранить образцы СОС всех возможных исходных сообщений, что затрудняет реализацию атаки 1. Угадывание (поиск) позиций искаженных при перехвате битов приводит к правильной декомпрессии сообщения. Однако, такая атака имеет высокую трудоемкость, которую можно оценить средним числом пробных декомпрессий блока, содержащего среднее число ошибок.

В целях нейтрализации атаки 2 может быть использован следующий прием: легальным пользователем *A* предварительно подвергается компрессии сообщение и псевдослучайная вставка (ПВ) как единый блок. ПВ отбрасывается после приема и декомпрессии образа пользователем *B*.

Вероятность успешной атаки 3 не высока, т.к. предполагается, что в канале утечки вероятность битовой ошибки значительно больше нуля.

Заключение. Рассмотрен метод зашиты информации от утечки по каналу ПЭМИН. В его основе лежит оценка трудоемкости нарушителя по восстановлению блока сообщения из его образа с ошибками сжатого методом эффективного неравномерного кодирования префиксными кодами на выходе канала утечки. Определяется общая постановка задачи. Приводятся некоторые стратегии нарушителя по поиску исходного сообщения, которое было на входе канала утечки. Увеличение защищенности передаваемой информации от утечки по каналу ПЭМИН (увеличение трудоемкости нарушителя) возможно реализовать путями:

1. увеличения длины блока предаваемого сообщения;
2. ухудшения качества канала утечки;
3. использования псевдослучайных вставок.

Направлениями исследований могут быть выбраны построение модели совокупности основной канал – канал утечки, разработка методики оценки защищенности предлагаемым методом передаваемой информации от утечки по каналу ПЭМИН (оценки трудоемкости нарушителя).

Полученные результаты развивают и углубляют известные исследования защиты информации от утечки по ПЭМИН и могут быть полезны специалистам в области построения подсистем защиты информации телекоммуникационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: моногр. - М.: Триумф, 2012. 816 с.
2. Молдовян Н. А. Молдовян А. А. Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. - М.: БХВ-Петербург, 2004. 448 с.
3. Москвитин Г.И. Комплексная защита информации в организации. - М.: Русайнс, 2017. 400 с.
4. Яковлев В. А. Защита информации на основе кодового зашумления. – СПб.: ВАС, 1993. 245с.

УДК 004.021

МОДЕЛЬ ПРОТОКОЛА СЕТИ ПЕРЕДАЧИ ДАННЫХ В УСЛОВИЯХ ДЕСТРУКТИВНЫХ КИБЕРНЕТИЧЕСКИХ ВОЗДЕЙСТВИЙ

Чулков Александр Анатольевич, Дементьев Владислав Евгеньевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: sir.alexanderchulkov@yandex.ru, dem-vlad@rambler.ru

Аннотация. Статья посвящена вопросу построения модели протокола сети передачи данных (СПД) в условиях деструктивных кибернетических воздействий (ДКВ), позволяющей классифицировать признаки протоколов СПД для оценки защищенности протоколов. Приведены основные угрозы безопасности данных в СПД и способы их реализации. Описана структура и общие принципы функционирования искусственной нейронной сети, послужившей основой предложенной модели.

Ключевые слова: сеть передачи данных, протокол, безопасность данных, анализ, классификация, оценка.

A FORMALIZED MODEL OF THE DATA TRANSMISSION NETWORK PROTOCOL IN THE CONDITIONS OF DESTRUCTIVE CYBERNETIC IMPACTS

Chulkov Alexander, Dementiev Vladislav
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: sir.alexanderchulkov@yandex.ru, dem-vlad@rambler.ru

Abstract. The article is devoted to the issue of constructing a model of the data transmission network protocol in the conditions of destructive cybernetic influences, which allows classifying the features of destructive cybernetic influences protocols to assess the security of protocols. The main threats to data security in the data transmission network and ways to implement them are given. The structure and general principles of functioning of the artificial neural network that served as the basis of the proposed model are described.

Keywords: data transmission network, Protocol, data security, analysis, classification, evaluation.

Введение. В процессе хранения, обработки и передачи данных в СПД возникают различные виды угроз их безопасности. Под угрозой безопасности данных понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой данных и (или) несанкционированными и (или) непреднамеренными воздействиями на них. Для определения путей решения задачи обеспечения безопасности данных в СПД были проанализированы угрозы безопасности циркулирующих в сети данных.

В результате проведенного анализа [1] выявлено, что основным объектом угроз безопасности являются обрабатываемые в СПД данные, в которых содержится как служебная, так и технологическая информация. Реализация угроз служебной информации предполагает наличие необходимых полномочий по доступу к ней. Указанные полномочия могут быть получены путем воздействия на технологическую информацию СПД, используемую для обеспечения функционирования сети и системы защиты информации. Примером угрозы, направленной на нарушение безопасности технологической информации, т. е. технологической безопасности (ТБ), является угроза модификации набора данных, содержащего информацию об учетных записях пользователей, которая может осуществляться путем передачи по сети произвольных последовательностей пакетов (в том числе с некорректно установленными полями служебного заголовка, опциями, флагом фрагментации, типом сервиса и т.п.).

Анализ существующих методов и средств диагностирования деструктивных воздействий на СПД показал, что они обладают рядом недостатков. Основным недостатком является отсутствие функции автоматического анализа таких воздействий, а, следовательно, не позволяют обеспечить выполнение требований по оперативности и достоверности диагностирования деструктивных воздействий на СПД. Принимая во внимание данный недостаток, а также основываясь на проведенном анализе уязвимостей протоколов СПД, возможных угроз и возможностей нарушителя, авторами предложена [2] модель протокола СПД позволяющая в условиях ДКВ классифицировать признаки протоколов СПД для оценки защищенности протоколов. В основу модели легла генеративно-состязательная искусственная нейронная сеть (ГС ИНС), которая в отличие от используемых ранее обладает повышенным быстродействием и способностью к решению более сложных задач. Обученные ГС ИНС способны находить сложные зависимости при отсутствии предопределенной информации об исследуемых процессах или объектах. В задаче классификации, которая предполагает, что во входном векторе образов можно выделить несколько классов, ГС ИНС должна присвоить каждому наблюдению один из классов или, в более общем случае, оценить вероятность того, что наблюдение принадлежит каждому из классов. В ситуации, когда классифицируемый входной сигнал не совпадает ни с одной из выборок (например, нарушен случайным помехами), в ГС ИНС производится процесс распознавания признаков протоколов, а позже в результате распознания – классификация.

Предложенная модель ГС ИНС состоит из двух взаимодействующих между собой ИНС. Первая ИНС является генеративной (далее – генератор), и предназначена для формирования некоторой случайной последовательности z признаков протоколов сети передачи данных. Вторая ИНС – дискриминативная (далее – дискриминатор). Дискриминатор выполняет функцию анализатора, который максимально эффективно должен отличать сгенерированную (ложную) последовательность от оригинальной последовательностиx признаков протоколов СПД.

Обозначим генератор как G, а дискриминатор – D. Также имеется определенный набор признаков протоколов X, характеризующих их либо с положительной (в соответсвии с RFC), либо с отрицательной (угрозы, уязвимости) стороны. Пусть на входе дискриминатора случайные входные данные обозначим как z, тогда на выходе дискриминатора будет число x в диапазоне [0:1], обозначающее достоверность или информативность признаков.

Цель генератора будет заключаться в создании максимально адекватной последовательности признаков протоколов СПД, т.е максимизировать $D\big(G(z)\big)$, а целевая функция генератора будет иметь вид:

$$argmax\log D\big(G(z)\big). \tag{1}$$

Тогда, цель дискриминатора будет заключаться не только в распознавании признаков угроз или уязвимостей протоколов, но и в выявлении легитимной последовательности, соответствующей нормальному алгоритму работы протокола, соответствующего RFC. Таким образом целевая функция дискриминатора будет иметь вид:

$$argmax\log D(x) + \log\Big(1 - D\big(G(z)\big)\Big). \tag{2}$$

Учитывая вышесказанное, функционал системы оценки защищенности протоколов СПД заключается в следующем.

Генератор выдает случайные числа из какого-то заданного распределения признаков $P(Z)$, например $N[0, I]$и генерирует из них признаки $X_p = G\big(Z; \theta_g\big)$, которые идут на вход второй сети (дискриминатора).

Дискриминатор получает на вход объекты из выборки X_s и созданные генератором X_p и обучается предсказывать вероятность того, что конкретный признак реальный, выдавая скаляр $D(X; \theta_d)$.

При этом генератор обучается создавать признаки протоколов, которые дискриминатор не отличит от реальных.

Для обучения дискриминатора выполняется k шагов: за шаг обучения дискриминатора параметры θ_d обновляются в сторону уменьшения кросс-энтропии:

$$\theta_d = \theta_d - \nabla_{\theta_d}\Big(log\big(D(X_s)\big) + log\Big(1 - D\big(G(Z)\big)\Big)\Big). \tag{3}$$

Затем следует обучение генератора: обновляются параметры генератора θ_g на предмет увеличения логарифма вероятности дискриминатору присвоить сгенерированному признаку метку реального.

$$\theta_g = \theta_g - \nabla_{\theta_g}\Big(log\Big(1 - D\big(G(Z)\big)\Big)\Big). \tag{4}$$

По сути, процесс обучения суммаризируется в одну формулу, задающую в некотором смысле минимакс-игру между дискриминатором и генератором:

$$\min_G \max_D L(D, G) = E_{x\sim p(x)} log D(x) + E_{z\sim q(z)} log\Big(1 - D\big(G(z)\big)\Big). \tag{5}$$

В [3] показывается, что при достаточной мощности обеих сетей у данной задачи есть оптимум, в котором генератор способен создавать распределение $P_g(X)$, совпадающее с $P(X)$, а для любого x дискриминатор выдает вероятность равную 0,5.

Заключение. Таким образом, разработанная модель протокола СПД в условиях ДКВ позволяет оценить защищенность протокола СПД на основе идентификации признаков протоколов СПД, их ранжирования, кластеризации и классификации. Процесс оценки строится на базе аппарата ГСС, позволяющего автоматизировать процедуры генерации признаков протоколов и их оценки. В итоге применения модели достигается распределение признаков протоколов СПД, позволяющее в дальнейшем оценить их защищенность.

СПИСОК ЛИТЕРАТУРЫ

1. Муханова А. А., Ревнивых А. В., Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 2. С. 55-72.
2. Дементьев В.Е., Чулков А.А. Новые информационные технологии и системы. Сборник научных статей XVI Международной научно-технической конференции. 2019. С. 231-233.
3. Дементьев В. Е. Методика оценки информативности признаков протоколов информационно-телекоммуникационных сетей /Технологии и средства связи. 2016. № 3. С. 42–45.

УДК 004.942

ПОСТРОЕНИЯ СЕТЕЙ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ КАК ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Шинкарёв Семён Александрович, Троцко Алиса Викторовна, Хабарова Карина Андреевна, Кислых Иван Алексеевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: se_men82@mail.ru, k.habarova@rambler.ru, alya_alisa.00@mail.ru, Kislih.Ivan@gmail.com

Аннотация. В настоящее время состояние инфотелекоммуникационных сетей показывает, что возможности традиционных технологий практически исчерпаны. Одним из вариантов развития инфотелекоммуникационных сетей является переход на концепцию программно-конфигурируемых сетей. Программно-конфигурируемый подход предлагает разделить уровень управления и уровень передачи данных путем переноса функций управления на отдельное устройство (контроллер).

Ключевые слова: концепция программно-конфигурируемых сетей; сеть связи специального назначения; контроллер.

CONSTRUCTION OF COMMUNICATION NETWORKS FOR SPECIAL PURPOSES AS SOFTWARE-CONFIGURED NETWORKS

Shinkarev Semyon, Trotsko Alisa, Khabarova Karina, Kislykh Ivan

The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: se_men82@mail.ru, k.habarova@rambler.ru, alya_alisa.00@mail.ru, Kislih.Ivan@gmail.com

Abstract. At present, the state of information and telecommunication networks shows that the capabilities of traditional technologies are almost exhausted. One of the options for the development of into telecommunication networks is the transition to the concept of a configurable networks program. The software-configurable approach offers to separate the control level and the data transfer level by transferring the control function to a separate device (controller)

Keywords: concept of software configurable networks; communication network for special purposes; controller.

Введение. Основной задачей сетей связи специального назначения является обеспечение устойчивой связи в интересах органов государственного управления, обороны страны, безопасности государства и обеспечения правопорядка, как в мирное, так и в военное время. Для решения этой задачи необходимо, чтобы сети связи обладали достаточной пропускной способностью и производительностью.

Согласно исследованиям, объем глобального интернет-трафика вырос более чем в четыре раза за последние несколько лет. Основным фактором роста стал видео-трафик. Его доля превысила 60% в глобальном пользовательском интернет-трафике. Похожая ситуация наблюдается и в сетях связи специального назначения, использование видеоконференцсвязи, передача видео беспилотными летательными аппаратами и многое другое, что требует визуализацию. Все это приводит к увеличению объемов передаваемого трафика и предъявляет новые требования к его передаче, а именно к маршрутизации, конфигурации сетей и управления потоками в ней.

Одним из вариантов решения указанных выше проблем является переход на концепцию программно-конфигурируемых сетей [1].

Программно-конфигурируемая сеть (ПКС) – это новый подход к построению архитектуры сетей связи, при котором уровень управления сетью и уровень передачи данных разделяются за счет переноса функций на отдельное центральное устройство, называемое контроллером.

Программно-конфигурируемые сети (Software Defined Networks, SDN) – одна из самых «горячих» сегодня технологий, вставших на пути коллапса сети, однако, несмотря на то что тема еще относительно нова, вокруг нее уже сформировалось несколько полярных мнений: от полного восторга до скепсиса и клише [2].

Компьютерные сети как основополагающая инфраструктура – стратегический фактор развития современных ИТ, однако архитектура Сети, основы которой закладывались еще в конце 60-х годов, устарела и уже не всегда способна адекватно и эффективно реагировать на новые потребности. Рост количества и разнообразия мобильных устройств, развитие различных технологий беспроводной связи привели к тому, что сегодня число их пользователей превысило число пользователей сетей с фиксированной связью. Однако рост мощности мобильных терминалов стимулирует увеличение вычислительной емкости приложений, что, в свою очередь, требует увеличения пропускной способности каналов связи – объем мобильного трафика растет в геометрической прогрессии, а виды трафика становятся все более разнообразными. По данным ведущих производителей сетевого оборудования, трафик удваивается примерно каждые девять месяцев, что в ближайшие несколько лет приведет к увеличению нагрузки на несколько порядков. В то же время сегодня эффективность доступного спектра частот для мобильных сетей уже близка к насыщению

Для того чтобы справиться со значительным ростом трафика, беспроводные сети должны иметь более плотное покрытие, и если сделать соту небольшой, приблизив мобильного клиента к базовой станции, то это увеличит пропускную способность соты и уменьшит количество пользователей в ней. По оценке экспертов, для этого потребуется в 20 раз увеличить плотность размещения базовых станций. Однако современная сетевая

архитектура плохо приспособлена для поддержки такого плотного трафика. Во-первых, невозможно равномерно увеличить плотность покрытия – базовые станции придется развертывать везде, где это возможно, то есть хаотично. Во-вторых, такой инфраструктурой будет очень сложно управлять, она будет испытывать неравномерные нагрузки, взаимные влияния сот и действие других факторов. В-третьих, плотная инфраструктура очень дорога в развертывании и эксплуатации.

Развитие микропроцессорной техники и телекоммуникаций привело к тому, что сейчас на каждого человека приходится в среднем около 40 чипов, однако появляются все новые сетевые устройства, внесение любых изменений в их существующие конфигурации трудоемко, затратно и практически невозможно без привлечения производителя. Нельзя гарантировать, что программно-аппаратные средства производителя содержат только ту функциональность, которая описана в документации, а в сетях ситуация может быть еще сложнее – такая функциональность может быть распределенной. Средства построения сетей сегодня проприетарны, их основной функционал реализован аппаратно и закрыт для изменений со стороны владельцев сетей.

В архитектуре ПКС выделяется три уровня [3]:

– инфраструктурный уровень, предоставляющий набор сетевых устройств (коммутаторов и каналов передачи данных);

– уровень управления, включающий в себя сетевую операционную систему с установленными поверх нее сетевыми приложениями, которые обеспечивают сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью;

– уровень приложений для гибкого и эффективного управления сетью.

По сравнению с традиционными сетями, данный подход дает следующие преимущества:

Программируемость и гибкость управления сетью, упрощение управления сетью и ее модификации за счет создания новых приложений или изменения существующих, автоматизация управления сетями.

Адаптивность управления сетью, возможность изменять состояние сети в режиме реального времени с учетом изменяющихся условий функционирования.

Упрощение структуры и логики сетевых устройств, поскольку теперь им не требуется обрабатывать огромное количество стандартов и протоколов, а достаточно выполнять только инструкции, полученные от контроллера.

Снижение стоимости сетевой инфраструктуры, в целом связанное с удешевлением модернизации системы и уменьшением энергопотребления.

Основой концепции ПКС является:

– разделение процессов передачи и управления данными (за счет снятия с коммутаторов нагрузки по управлению данными эти устройства направят все свои мощности на ускорение перемещения трафика, что повысит производительность);

– единый, унифицированный, независящий от поставщика интерфейс между уровнем управления и уровнем передачи данных (при использовании протокола взаимодействия между сетевыми устройствами и программно-конфигурируемой сети решается проблема зависимости от сетевого оборудования какого-либо конкретного поставщика, поскольку используется общие абстракции для пересылки пакетов, которые сетевая операционная система использует для управления сетевыми коммутаторами);

– логически централизованное управление сетью, осуществляемое с помощью контроллера с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями (логически-централизованное управление данными в сети предполагает вынесение всех функций управления сетью на отдельный физический сервер, называемый контроллером, который находится в ведении администратора сети).

В настоящее время ПКС строятся на базе специальных коммутаторов, реализующих только функции передачи данных, для управления которыми используют протоколы взаимодействия, например в настоящее время используется протокол OpenFlow.

Заключение. Таким образом, концепция ПКС для построения сетей связи специального назначения (СССН) является перспективным направлением в развитии сетевых технологий. Использование данного подхода позволит повысить производительность и масштабируемость сетей, упростить управления и снизить затраты на оборудование и сетевые приложения. Поэтому необходима дальнейшая оценка целесообразности и эффективности использования данного подхода в построении СССН как ПКС с учетом требований предъявляемых к достоверности, своевременности и безопасности связи, потому что на данный момент основными производителями сетевого оборудования являются западные вендоры (Cisco, HP), что накладывает определенные трудности.

СПИСОК ЛИТЕРАТУРЫ

1. http://www.cisco.com/ (дата обращения 28.01.17)
2. Коломеец А. Е., Сурков Л. В. Программно-конфигурируемые сети на базе протокола OpenFlow // Инженерный вестник 05.05.14 С. 519 – 524
3. Н.Н.Белянина, И.Б. Щербаков. Особенности разработки операторами антикризисных пакетов телекоммуникационных услуг в сегменте B2B. Актуальные проблемы инфотелекоммуникаций в науке А43 и образовании V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; Т. 3 / под ред С.В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. – СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. – 550 с.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

СРАВНЕНИЕ ПОДХОДОВ К ДИАГНОСТИРОВАНИЮ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ ПО ПОКАЗАТЕЛЮ ОПЕРАТИВНОСТИ

Авраменко Владимир Семенович, Маликов Альберт Валерьянович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: vsavr@yandex.ru, mkv.vas@yandex.ru

Аннотация. В статье рассматривается подход к оценке оперативности диагностирования компьютерных инцидентов на основе методов сетевого планирования и управления. Полученные в ходе эксперимента значения продолжительности этапов методики диагностирования позволяют определить математическое ожидание и среднеквадратическое отклонение времени выполнения каждого этапа диагностирования, а также общего времени диагностирования компьютерных инцидентов в инфокоммуникационной системе. Требуемое значение продолжительности диагностирования устанавливается на основе анализа длительности активной фазы нарушений безопасности информации. Применение искусственных нейронных сетей позволяет повысить оперативность анализа компьютерных инцидентов.

Ключевые слова: компьютерный инцидент; оценка оперативности; диагностирование; искусственные нейронные сети; критерий.

COMPARISON OF APPROACHES TO DIAGNOSING COMPUTER INCIDENTS IN INFOCOMMUNICATION SYSTEMS BASED ON EFFICIENCY INDICATOR

Avramenko Vladimir, MalikovAl'bert
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: vsavr@yandex.ru, mkv.vas@yandex.ru

Abstract. The article considers an approach to assessing the efficiency of diagnosing computer incidents based on network planning and management methods. The values obtained during the experiment for the duration of stages of the diagnostic method allow us to determine the mathematical expectation and standard deviation of the execution time of each stage of diagnostics, as well as the total time for diagnosing computer incidents in the infocommunication system. The required duration of diagnostics is determined based on the analysis of the duration of the active phase of information security violations. The use of artificial neural networks makes it possible to improve the efficiency of computer incident analysis.

Keywords: computer incident; efficiency evaluating; diagnostics; artificial neural networks; criterion.

Введение. Одной из основных задач системы защиты информации от несанкционированного доступа и компьютерных атак в инфокоммуникационной системе является оперативное обнаружение и реагирование на возникающие нарушения безопасности информации. После обнаружения компьютерных инцидентов решается задача по их диагностированию. Основными источниками информации для проведения диагностирования служат журналы регистрации событий средств автоматизации и средств защиты информации. Также для уточнения причин или характеристик произошедших действий могут быть задействованы дополнительные источники, например, системы контроля учета доступа в помещение и др. В указанных источниках содержатся признаки нарушения безопасности информации. На основе полученных значений характеристик нарушения безопасности информации принимается решение по реагированию на компьютерные инциденты.

В современных условиях функционирования инфокоммуникационных систем, характеризующихся высокой динамикой проведения кибератак с одной стороны, и высокими требованиями ко времени восстановления систем после сбоев и отказов, резко возросли требования к оперативности диагностирования компьютерных инцидентов. Под оперативностью диагностирования компьютерного инцидента понимается свойство системы диагностирования определять значения характеристик нарушения безопасности за допустимое время. Показателем оперативности диагностирования компьютерного инцидента является вероятность того, что продолжительность диагностирования $t_{д}$ не превысит допустимое значение $t_{ддоп}$, то есть $P(t_{д} \le t_{ддоп})$.

Одним из перспективных путей повышения оперативности диагностирования является автоматизация сбора и анализа признаков нарушения безопасности информации, в том числе и с использованием искусственных

нейронных сетей, применяемых в различных областях деятельности [1, 2]. В работах [3, 4] предложена реализация системы диагностирования компьютерных инцидентов на основе искусственных нейронных сетей. Результаты проведенных исследований указывают на то, что применение обученных искусственных нейронных сетей при решении задачи классификации на множестве значений характеристик нарушения безопасности информации позволяет существенно повысить оперативность диагностирования по сравнению с классическими методами.

Для оценки оперативности диагностирования компьютерных инцидентов в инфокоммуникационных системах целесообразно использовать методику определения оперативности, основанную на использовании методов сетевого планирования и управления. Процесс диагностирования компьютерных инцидентов включает операции (работы), которые удобно представлять сетевым графом с различной степенью детализации.

В общем случае время реализации процесса диагностирования в инфокоммуникационной системе будет складываться из продолжительности операций рассматриваемых этапов.

Время выполнения каждой операции является случайной величиной. На практике для оценки продолжительности операций, ограниченных конечных интервалом, используется бета-распределение в интервале $[t_{\min}, t_{\max}]$, $t_{\min}$ – минимальное время решения задачи; $t_{\max}$ – максимальное время решения задачи.

При этом ожидаемая продолжительность операции и дисперсия вычисляются по формулам [5]:

$$t_{\text{ож}} = \frac{3t_{\min} + 2t_{\max}}{5},\ \sigma^2(t) = 0.4(t_{\max} - t_{\min})^2.$$

Вероятность того, что продолжительность совокупности операций не превысит запланированного срока $t_{\text{д тр}}$ вычисляется по формуле $P_{\text{д}}(t_{\text{д}} \le t_{\text{д тр}}) = \Phi(Z)$, где $\Phi(Z)$ – значение функции Лапласа, заданное таблично, $Z = (t_{\text{д тр}} - t_{\text{ожΣ}}) / \sqrt{\sum_{i=1}^{n} \sigma^2(t_{\text{д}})}$, $t_{\text{ожΣ}}$ - ожидаемая продолжительность по всем этапам методики.

На основании данных, полученных в ходе экспериментов по диагностированию компьютерных инцидентов на стенде, имитирующем основные элементы инфокоммуникационных систем, был произведен расчет вероятности выполнения операций по диагностированию за установленное время.

В ходе функционирования типовой инфокоммуникационной системы, исходя из продолжительности активной фазы компьютерных атак и прочих нарушений безопасности информации, на диагностирование отводится не более 20 минут, т.е. $t_{\text{д тр}} = 20$ мин. В этом случае для традиционного подхода к диагностированию получаем значение аргумента $Z \approx 0{,}84$, а для подхода с применением искусственных нейронных сетей $Z \approx 1{,}89$

Используя значения функции Лапласа $\Phi(Z)$, заданные таблично, значение вероятности диагностирования компьютерных инцидентов за время, не превышающее требуемое значение при $t_{\text{д тр}} = 20$ мин, составляет для классического подхода $P_{\text{д}}(t_{\text{д}} \le t_{\text{д тр}}) = 0{,}8$, а для нейросетевого – $P_{\text{д}}(t_{\text{д}} \le t_{\text{д тр}}) = 0{,}97$. Таким образом, значение показателя оперативности нейросетевого диагностирования компьютерных инцидентов более чем на 20% ($\frac{0{,}97 - 0{,}8}{0{,}8} = 0{,}21$) превосходит значение показателя оперативности диагностирования компьютерных инцидентов при применении классического подхода, основанного на визуальном просмотре журналов событий.

При этом в ходе диагностирования компьютерных инцидентов на основе искусственных нейронных сетей осуществляется определение значений сразу нескольких характеристик нарушения безопасности, в то время как при классическом диагностировании количество определяемых значений напрямую зависит от компетентности и опыта администратора.

Заключение. Оценка оперативности диагностирования компьютерных инцидентов на основе методов сетевого планирования и управления позволяет сделать вывод о превосходстве нейросетвого подхода к диагностированию компьютерных инцидентов в инфокоммуникационных системах над классическим подходом. Применение многослойных ИНС позволяет обеспечить определение значений целого спектра характеристик нарушения безопасности, что весьма актуально в условиях неопределенности сценариев реализации нарушений безопасности и скоротечности их активных фаз.

СПИСОК ЛИТЕРАТУРЫ

1. Михайличенко, Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных // Системы управления, связи и безопасности. 2019. № 1. С.54-66.
2. Михайличенко, Н.В., Паращук, И.Б. Особенности применения нейро-нечетких моделей для систем поддержки принятия решений в задачах оценки эффективности функционирования специализированных дата-центров // Журнал «Информация и космос» № 1, 2019. С.84-88.
3. Маликов, А.В., Авраменко, В.С., Саенко, И.Б. Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы, 2019, № 6. С.32–42.
4. Авраменко, В.С. Маликов, А.В. Диагностирование компьютерных инцидентов безопасности на основе комбинированной искусственной нейронной сети // Защита информации. Инсайд. 2019. № 6. С.72 – 76.
5. Плескунов, М. А. Задачи сетевого планирования: учебное пособие /М. А. Плескунов. – Екатеринбург: Изд-во. Урал. ун-та, 2014. – 92 с.

УДК 004.056

HONEYPOT-РЕШЕНИЯ КАК ИНСТРУМЕНТ БЕЗОПАСНОСТИ ДЛЯ КОРПОРАТИВНЫХ СЕТЕЙ

Акилов Марк Валерьевич, Кушнир Дмитрий Викторович, Андрианов Владимир Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: saintgnome047@gmail.com, dmitry.kushnir@gmail.com, vladimir.i.andrianov@gmail.com

Аннотация. Honeypot и honeynet - это нетрадиционные инструменты безопасности для изучения методов, инструментов и целей злоумышленников. Таким образом, анализ данных является важной частью honeypot и honeynet. В статье акцентируется внимание на анализе данных, собранных с разных приманок. Представлена статистика атак на основе данных, собранных honeypot в результате выполненного эксперимента.

Ключевые слова: honeypot, honeynet, анализ данных, сбор данных.

HONEYPOT SOLUTIONS AS A SECURITY TOOL FOR CORPORATE NETWORKS

Akilov Mark, Kushnir Dmitry, Andrianov Vladimir
Bonch-Bruevich Saint-Petersburg state university of communication
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: saintgnome047@gmail.com, dmitry.kushnir@gmail.com, vladimir.i.andrianov@gmail.com

Abstract. Honeypots and honeynets are unconventional security tools to study techniques, methods, tools, and targets of attackers. Therefore, data analysis is an important part of honeypots and honeynets. The article focuses on the analysis of data collected from different honeypots. The statistics of attacks based on data collected by the honeypot as a result of the performed experiment are presented.

Keywords: honeypot, honeynet, data analysis, data collection.

Традиционные способы защиты (такие как, межсетевые экраны, IDS, IPS) становятся все менее эффективными. Это связано с изменяющимся характером поведения, методов и инструментов злоумышленников. Поэтому злоумышленники на несколько шагов опережают защитные механизмы. С этой точки зрения необходимо найти новые подходы для защиты информации и инфраструктуры организаций. Одним из эффективных подходов к их защите является концепция honeypot и honeynet.

Honeypot (приманка с англ.) - это «вычислительный ресурс, ценность которого в том, чтобы быть атакованным» [2]. Ланс Шпицнер определяет honeypot как «ресурс информационной системы, ценность которого заключается в его компрометации или незаконном использовании» [2]. Honeypot - полезный инструмент для изучения, процедур, целей и методов злоумышленников. Приманки классифицируются в соответствии с их ролью и уровнем взаимодействия.

Согласно первой классификации, приманки подразделяются на honeypot на стороне сервера, и honeypot, реализуемые на стороне клиента. Серверные приманки полезны для обнаружения новых эксплойтов, сбора вредоносных программ и обогащения исследований анализа угроз (например, Conpot) [3]. С другой стороны, приманки для атак на стороне клиента называются клиентскими (например, Thug). Основным мотивом приманок на стороне клиента является выявление и обнаружение вредоносных действий в Интернете.

Вторая классификация основана на уровне взаимодействия. Уровень взаимодействия может быть определен, как диапазон возможностей, которые honeypot предоставляет злоумышленнику. Honeypot с низким уровнем взаимодействия обнаруживают злоумышленников, используя программную эмуляцию характеристик конкретной операционной системы и сетевых служб в операционной системе хоста. Преимущество такого подхода заключается в улучшении контроля над действиями злоумышленника, поскольку злоумышленник ограничен программным обеспечением, работающим в операционной системе хоста. С другой стороны, недостатком подхода является тот факт, что honeypot с низким уровнем взаимодействия эмулирует службу или пару служб, но не эмулирует полную операционную систему. Примерами такого типа приманок являются программные продукты Dionaea, Honeyd. Honeypot со средним уровнем взаимодействия предлагают злоумышленникам больше возможностей для взаимодействия с операционной системой, чем с низким уровнем взаимодействия, но с меньшей функциональностью, чем решения с высоким уровнем взаимодействия. Примером такого типа приманки является программный продукт Kippo.

Чтобы получить больше информации о злоумышленниках, их методах и атаках, применяется полная операционная система со всеми сервисами. Этот тип приманки называется приманкой с высоким уровнем взаимодействия. Основная цель этого типа honeypot - предоставить злоумышленнику доступ к реальной операционной системе. Примерами такого типа приманок являются программные продукты HonSSH, Sebek. Концепция honeypot получила расширение в honeynet, который определяется как «строго контролируемая сеть honeypot» [1-2].

На практике реализуется Honeynet, работающая на одном компьютере в виртуальной среде. Этот тип honeynet определяется, как виртуальный honeynet. Чтобы успешно развернуть honeynet, необходимо правильно развернуть его архитектуру [4]. Не существует «единого правила того, как следует развертывать эту архитектуру». Выделены три основных функции, которые определяют архитектуру honeynet:

Сбор данных отслеживает и регистрирует все действия злоумышленника в рамках honeynet.

Контроль данных, целью которого является контроль и сдерживание активности злоумышленника.

Сбор данных - все данные собираются и хранятся в одном центральном месте. Первые две основные функции являются наиболее важными, и они применимы к каждому развертыванию Honeynet. Последняя функция - сбор данных - применяется организацией в случае, если в распределенных средах у организации есть несколько сетей связи.

СПИСОК ЛИТЕРАТУРЫ

1. Виткова Л.А., Исаков А.С., Ковцур М.М. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 182-186.
2. Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях, «Труды учебных заведений связи». 2019. Т. 5. № 3. С. 86-97.
3. Ковцур М.М., Ахрамеева К.А., Юркин Д.В., Акилов М.В., Сравнительный анализ современных Honeypot решений для корпоративных сетей 2020 научный журнал «Аллея Науки» Т. 1 ISSN 2587-6244 С. 768-771
4. Виткова Л.А., Герлинг Е.Ю., Головлёва Ю.А., Ковцур М.М. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 140-142.

УДК 004.056.52

ДОКАЗАТЕЛЬСТВО С НУЛЕВЫМ РАЗГЛАШЕНИЕМ В СИСТЕМАХ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Александрова Елена Борисовна, Шматов Вадим Сергеевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: helen@ibks.spbstu.ru, shmatov96@mail.ru

Аннотация. С повышением популярности систем электронного голосования возрастают и требования к обеспечению безопасности. Перспективным подходом являются протоколы с нулевым разглашением. В статье рассматриваются современные универсальные протоколы. Выполняется анализ их недостатков и ограничений при применении в системах электронного голосования. Приводятся перспективные направления исследований в этой области.

Ключевые слова: электронное голосование; нулевое разглашение; постквантовая криптография.

ZERO-KNOWLEDGE PROOF IN E-VOTING SYSTEMS

Aleksandrova Elena, Shmatov Vadim
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: helen@ibks.spbstu.ru, shmatov96@mail.ru

Abstract. As the popularity of e-voting systems increases, so do the security requirements. Zero knowledge protocols are a promising approach. The article reviews modern universal protocols. The analysis of their shortcomings and limitations in relation to e-voting systems is carried out. The promising directions of further research in this area are given.

Keywords: e-voting; zero knowledge; post-quantum cryptography.

В наши дни наблюдается активное внедрение систем электронного голосования в различные области повседневной жизни. Например, согласно данным ЦИК, более миллиона россиян проголосовали онлайн по поправкам в Конституцию в 2020 году. Со временем популярность электронного голосования в государственной и корпоративной сферах будет только возрастать, поэтому вопросы обеспечения безопасности при проведении голосований становятся все актуальнее. Важными свойствами в любой системе являются тайна голосования, нефальсифицируемость и возможность публичной проверки результатов. Добиться выполнения всех этих свойств можно при помощи протоколов с нулевым разглашением. Целью работы является исследование возможности применения универсальных протоколов доказательства с нулевым разглашением для проведения электронного голосования. Для этого рассматриваются современные протоколы, анализируются их свойства и ограничения, выполняется оценка возможности их использования в системах голосования.

Протоколы с нулевым разглашением делятся на два класса – специальные и универсальные. Специальные предназначены для решения одной прикладной задачи, а универсальные позволяют доказать любое истинного утверждение для NP-полного языка. Преимуществом специальных протоколов является высокая производительность, но при их использовании для электронного голосования возникают две проблемы. Во-первых, сфера электронных голосований активно развивается, и требования к системам голосования постоянно уточняются. Каждое изменение требований может приводить к необходимости разработки нового специального протокола и изучению его свойств. Для универсального протокола изменится лишь описание доказываемого предиката. Во-вторых, специальные протоколы используются в меньшем количестве систем из-за узкой направленности, поэтому они в целом меньше изучены, чем универсальные.

Идея универсальных доказательств с нулевым разглашением довольно стара, но до недавнего времени не существовало протоколов, применимых на практике. Одним из первых эффективных протоколов стал Bulletproof [1]. В нем доказываемое утверждение представляется в виде арифметической схемы – множества операций сложения и умножения, каждая из которых принимает на вход два значения с определенными весами и возвращает третье значение, идущее на вход другим операциям или на выход схемы в целом. Эта схема конвертируется в систему ограничений первого ранга (rank 1 constraint system, R1CS). Затем выполняется «выравнивание» – преобразование системы в единое равенство. Наконец, для этого равенства доказывающая сторона может вычислить аргумент с нулевым разглашением, используя протокол подтверждения скалярного произведения [2]. Стойкость Bulletproof основана на задаче дискретного логарифмирования. Размер доказательства составляет $O(\log N)$, где N – число умножений в алгебраической схеме, сложность создания и проверки доказательств равна $O(N \cdot \log N)$. Таким образом, проверка множества доказательств может потребовать значительных затрат ресурсов.

Эту проблему решает протокол Pinocchio [3], основанный на zk-SNARK [4]. Его стойкость также определяется сложностью задачи дискретного логарифмирования в группе точек эллиптической кривой. Для оптимизации в нем вместо самой алгебраической схемы используется ее сжатое представление – ключи для создания и проверки доказательств. Благодаря этому размер и сложность проверки доказательства постоянны и не зависят от N. Основным недостатком является то, что для создания ключей требуется доверенная инициализация.

Ни Bulletproof, ни Pinocchio не защищены от атак квантового компьютера – задача дискретного логарифмирования может быть легко решена с помощью алгоритма Шора [5]. Квантовая угроза вызвала интерес к поиску универсальных протоколов с нулевым разглашением, основанных на постквантовых примитивах. Например, в [6] предлагается версия zk-SNARK, в которой ключи и доказательства представляют собой не точки эллиптической кривой, а шифртексты криптосистемы на решетках [7]. К сожалению, эффективного алгоритма спаривания на решетках нет, поэтому при проверке доказательства требуется ключ для расшифрования. Из-за этого проверяющая сторона может подделывать доказательства, что является неприемлемым для систем электронного голосования.

Другой протокол, также основанный на решетках, описан в [8]. Он не требует доверенной инициализации или стороны, но размер доказательства в нем составляет $O\left(\sqrt{N \log^3 N}\right)$, сложность проверки – $O(N)$. Это затрудняет практическое использование данного протокола.

Принципиально другой подход к построению постквантовых схем доказательства с нулевым разглашением основан на усилении ошибок. Основная идея этого метода заключается в том, чтобы увеличить размер доказательства с помощью интерполяции и тем самым существенно увеличить вероятность обнаружения ошибки в доказательстве при изучении даже небольшой его части. Благодаря созданию обязательства с помощью дерева Меркла [9] и раскрытия лишь малой части доказательства достигается небольшой итоговый размер и высокая скорость проверки.

Один из протоколов, использующий описанный выше метод, – zk-STARK [10]. Он позволяет сгенерировать доказательство размером $O(\log^2 N)$ со сложностью проверки $O(\log^2 N)$. Наибольшая эффективность достигается при доказательстве корректности вычисления рекурсивной функции, так как в zk-STARK интерполируется последовательность значений некоторой функции. Это может быть полезно для построения функции проверяемой задержки, но с трудом применимо к процедуре электронного голосования.

Усиление ошибки также используется в протоколе Aurora [11]. В отличие от zk-STARK, этот метод комбинируется с протоколом проверки суммы [12], что позволяет построить доказательство для системы ограничений первого ранга. Размер доказательства также равен $O(\log^2 N)$, а сложность проверки выше, чем у zk-STARK из-за отсутствия «сжатия» алгебраической схемы – $O(N)$. Кроме того, для выполнения интерполяции и усиления ошибок доказывающей стороне требуется большой объем памяти, что накладывает ограничения на устройства, которые могут генерировать доказательства.

Таким образом, использование универсальных протоколов с нулевым разглашением представляется целесообразным для обеспечения безопасности голосований. Наиболее эффективные протоколы основаны на операциях в циклических группах и уязвимы к квантовым атакам. Безопасность постквантовых протоколов обеспечивается либо криптографией на решетках, либо усилением ошибки и хэш-функциями. Наиболее эффективные из постквантовых протоколов, такие как Aurora, могут использоваться для проведения голосований, но все же требуют высокой вычислительной мощности от участников. Поэтому построение новых эффективных протоколов с нулевым разглашением остается перспективным направлением исследований. Кроме того, возможность использования некоторых постквантовых примитивов, таких как изогении суперсингулярных эллиптических кривых, для построения доказательств до сих пор не исследована.

СПИСОК ЛИТЕРАТУРЫ

1. Bünz B. et al. Bulletproofs: Short proofs for confidential transactions and more //2018 IEEE Symposium on Security and Privacy (SP). – IEEE, 2018. – С. 315-334.
2. Bootle J. et al. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2016. – С. 327-357.
3. Parno B. et al. Pinocchio: Nearly practical verifiable computation //2013 IEEE Symposium on Security and Privacy. – IEEE, 2013. – С. 238-252.
4. Gennaro R. et al. Quadratic span programs and succinct NIZKs without PCPs //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2013. – С. 626-645.
5. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer //SIAM review. – 1999. – Т. 41. – №. 2. – С. 303-332.

6. Gennaro R. et al. Lattice-based zk-SNARKs from square span programs //Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. – 2018. – С. 556-573.
7. Brakerski Z., Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE //SIAM Journal on Computing. – 2014. – Т. 43. – №. 2. – С. 831-871.
8. Baum C. et al. Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits //Annual International Cryptology Conference. – Springer, Cham, 2018. – С. 669-699.
9. Merkle R. Secrecy, authentication, and public key systems //Ph. D. Thesis, Stanford University. – 1979.
10. Ben-Sasson E. et al. Scalable, transparent, and post-quantum secure computational integrity //IACR Cryptol. ePrint Arch. – 2018. – Т. 2018. – С. 46.
11. Ben-Sasson E. et al. Aurora: Transparent succinct arguments for R1CS //Annual international conference on the theory and applications of cryptographic techniques. – Springer, Cham, 2019. – С. 103-128.
12. Lund C. et al. Algebraic methods for interactive proof systems //Journal of the ACM (JACM). – 1992. – Т. 39. – №. 4. – С. 859-868.

УДК 621.391, 004.056

ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ ВСЕПРОНИКАЮЩИХ СЕНСОРНЫХ СЕТЕЙ

Астахова Татьяна Николаевна[1], Колбанев Михаил Олегович[2], Романова Анна Александровна[1,2]
[1] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
[2] Санкт-Петербургский государственный электротехнический университет
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: mokolbanev@mail.ru, anya-romanova-07@yandex.ru, ctn_af@mail.ru

Аннотация. В работе рассмотрена энергетическая безопасность всепроникающих сенсорных сетей. Приведены показатели связанности сети, зависящие от пространственных, временных и энергетических параметров.

Ключевые слова: вероятность связности; всепроникающая сенсорная сеть; энергетическая безопасность.

ENERGY SECURITY OF UBIQUITOUS SENSOR NETWORKS

Astakhova Tatyana[1], Kolbanev Mikhail[2], Romanova Anna[1,2]
[1] Nizhny Novgorod State University of Engineering and Economics
22a Oktyabrskaya St, Knyaginino, 606340, Russia
[2] Saint-Petersburg Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: mokolbanev@mail.ru, anya-romanova-07@yandex.ru, ctn_af@mail.ru

Abstract. The energy security of ubiquitous sensor networks is discussed in the paper. The indicators of network connectivity depending on the spatial, time and energy parameters are given.

Keywords: connectivity probability; ubiquitous sensor network; energy security.

Введение. Всепроникающие сенсорные сети представляют собой важную часть критической инфраструктуры многих объектов. От их работы зависит безопасность выполнения разнообразных экологических, техносферных, транспортных, энергетических и других процессов. Одним из ключевых критериев эффективности функционирования беспроводных сенсорных сетей является ее способность обеспечить передачу данных с определенным уровнем качества доставки.

Безопасность самих всепроникающих сенсорных сетей определяется надежностью сенсорных устройств, способом защиты собираемых данных, защищённостью от перегрузок, а также от уровня энергопотребления устройств, имеющих автономное питание [1, 2]. Последнее обстоятельство требует исследования энергетической безопасности всепроникающих сенсорных сетей, т.е. таких состояний их энергетической подсистемы, при которых сеть выполняет свои функции с заданным качеством.

Энергетическая безопасность беспроводных сенсорных сетей может быть определена как состояние защищённости каждого элемента (транзитного узла, сенсорного устройства, сетевого элемента и т.д.) от угроз, которые лишают сеть качественно выполнять свою функцию.

Одной из характеристик, которая позволяет оценить энергетическую безопасность сети, является связанность сети, зависящая от пространственных, временных и энергетических параметров [3, 4].

В работе в качестве показателей связанности предлагается использовать стохастическую характеристику качества функционирования беспроводных сенсорных сетей, которая отражает способность сети устанавливать соединения между сетевыми элементами в пределах границ сенсорного поля в реальном масштабе времени и учитывать электропотребление сенсорными устройствами.

При определении связности беспроводных сенсорных сетей необходимо учитывать не только выбранную топологию, сетевые перегрузки и надежность сетевых элементов, но и емкость электрических батарей каждого из устройств, поскольку к нарушению связности могут привести: разрывы соединений в моменты окончания запаса энергии батареи одного из сетевых элементов, невозможность установления соединений из-за ограниченной мощности сигнала на передающей антенне сенсорного устройства и слишком больших расстояний от него до соседних сетевых элементов.

Показателями связности беспроводной сенсорной сети выбраны следующие вероятностно-временные характеристики процесса информационного взаимодействия сенсорных устройств друг с другом и с головным

узлом, рассчитываемые при заданном уровне энергопотребления устройствами и размерах сенсорного поля, вероятность связности сети, время доставки сообщений до головного узла кластера беспроводной сенсорной сети.

Заключение. Таким образом, рассмотрен показатель связности, который охватывает в комплексе пространственные, временные и энергетические характеристики сети, что позволяет с общих позиций описать широкий комплекс задач энергетической безопасности, возникающих при исследовании процессов функционирования беспроводных сетей на этапах сбора, распространения и обработки данных сенсорными устройствами. Предложенные показатели позволяют повысить точность оценки качества функционирования всепроникающей сенсорной сети и ее защищенности от угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н. А., Колбанёв М. О., Шамин А. А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях. // Информационные технологии и телекоммуникации. Том 5, №1, 2017. С. 88-96.
2. Астахова Т. Н., Колбанев М. О., Шамин А. А. Обеспечение энергоэффективности интернета вещей. // Региональная информатика и информационная безопасность: сборник научных трудов. Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2018. С. 203-204.
3. Astakhova T., Verzun N., Kolbanev M., Shamin A. A model for estimating energy consumption seen when nodes of ubiquitous sensor networks communicate information to each other. // Proceedings of the 10th Majorov International Conference on Software Engineering and Computer Systems, Saint Petersburg, Russia, December 20-21, 2018. – Available: http://ceur-ws.org/Vol-2344/paper5.pdf.
4. Астахова Т.Н., Верзун Н.А., Колбанев М.О., Полянская Н.А., Шамин А.А. Вероятностно-энергетические характеристики взаимодействия умных вещей. // Вестник НГИЭИ. № 4 (95). 2019. С. 66-77.

УДК 004.056

ПОДХОД К ЗАЩИТЕ БЛОКЧЕЙН-СИСТЕМ ОТ УГРОЗ, ОБУСЛОВЛЕННЫХ НЕРАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ ВЫЧИСЛИТЕЛЬНЫХ МОЩНОСТЕЙ

Бусыгин Алексей Геннадьевич, Калинин Максим Олегович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: a.busygin@ibks.spbstu.ru, max@ibks.spbstu.ru

Аннотация. Предложен подход к защите блокчейн-систем от угроз, обусловленных неравномерным распределением вычислительных мощностей. Подход основан на анализе изменений общей вычислительной мощности блокчейн-системы.

Ключевые слова: информационная безопасность; блокчейн; неравномерное распределение вычислительных мощностей; оценка вычислительной мощности.

APPROACH TO PROTECTION OF BLOCKCHAIN SYSTEMS AGAINST THREATS CAUSED BY UNEVEN DISTRIBUTION OF COMPUATIONAL POWER

Busygin Alexey, Kalinin Maxim
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: a.busygin@ibks.spbstu.ru, max@ibks.spbstu.ru

Abstract. An approach to protection of blockchain systems against threats caused by uneven distribution of computational power is proposed. The approach is based on analysis of blockchain system computational power changes.

Keywords: information security; blockchain; uneven distribution of computational power; computational power assessment.

Блокчейн является одной из основных технологий построения распределённых реестров, применяемых для защищённой обработки данных финансовых транзакций, ценных бумаг, юридически значимых документов, систем доменных имён, инфраструктур открытых ключей, логистических и иных систем. Блокчейн-системы подвержены угрозам информационной безопасности, обусловленным неравномерным распределением вычислительных мощностей. Примером реализации таких угроз является «атака большинства» («атака 51%»).

На данный момент предложен ряд способов защиты от данной угрозы. В работе [1] приведён анализ данных способов защиты, показаны их недостатки и ограничения.

В работе [2] предложена модель предложена модель, позволяющая выполнить оценку общей вычислительной мощности блокчейн-системы. В данной работе предлагается использование данной модели для оценки вычислительной мощности блокчейн-системы по следующей формуле:

$$H_i = \frac{2^n k}{h_{max}(t_i - t_{i-k})}, \quad (1)$$

Где H_i — оценка общей вычислительной мощности блокчейн-системы в момент генерации i-ого блока, n — размер в битах значений криптографической хэш-функции, используемой для цепной связи блоков, h_{max} — минимальное значение хэш-образа блока, определяющее сложность генерации нового блока, t_j — время

генерации j-ого блока, k — число предшествующих блоков, учитываемых при расчёте вычислительной мощности сети.

В рамках используемой модели для реализации рассматриваемой в данной работе угрозы нарушителю необходимо переключить контролируемые вычислительные мощности с генерации основной цепи блоков, на генерацию альтернативной цепи блоков. В результате будет наблюдаться изменение общей вычислительной мощности блокчейн-системы ΔH, приведённое на рис. 1 и соответствующее вычислительной мощности, контролируемой нарушителем.

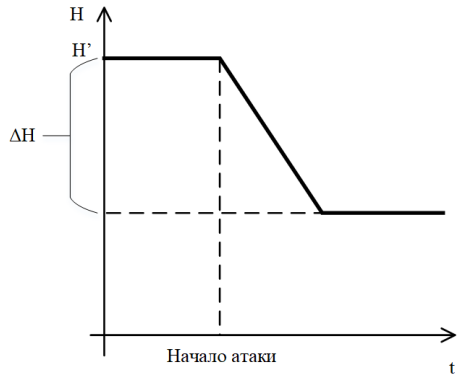

Рис. 1. Оценка вычислительной мощности, контролируемой нарушителем

Если вероятность успешной реализации угрозы превысит некоторое пороговое значение, то текущее состояние блокчейн-системы (последний подтверждённый блок) фиксируется с помощью механизма контрольных точек. Зафиксированное состояние не может быть изменено, что обеспечивает его защищённость.

Оценка вероятности успешной реализации угрозы может быть выполнена по следующей формуле, приведённой в работе [3]. В рамках используемой модели в качестве значения параметра p выбирается следующее:

$$p = \frac{\Delta H}{H'}. \quad (2)$$

Подход основан на предположении о замкнутости блокчейн-системы (нарушитель не может получить приращения вычислительной мощности, сравнимого с общей вычислительной мощностью блокчейн-системы, за счёт подключения новых вычислительных ресурсов). Данное предположение справедливо для крупных блокчейн-систем. Таким образом, данный подход может быть применён к крупным блокчейн-системам, для которых данное предположение справедливо.

Работа выполнена в рамках Государственного задания на проведение фундаментальных исследований (код темы 0784-2020-0026). Дополнительное соглашение к Соглашению о предоставлении субсидии из федерального бюджета на финансовое обеспечение выполнения государственного задания на оказание государственных услуг (выполнение работ) № 075-03-2020-158/2 от 17.03.2020 г. (внутренний номер 075-ГЗ/Щ4575/784/2).

СПИСОК ЛИТЕРАТУРЫ

1. Sayeed S., Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack // Applied Sciences. 2019, vol. 9, №9. P. 1788.
2. А.Г. Бусыгин. Модель основанной на технологии блокчейн системы для оценки защищённости от угроз, обусловленных неравномерным распределением вычислительных мощностей // Проблемы информационной безопасности. Компьютерные системы. 2019, №4. С. 114-117.
3. Nakamoto S. Bitcoin: A peer-to-Peer Electronic Cash System // Bitcoin.org [Электронный ресурс]. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 01.12.2019).

УДК 004.056.5

ПОДХОД К РАЗГРАНИЧЕНИЮ ДОСТУПА К ИНФОРМАЦИИ В СИСТЕМЕ МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Бушуев Сергей Николаевич[1], Саенко Игорь Борисович[2]

[1] Акционерное общество «Научно производственное предприятие ТЕЛДА»
Белоостровская ул., 25, Санкт-Петербург, 197342, Россия,
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: bsn5688@yandex.ru, ibsaen@comsec.spb.ru

Аннотация. Рассмотрен подход к разграничению доступа к информации в системе мониторинга чрезвычайных ситуаций, базирующийся на использовании модели разграничения доступа, основанной на атрибутах. Приведены особенности предлагаемой модели разграничения доступа. Сформулированы цели и функциональные задачи системы мониторинга, которые следует учитывать в системе разграничения доступа. Выявлены основные группы атрибутов, которые используются в предложенной модели разграничения доступа. Обсуждаются вопросы реализации и экспериментальной оценки разработанной системы разграничения доступа для системы мониторинга чрезвычайных ситуаций.

Ключевые слова: разграничение доступа, система мониторинга, чрезвычайная ситуация, критически важная информационная система.

AN APPROACH TO INFORMATION ACCESS CONTROL IN THE EMERGENCY MONITORING SYSTEM

Bushuev Sergey[1], Saenko Igor[2]

[1] Joint-Stock Company «Scientifically manufacturing enterprise TELDA»
25, Beloostrovskaya St, St. Petersburg, 197342, Russia

[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

e-mails: bsn5688@yandex.ru, ibsaen@comsec.spb.ru

Abstract. An approach to information access control in an emergency monitoring system based on the use of an attribute-based access control model is considered. The features of the proposed model of access control are given. The goals and functional tasks of the monitoring system are formulated, which should be taken into account in the access control system. The main groups of attributes that are used in the proposed access control model are identified. The issues of implementation and experimental evaluation of the developed access control system for the emergency monitoring system are discussed.

Keywords: access control, monitoring system, emergency situation, critical information system.

Введение. Системы мониторинга чрезвычайных ситуаций представляют собой особый вид критически важных информационных систем, которые характеризуются повышенным вниманием к использованию информационных технологий и обладают повышенными требованиями к безопасности обрабатываемой информации. Повышение совокупной стоимости активов устройств, программного обеспечения и критически важных данных таких систем, а также увеличение числа атак на них определяют актуальность задач разграничения доступа к информации в системах мониторинга чрезвычайных ситуаций, а также обнаружения и разрешения конфликтов в используемых ими политиках разграничения доступа.

Считается, что одним из центральных вопросов построения систем мониторинга чрезвычайных ситуаций является качественное решение проблемы разграничения доступа. Эта проблема является одной из составляющих общей проблемы обеспечения безопасности информации в таких системах. Однако недостатком большинства существующих критически важных информационных систем является отсутствие возможности гибкого управления со стороны пользователей доступом к своим данным, что вызвано универсальностью решений по контролю доступа [1]. Неоднородность и большое разнообразие ресурсной среды в системе мониторинга чрезвычайных ситуаций требуют всестороннего и детально проработанного механизма управления доступом, чтобы обеспечить динамические, постоянно расширяемые и хорошо настраиваемые требования по защите информации [2]. Однако существующие механизмы безопасности, как правило, реализуемые в критически важных информационных системах, не удовлетворяют этим требованиям [3]. Кроме того, проблемы безопасности информации в системах мониторинга чрезвычайных ситуаций обостряются, если используются открытые веб-сервисы [4]. Все это требует проработки вопросов совершенствования политик разграничения доступа и моделей, лежащих в их основе.

Предлагаемая система разграничения доступа к информации ориентирована на реализацию следующих возможностей системы мониторинга чрезвычайных ситуаций. Основными целями функционирования такой системы являются: снижение рисков возникновения чрезвычайных ситуаций, в том числе вероятности их возникновения, а также причиняемого вреда жизни и здоровью сотрудников и материального ущерба, создание единого информационного поля обеспечения, координации и согласованного взаимодействия подсистем подразделений, входящих в систему мониторинга чрезвычайных ситуаций, предоставление объективной, своевременной и полной информации о состоянии текущей, оперативной и общей обстановки на контролируемых объектах как в повседневном режиме, так и в условиях чрезвычайных ситуаций, повышение своевременности реагирования, качества управленческих решений эффективности действий оперативных служб, сил и средств при локализации и ликвидации чрезвычайных ситуаций.

Основными функциональными задачами такой системы являются: мониторинг функционирования и производственной деятельности, состояния защищенности объектов в режиме круглосуточного дежурства с целью обеспечения информацией должностных лиц,обработка информации о функционировании и производственной деятельности, состоянии защищенности объектов, информационное обеспечение в условиях чрезвычайной ситуации, методическое обеспечение круглосуточного мониторинга функционирования и производственной деятельности, состояния защищенности объектов, предупреждения и ликвидации чрезвычайных ситуаций с задействованием информационно-аналитической системы, а также некоторые другие задачи.

Для обеспечения безопасности информации при решении такого разнородного комплекса задач необходимо построение системы разграничения доступа к обрабатываемым данных, основанной на более гибкой, чем известные, модели разграничения доступа. В качестве таковой модели выбрана модель разграничения доступа, основанная на атрибутах (Attribute-Based Access Control, ABAC) [5, 6]. Эта модель выделяет атрибуты объектов, действий, субъектов и условий доступа. При применении этой модели значения атрибутов сравниваются с политикой безопасности, после этого принимается соответствующее решение о предоставлении доступа. Атрибутивная модель учитывает, что крупная информационная система, как правило, состоит из нескольких более мелких систем, изначально имеющих различные модели безопасности.

Для построения предлагаемой системы разграничения доступа в системе мониторинга чрезвычайных ситуаций был произведен анализ предметной области, который позволил сформировать несколько ключевых групп атрибутов. Эти группы включали характеристики контролируемых объектов, данные о силах и средствах ликвидации последствий чрезвычайных ситуаций, сведения о пользователях системы мониторинга, а также сведения о правилах, образующих политики безопасности.

В качестве примера реализации предложенной системы разграничения доступа к информации в системе мониторинга чрезвычайных ситуаций была выбрана предметная область мониторинга состояния гидротехнических объектов. Эта система обеспечивает сбор технологической и других видов информации от соответствующих систем гидроэлектростанций и региональных центров мониторинга, её анализ, информирование руководства о состоянии объектов электроэнергетики, мониторинг технологических нарушений, выявление чрезвычайных ситуаций, а также контроль за ходом мероприятий по их устранению. Система представляет собой автоматизированный комплекс, ориентированный на прямое и непрерывное обеспечение органов управления о возможных производственных, экономических, информационных и других угрозах безопасности и функционированию контролируемых объектов. Взаимосвязь между компонентами системы обеспечивается путем передачи между программными модулями подсистем соответствующих наборов данных. В каждой подсистеме создается интерфейс, обеспечивающий передачу и прием данных в соответствующих форматах.

Экспериментальная оценка предлагаемой системы разграничения доступа продемонстрировала ее более высокую эффективность по сравнению с известными решениями, применяемыми в системах мониторинга подобного типа.

Заключение. Предложенный подход к разграничению доступа к информации в системах мониторинга чрезвычайных ситуаций, основанный на применении модели ABAC, обеспечивает более высокую эффективность функционирования такой системы. Дальнейшие исследования связываются с распространением полученных решений на более широкую область критически важных информационных систем.

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01369) в СПИИРАН и бюджетной темы 0073-2019-0002.

СПИСОК ЛИТЕРАТУРЫ

1. Саенко И.Б., Бирюков М.А., Ясинский С.А., Грязев А.Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. 2018. №1. С. 81–85.
2. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17-19 February, 2010. Los Alamitos, California. IEEE Computer Society. 2010. Pp. 617–623.
3. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. №1. С. 121–126.
4. Patel S.Ch., Umrao L.S., Singh R.Sh. Policy-based Access Control in Cloud Computing // Proceedings of the International conference on Artificial Intelligent and Soft Computing, December 2012. 6 pages.
5. Servos D., Osborn S.L. Current Research and Open Problems in Attribute-Based Access Control // ACM Comput. Surv. 2017. Vol. 49. No. 4. Article 65, 45 pages.
6. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Анализ методов атрибутного разграничения доступа // ПДМ. 2019. №44. URL: https://cyberleninka.ru/article/n/analiz-metodov-atributnogo-razgranicheniya-dostupa (дата обращения: 20.07.2020).

УДК 004.056

ОБЗОР ПОДХОДОВ К КЛАССИФИКАЦИИ УГРОЗ БЕЗОПАСНОСТИ УМНОГО ГОРОДА

Виткова Лидия Андреевна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: vitkova@comsec.spb.ru

Аннотация. Концепция Умного города – это ключевой момент дальнейшего развитии нашего ближайшего будущего. Одной из важнейших составляющих таких городов является транспортная инфраструктура. Реализация угроз для такой инфраструктуры может иметь критические последствия для города. Чтобы предотвратить такие угрозы в будущем, мы должны исследовать их и противодействовать им в настоящем.

Ключевые слова: угрозы информационной безопасности, Умный город, транспортная инфраструктура.

SURVEY OF APPROACHES TO THE CLASSIFICATION OF SECURITY THREATS SMART CITY

Vitkova Lidia
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: vitkova@comsec.spb.ru

Abstract. The concept of a Smart City is the forefront in the development of our near future. One of the most important part of such cities is the transport infrastructure. Threats implementation for such infrastructure can have critical consequences for a city. To prevent such threats in the future we should investigate and counteraction them in the present.

Keywords: threats, smart city, transport infrastructure.

Введение. Информационные технологии стали неотъемлемой часть современного мира. В результате возникла необходимость обработки большого объема потоков гетерогенных данных, которые имеют множество внутренних скрытых связей. Для решения этого применяются технологии, в основе которых лежат алгоритмы искусственного интеллекта [1]. Например, в местах проживания людей появились концепции Умного Города (УГ). Одной из основополагающих частей «умного города» можно считать транспортную инфраструктуру (ТИ). Транспортная инфраструктура умного города является исследуемой областью данной работы. Она необходима для функционирования современного общества, а также имеет важное экономическое значения для бизнеса и стратегическое для государства. Тем не менее, любой прогресс имеет и множество негативных сторон. Растёт количество новых угроз информационной безопасности [2, 3]. Последние могут иметь критические последствия именно для ТИ УГ. В том числе, могут приводить к нарушению работы смежных инфраструктур (например, служб доставки еды и корреспонденции), а также становится причиной человеческих жертв (например, ДТП). Таким образом, существование угроз в ТИ УМ является актуальной проблемой информационной безопасности (ИБ). Необходимость решения такой проблемы по прогнозам будет только расти [4].

Анализ. Несмотря на возможные подходы к разрешению данной проблемы, в любом случае они будут строиться на некоторой научной и практической базе. Интеллектуализацию жизнедеятельности можно считать достаточно новой сферой. И полноценная база угроз информационной безопасности еще не сформирована. Данная работа является базовой работой для последующих исследований и экспериментов. В рамках исследования авторы ставили перед собой цель провести анализ подходов к классификации угроз безопасности. В том числе таких, которые посвящены проблемам информационной безопасности Интернета Вещей, умного города, транспортной инфраструктуре. В частности, рассмотреть возможные подходы к классификации угроз при помощи машинного обучения.

Существует множество работ, связанных с исследованием вопросов безопасности Интернета вещей (IoT) как концепции в общем. Например, [5] посвящена подробному разбору проблем безопасности Интернета Вещей, противодействию им, а также обсуждению будущих направлений развития безопасности в этой сфере. Также в своей другой работе [6] авторы не только исследуют опросы безопасности IoT, но и также и рассматривают подходы к обнаружению и оценке угроз информационной безопасности.

В последние годы все чаще публикуются обзоры, посвященные дискуссии вокруг актуальности информационной безопасности Интернета Вещей. Делаются хорошие попытки систематизации накопленных ранее специалистами знаний и прогнозирование будущих проблем [7,8]. Также делаются выводы с рекомендациями по настройкам безопасности [9, 10].

В отдельную область выделяются вопросы безопасности Интернета транспортной инфраструктуры IoV. Можно перечислить следующие проблемы: обеспечение информационной безопасности и транспортного Интернета вещей (IoV) [11, 12, 13], обеспечение безопасности автомобильного движения [14, 15], управление транспортными потоками [16], предотвращение аварий и преступлений [17, 18, 19], автоматизированное оповещение служб экстренной помощи [20, 21] и др.

Однако все множество работ, посвященных информационной безопасности транспортной инфраструктуры умного города посвящено обсуждению атак, уязвимостей, не содержит примеров и методов классификации угроз на более абстрактном уровне.

Для абстрактного представления угроз безопасности сегодня часто используются онтологии. Так например, работа [22] посвящена разработке онтологии. Разработанная онтология основана на определении понятий и отношений между первичными признаками исходных данных безопасности и формировании набора иерархически взаимосвязанных показателей безопасности. А в [23] авторы пишут, что разрабатываемая модель информационной безопасности должна быть адаптивной. Так как Интернет вещей (IoT) характеризуется высокой вариативностью.

В работе [24] исследуются методы, основанные на ML и DL. Авторы пишут о том, что такие методы имеют возможность извлекать уроки из структуры трафика с использованием обучающих и тестовых наборов данных в обширных сетевых доменах для принятия интеллектуальных решений относительно идентификации атак и смягчения их последствий. Они также в своей работе предложили архитектуру DL и ML-based Secure Data Analytics (SDA) для классификации обычных или атакующих входных данных.

Заключение. Как показывает обзор релевантных работ в части классификации угроз безопасности, большинство исследователей сосредоточены на выбранной ими области. Таким образом, ни одна из существующих работ не претендует на высокий уровень формализации самого подхода к классификации угроз. Представляется перспективным задача разработки универсального подхода к систематизации угроз, с возможностью прогнозирования ранее не выявленных в системе.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 19-29-06099 мк)

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. Комплексный подход к обеспечению безопасности киберфизических систем на системе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С.29-38. DOI: 10.21681/2311-3456-2018-3-29-38.
2. Котенко И.В., Дойникова Е.В., Чечулин А.А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд, № 4, 2012. С.54-66.
3. M. Buinevich, K. Izrailov, E. Stolyarova and A. Vladyko, "Combine method of forecasting VANET cybersecurity for application of high priority way," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 266-271, doi: 10.23919/ICACT.2018.8323720.

4. IoT and OT Security Research Exposes Hidden Business Challenges, Forrester Consulting report commissioned by Forescout Technologies, Inc. 2017. [электронный ресурс]/ URL: https://www.forescout.com/iot_forrester_study/
5. Ahmed A. W., Ahmed M. M., Khan O. A., Shah M. A., "A comprehensive analysis on the security threats and their countermeasures of IoT", International Journal Of Advanced Computer Science and Applications, vol. 8, no. 7, pp. 489-501, 2017.
6. Ahmed H., Nasr A., Abdel-Mageid S., Aslan H. (2019). "A survey of IoT security threats and defenses". International Journal of Advanced Computer Research. 9. 325-350. 10.19101/IJACR.2019.940088.
7. Ataç C, Akleylek S . (2019). A Survey on Security Threats and Solutions in the Age of IoT
8. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. (2017). "Internet of Things security: A survey". Journal of Network and Computer Applications, 88, 10–28. doi:10.1016/j.jnca.2017.04.002
9. Abdul-Ghani H., Konstantas D., Mahyoub M. (2018). "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model"
10. Azam F., Munir R., Ahmed M., Ayub M., Sajid A., Zaheer A. (2019). "Internet Of Things (Iot), Security Issues And Its Solutions"
11. Sharma, Surbhi, and Baijnath Kaushik. "A survey on internet of vehicles: Applications, security issues & solutions." Vehicular Communications 20 (2019): 100182.
12. Arif, Muhammad, et al. "A survey on security attacks in VANETs: Communication, applications and challenges." Vehicular Communications (2019): 100179
13. Sheikh, Muhammad Sameer, Jun Liang, and Wensong Wang. "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)." Sensors 19.16 (2019): 3589.
14. Subramaniyam, CN Siva, et al. "A Survey on IoT Based Intelligent Road Traffic and Transport Management Systems." Int. J. Innov. Res. Comput. Commun. Eng. 5.12 (2017): 1302-1309.
15. Seliverstov, Ya A., et al. "Intelligent systems preventing road traffic accidents in megalopolises in order to evaluate." 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). IEEE, 2017.
16. Subramaniyam, C. S., Sivaraman, K., Ramachandran, S. S., & Veeraraghavan, A. K. (2017). A Survey on IoT Based Intelligent Road Traffic and Transport Management Systems. Int. J. Innov. Res. Comput. Commun. Eng., 5(12), 1302-1309.
17. Sheikh, Muhammad Sameer, and Jun Liang. "A Comprehensive Survey on VANET Security Services in Traffic Management System." Wireless Communications and Mobile Computing 2019 (2019).
18. Vivo-Delgado, Gerard, and Francisco J. Castro-Toledo. "Urban security and crime prevention in smart cities: a systematic review." (2020).
19. Yannick Chevalier, Roland Rieke, Florian Fenzl, Andrey Chechulin, Igor Kotenko. ECU-Secure: Characteristic Functions for In-Vehicle Intrusion Detection. Proceedings of the 13th International Symposium on Intelligent Distributed Computing (IDC 2019), Saint-Petersburg, Russia, 7-9 October 2019. Springer-Verlag, Studies in Computational Intelligence, Vol.868, 2020. P.495-504. DOI: 10.1007/978-3-030-32258-8_58.
20. Valle Quiroz, Felipe Eduardo. "An intelligent decision system for interworking of 802.11 P and LTE in heterogeneus vehicular networks." (2019).
21. Vasily Desnitsky, Nikolay Rudavin, Igor Kotenko. Modeling and Evaluation of Battery Depletion Attacks on Unmanned Aerial Vehicles in Crisis Management Systems // Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence, vol 868. Springer, Cham, p. 323-332, 2020.
22. Doynikova, Elena, Andrey Fedorchenko, and Igor Kotenko. "Ontology of metrics for cyber security assessment." Proceedings of the 14th International Conference on Availability, Reliability and Security. 2019.
23. Bruno Mozzaquatro, Raquel Melo, Carlos Agostinho and Ricardo JardimGoncalves. 2016. An ontology-based security framework for decision-making in industrial systems. In Proceedings of the 4th International Conference on Model-Driven Engineering and Software Development, 779-788.
24. Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Machine learning models for secure data analytics: a taxonomy and threat model. Computer Communications.

УДК 004.056

О МОДЕЛИРОВАНИИ ПРОЦЕССОВ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ АКТИВНОСТИ В ИНТЕРНЕТЕ И СОЦИАЛЬНЫХ СЕТЯХ

Виткова Лидия Андреевна, Дойникова Елена Владимировна, Проничев Алексей Петрович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: vitkova@comsec.spb.ru

Аннотация. В эпоху глобальной цифровизации общества ежедневно создается огромное количество отдельных информационных объектов и веб-страниц. Остро для государства и общества стоит вопрос о разработки моделей информационного обмена (распространения), выявления, противодействия распространению информации в сети Интернет. Авторы исследуют правовые и системные предпосылки для моделирования процессов выявления и противодействия.

Ключевые слова: информационная безопасность в сети Интернет, противодействие распространению информации, мониторинг и выявление террористической и экстремистской активности.

ABOUT MODELING THE PROCESSES OF DETECTING AND COUNTERING TERRORIST AND EXTREMIST ACTIVITY ON THE INTERNET AND SOCIAL NETWORKS

Vitkova Lidia, Doynikova Elena, Pronichev Aleksei
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: vitkova@comsec.spb.ru

Abstract. In the era of global digitalization of society, a huge number of individual information objects and web pages are created every day. The issue of developing models for information exchange (dissemination), identifying and countering the spread of information on the Internet is acute for the state and society. The authors investigate the legal and system prerequisites for modeling the processes of detection and counteraction.

Keywords: information security on the Internet, countering the spread of information, monitoring and detecting terrorist and extremist activity.

В Стратегии противодействия экстремизму в РФ до 2025 года [1] введены такие основные понятия как:

1. идеология насилия - совокупность взглядов и идей, оправдывающих применение насилия для достижения политических, идеологических, религиозных и иных целей;
2. экстремистская идеология - совокупность взглядов и идей, представляющих насильственные и иные противоправные действия как основное средство разрешения политических, расовых, национальных, религиозных и социальных конфликтов;
3. субъекты противодействия экстремизму - федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления;

Таким образом, процесс выявления и противодействия террористической и экстремистской активности в Интернете и социальных сетях может быть инициирован и реализован только на уровне субъектов противодействия. И система мониторинга и противодействия может быть внедрена только на уровне субъектов.

При этом в Стратегии сказано, что социальные сети, мессенджеры и сеть «Интернет» в целом , стали основным средством связи для экстремистских организаций, которое используется ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии. Проблема распространения экстремистской идеологии угрожает государственной и общественной безопасности. Одним из основных способов дестабилизации общественно-политической и социально-экономической обстановки является привлечение различных групп населения к участию в протестных акциях, которые умышленно трансформируются в массовые беспорядки.

Огромное количество отдельных информационных объектов, веб-страниц, страниц на базе доменов социальных сетей, создается ежедневно. И вопрос разработки моделей информационного обмена (распространения), выявления, противодействия распространению такой информации в сети Интернет и в социальной сети представляется актуальным [2, 3].

Работа выполнена при финансовой поддержке гранта рнф (проект № рнф 18-11-00302) в спиран.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» Режим электронного доступа: URL: https://www.garant.ru/products/ipo/prime/doc/74094369/ (Дата обращения 30.06.2020)
2. Виткова Л.А., Чечулин А.А., Науменко К.А. Мониторинг повестки дня в медиасистемах при одновременном применении алгоритмов изменения задания// В книге: Перспективные направления развития отечественных информационных технологий материалы V межрегиональной научно-практической конференции. Севастопольский государственный университет; Санкт-Петербургский институт информатики и автоматизации РАН. Севастополь, 2019. С. 323-325.
3. Виткова Л.А., Дойникова Е.В., Котенко И.В. Модель мер противодействия нежелательной, сомнительной и вредоносной информации в сети интернет// В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) сборник научных статей VIII Международной научно-технической и научно-методической конференции : в 4 т.. 2019. С. 223-227.

УДК 004.056

ВЫБОР КРИТЕРИЕВ КЛАССИФИКАЦИИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ДЛЯ ВЫЯВЛЕНИЯ ВЕКТОРОВ АТАК

Гайфулина Диана Альбертовна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: gaifilina@comsec.spb.ru

Аннотация. В данном исследовании рассматриваются критерии классификации киберфизических систем. Предлагается использовать оценки сложности, связности и критичности, а также социальный аспект для определения компонентного состава системы и ее характеристик. Полученное описание позволит понять, какие вектора атак характерны для целевой киберфизической системы, и в дальнейшем учитывать их при разработке, администрировании и использовании данных систем.

Ключевые слова: информационная безопасность, киберфизическая система, классификация киберфизических систем, вектора атак.

SELECTION OF CLASSIFICATION CRITERIA FOR CYBER-PHYSICAL SYSTEMS TO IDENTIFY ATTACK VECTORS

Gaifulina Diana
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: gaifilina@comsec.spb.ru

Abstract. This study examines the classification criteria for cyber-physical systems. It is suggested to use assessments of complexity, connectivity and criticality as well as the social aspect to determine the component composition of the system and its characteristics. The resulting description will help to understand which attack vectors are typical for the target cyber-physical system, and then take them into account when developing, administering, and using of these system.

Keywords: information security, cyber-physical system, classification of cyber-physical systems, attack vectors.

В современном мире непрерывно растет распространенность и востребованность киберфизических систем (КФС), которые нашли свое применение в различных формах – от промышленных установок до «умных» устройств личного использования. Впервые термин «киберфизическая система» (Cyber-Physical System, CPS) был предложен для обозначения комплексов, состоящих из природных объектов, искусственных подсистем и контроллеров. В настоящее время к киберфизическим системам также относят системы управления производством (АСУ ТП, SCADA-системы), Интернет вещей (Internet of Things, IoT), робото-технические системы, беспилотные летательные аппараты и автомобили. Киберфизическая система, таким образом, является результатом объединения встроенных программно-аппаратных систем, с одной стороны связанных с физической средой с помощью датчиков, а с другой стороны, с глобальными сетями.

Обеспечение безопасности подобных систем представляет собой важную задачу и развивается по различным направлениям, важное место среди которых занимает выявление векторов атак. Вектора атак могут базироваться как на эксплуатации уязвимостей системы, так и на социальной инженерии, при этом различные вектора не являются взаимоисключающими. Выбор злоумышленником конкретной последовательности атакующих действий зависит от его квалификации, а также от целей и возможностей, определяемых особенностями целевой системы.

Следовательно, анализ компонентного состава КФС позволит охарактеризовать инфраструктуру системы и обрабатываемые ею данные, помогая определить, что является целью злоумышленника, и какие возможности он использует при атаке на данную систему. Подобный анализ, в свою очередь, предполагает выбор определенных критериев, по которым производится классификация киберфизических систем, так как на данный момент сложно обозначить стандартизированный набор аспектов. На основании анализа научной литературы данной тематики предлагается использовать следующие критерии классификации:

- сложность в соответствии с функциональными возможностями и используемыми компонентами,
- связность в соответствии с используемыми интерфейсами и протоколами передачи данных,
- критичность системы или ее элементов в соответствии с зависящими от них бизнес-процессами,
- социальный аспект в соответствии с характером взаимодействия системы с социумом.

Для оценки сложности составляющие системы принято разделять на различные уровни, в зависимости от функциональности элементов каждого слоя, например на физический, сетевой и уровень сервисов [1]. Задачей физического уровня является надежное считывание информации с датчиков и сенсоров. Сетевой уровень обеспечивает повсеместный доступ и передачу данных. На уровне сервисов выполняются функции по сбору и хранению данных, по обеспечению эффективности энергообеспечения и логистики. В некоторых работах рассматривается структура киберфизической системы, состоящая из пяти уровней, например, 5C-архитектура [2], согласно которой выделяют уровни соединения, преобразования данных в информацию, кибернетики, познания и конфигурации. Также распространенной архитектурой киберфизической системы является структура из семи уровней модели ISO/OSI: от физического до прикладного уровня. Таким образом, элементы киберфизической системы могут быть классифицированы по своей функциональности, т.е. от места, занимаемого в общей архитектуре системы. Оценку сложности можно проводить также, используя следующие критерии инфраструктуры киберфизических систем: структура (одноуровневые, иерархические системы) и количество контуров управления, количественный (фиксированный или переменный) и качественный (однородные и гетерогенные системы) состав элементов и динамика поведения (адаптивные, самоорганизующиеся и т.д.) [3].

В исследовании предлагаются следующие критерии, позволяющие оценить связность киберфизической системы: инструментарий (характеризует технологии взаимодействия с окружающим миром, например сенсоры и RFID-метки) и стандарты связи (технологии взаимодействия элементов КФС между собой) [4]. Наиболее актуальными стандартами беспроводной связи являются NFC, RFID, ZigBee, Z-Wave, Bluetooth, Wi-Fi, 3GPP, NB-IOT, LoRa. К наиболее распространенным проводным сетевым интерфейсам передачи данных между микроконтроллерами киберфизических систем относят UART, SPI, I2C, 1-Wire и CAN. Интерфейсами, обеспечивающими взаимодействие компьютера и внешних устройств, являются Ethernet, USB, FireWire, SATA, eSATA, SAS, HDMI и Thunderbolt. Также для оценки связности используются критерии топологии сети (например, древовидная, ячеистая или сотовая), географическая распределенность киберфизической системы (централизованные и распределенные системы) и ее открытость (использование локальных или глобальных сетей). В сложных гетерогенных системах каналы связи должны отвечать строгим требованиям по пропускной способности, задержке и дальности, при этом придерживаясь ограниченного энергетического бюджета и обеспечивая высокий уровень безопасности.

Для оценки уровня критичности системы часто исследуются модели бизнес-процессов, которые применяются при анализе потенциальных угроз и уязвимостей. Критическая информационная инфраструктура представляет собой совокупность автоматизированных систем управления производственными и технологическими процессами критически важных объектов, а также обеспечивающие их взаимодействие информационно-телекоммуникационные сети [5]. К данным объектам могут быть отнесены и киберфизические системы следующих сфер применения: здравоохранение, наука, транспорт, связь, энергетика, финансовый рынок, оборонная и ракетно-космическая промышленность и т.п. Критичность в данном случае заключается в том, что полный или частичный отказ подобных систем может привести к экономическому, финансовому или иному ущербу, в том числе жизни и здоровья человека. Ранжирование элементов КФС по степени критичности в каждом конкретном случае зависит от типов систем, выбранных частных показателей критичности, экспертной информации и т.п.

Эффективность функционирования киберфизической системы также зависит от социального аспекта – взаимодействия персонала и потребителя с системой, поэтому интересы различных групп социума должны учитываться от этапа разработки системы до процесса ее обслуживания. Критерий социализации элементов киберфизической системы может включать следующие типы взаимодействия: проектирование, производство, купля/продажа, хранение, выполнение работы, техническое обслуживание и утилизация [6]. Характер взаимодействия киберфизической системы с людьми описывает человеческий фактор: принимает ли система решения без вмешательства человека (автономная система), направляет человека по время выполнения своей задачи (автоматизированная система), полностью управляется человеком (инструмент) или только предоставляет необходимые данные (руководящая система). Критерий наличия модели восприятия внешнего мира описывает как объекты КФС воспринимают окружающий мир: отсутствие модели, фиксированная модель или генерирующаяся модель [3].

Приведенные критерии классификации киберфизических систем позволяют оценить сложность, связность и критичность системы, а также выделить ее социальный аспект, тем самым определив компонентный состав и характеристики целевой системы. Полученное описание позволит понять, какие опасности характерны для целевой КФС, и в дальнейшем учитывать их при разработке, администрировании и использовании системы. Таким образом, имея информацию о компонентном составе киберфизической системы, можно будет выявить перечень возможных векторов атак, которым данная система может быть подвержена, и, следовательно, сформировать список средств и методов защиты, необходимых для обеспечения ее безопасности.

Работа выполнена при частичной поддержке РФФИ (проект № 19-17-50205).

СПИСОК ЛИТЕРАТУРЫ

1. Xiao-Le W., Hong-Bin H., Su D., Li-Na C. A service-oriented architecture framework for cyber-physical systems // Recent Advances in Computer Science and Information Engineering. Springer, Berlin, Heidelberg, 2012. pp. 671-676.
2. Lee J., Bagheri B., Kao H. A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems // Manufacturing letters. 2015. vol. 3. pp. 18-23.
3. Zegzhda D. P., Poltavtseva M. A., Lavrova D. S. Systematization and security assessment of cyber-physical systems // Automatic control and computer sciences. 2017. vol. 51. №. 8. pp. 835-843.
4. Cardin O. Classification of cyber-physical production systems applications: Proposition of an analysis framework // Computers in Industry. 2019. vol. 104. pp. 11-21.
5. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) // АО «Консультант Плюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 13.04.2020).
6. Микони С. В. Модель участников жизненного цикла социо-киберфизической системы // Технологическая перспектива в рамках евразийского пространства: новые рынки и точки экономического роста, 2019. С. 341-347.

УДК 004.056

МЕСТО И РОЛЬ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

Гайфулина Диана Альбертовна, Котенко Игорь Витальевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: gaifilina@comsec.spb.ru

Аннотация. В данном исследовании проводится обзор основных подходов к корреляции событий безопасности для анализа защищенности облачных систем. Определяется значимость методов глубокого обучения для работы с большим объемом данных событий безопасности.

Ключевые слова: информационная безопасность, облачные системы, анализ защищенности, корреляция событий безопасности, глубокое обучение, нейронные сети.

PLACE AND ROLE OF CORRELATION OF SECURITY EVENTS IN CLOUD SYSTEMS BASED ON DEEP LEARNING METHODS

Gaifulina Diana, Kotenko Igor
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: gaifilina@comsec.spb.ru

Abstract. This research provides an overview of the main approaches to the correlation of security events for cloud systems security analysis. The significance of deep learning methods for working with a large amount of data about security events is determined.

Keywords: information security, cloud systems, security analysis, correlation of security events, deep learning, neural networks.

К современным информационным системам предъявляются требования к обработке и хранению огромного количества информации, поэтому все большую популярность благодаря своей гибкости и масштабируемости приобретают облачные системы. Облачные технологии представляют собой распределенные

вычислительные платформы, оборудование и программное обеспечение которых поставляются в виде услуги через сеть Интернет. Облачные вычисления могут результативно применяться для аналитики данных, поскольку архитектура облаков обеспечивает поддержку масштабируемости, виртуализации и хранения огромных объемов структурированных и неструктурированных данных. В то же время с развитием технологий совершенствуются и способы реализации атак на них. Для реагирования на угрозы безопасности необходимы модернизированные методы и средства, позволяющие анализировать большое число событий в реальном времени или близком к нему режиме. Управление инцидентами и событиями безопасности должно нести упреждающий характер, при котором принятие решений осуществляется еще до возникновения критической ситуации.

Наиболее распространенными решениями для аналитики событий безопасности являются SIEM-системы (Security information and event management), обрабатывающие данные из гетерогенных источников, таких как сетевое оборудование, сканеры уязвимостей и журналы событий. Выделяют следующие уровни построения SIEM-системы: сбор, управление и анализ данных [1]. Результатом последнего являются отчеты и предупреждения о состоянии безопасности объекта защиты. Для решения поставленных задач используются различные методы анализа событий, важное место среди которых занимает корреляция, позволяющая выявлять взаимосвязи между разнородными событиями и инцидентами. Использование методов корреляции событий безопасности также позволяет снизить объем исходного потока данных за счет их группирования. Определение взаимосвязи между событиями из разных источников способствует лучшему пониманию развития атаки.

Существуют как сигнатурные, так и бессигнатурные методы корреляции. Применение первых заключается в формирование правил определения инцидентов, а вторых – в использовании моделей обучения. Среди наиболее применяемых на практике подходов к корреляции событий безопасности можно назвать следующие [2-4]:

- статистический метод, заключающийся в измерении степени статистической связи между событиями;
- рассуждения на основе правил (rule-based reasoning, RBR), при которых взаимосвязи определяются спецификациями аналитиков;
- рассуждения на основе прецедентов (case-based reasoning, CBR), при которых корреляция производится по векторам предварительно заданной матрицы событий;
- рассуждения на основе модели (model-based reasoning, MBR);
- корреляция на основе графов (graph based), заключающаяся в поиске зависимостей между событиями в графическом представлении и определении причины возникновения инцидента;
- машинное обучение, в частности нейронные сети, применяемые для обнаружения аномалий в потоке событий.

Стоит отметить, что выяснение причин инцидентов является весьма трудоемкой задачей, требующей анализа большого количества данных и обширной базы знаний. По этой причине использование нейронных сетей является наиболее эффективным. В тоже время глубокое обучение, как подвид машинного обучения, становится все более распространенным методом интеллектуального анализа данных. Такие крупные компании как Microsoft и Google активно внедряют методы глубокого обучения в свои разработки. Алгоритмы на основе глубокого обучения позволяют осуществлять автоматический отбор информативных признаков и работать напрямую с необработанными данными, извлекая из них общие представления на разных уровнях детализации.

Архитектура глубокого обучения поддерживает множество слоев нейронной сети, а процесс обучения нейронной сети состоит в подборе оптимальных параметров для нейронов. Обучение с учителем предполагает, что веса сети изменяются до тех пор, пока для входного вектора значений не будет получено приемлемое значение корреляции с выходным вектором. Популярными методами обучения с учителем являются сверточные нейронные сети (Convolutional Neural Network, CNN) и нейронные сети прямого распространения (Feed Forward Neural Network, FFNN). Обучение без учителя заключается в настройке весов нейронной сети таким образом, чтобы предъявление достаточно близких входных векторов давало одинаковые выходные значения. Распространенными методами глубокого обучения без учителя являются глубокие сети доверия (Deep Belief Networks, DBN), такие как автокодировщики (autoencoder, AEnc) и ограниченная машина Больцмана (Restricted Boltzmann Machine, RBM), и рекуррентные нейронные сети (Recurrent Neural Network, RNN). Существует также класс гибридных методов, включающих генеративно-состязательные сети (Generative Adversarial Networks, GAN) и рекурсивные нейронные сети (Recursive neural network, ReNN) [5].

Примером использования глубокого обучения для анализа событий безопасности является работа [6], в которой представлен подход к обнаружению внутренних нарушителей путем анализа журнала системных событий. Для выявления шаблонов нормального поведения использовалась рекуррентная нейронная сеть на основе блока долгой краткосрочной памяти (Long Short-Term Memory, LSTM). Данная сеть позволяет продемонстрировать динамическое поведение, так как связи между ее нейронами образуют направленный цикл. Анализируя последовательность измерений различных параметров текущего процесса, сеть обучается предсказывать его состояние в следующий момент времени. При построении каждого нового скрытого слоя используются значения всех признаков, что позволяет фиксировать временные шаблоны в поведении пользователей и строить более точную модель поведения пользователя с течением времени. Для поиска аномалий применяется регрессионная модель, предсказывающая поведение в определенный момент времени на основе вероятностных распределений, соответствующих предшествующим наблюдениям. Подход протестирован на наборе данных CERT v6.2 [7], описывающем активность 4000 сотрудников организации на протяжении 516 дней,

и полнота обнаружения аномалий составила около 99%. В исследовании [8] рекуррентная нейронная сеть используется для классификации атрибутов пользователя. Для расчета отклонений в поведении на основе результатов нескольких классификаторов введен калькулятор аномалий. Результаты эксперимента показывают точность классификации, достигающую 96,97%. Частое применение рекуррентных нейронных сетей объясняется тем, что многие данные, связанные с кибербезопасностью, могут быть представлены в виде временных рядов. К ним относятся сетевой трафик, журналы событий, последовательности системных вызовов и т.п. Рекуррентные нейронные сети хорошо зарекомендовали себя в обработке последовательных данных, по которым предсказывают состояние процесса в следующий момент времени.

Для эффективного использования глубокого обучения требуется огромное количество данных, которому, в свою очередь, необходим большой объем памяти. Также возрастают требования к мощности вычислительных ресурсов, в том числе электропитанию, что влечет за собой рост капитальных вложений. Исходя из данных фактов, наиболее простым и эффективным способом внедрения методов глубокого обучения является использование облачных вычислений для обработки данных. Сочетание передового аналитического программного обеспечения и доступной вычислительной мощности делает облако идеальным местом для выполнения аналитики с использованием глубокого обучения. Таким образом, при работе с большим числом данных, в особенности необработанных, корреляция событий безопасности на основе методов глубокого обучения является эффективным решением для анализа защищенности облачных систем.

Работа выполнена при частичной поддержке бюджетной темы № 0060-2019-0010.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. Вып.1 (20). СПб.: Наука, 2012. С.27-56
2. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В., Анализ методов корреляции событий безопасности в SIEM-системах.Часть 1 // Труды СПИИРАН. 2016. Вып. 4 (47). С. 5-27.
3. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В., Анализ методов корреляции событий безопасности в SIEM-системах.Часть 2 // Труды СПИИРАН. 2016. Вып. 6(49). С. 208-225.
4. Новикова Е. С. Бекенева, Я. А., Шоров, А. В., & Федотов, Е. С.. Обзор алгоритмов корреляции событий безопасности для обеспечения безопасности облачных вычислительных сред // Информационно-управляющие системы, 2017. №. 5 (90). С.95-104.
5. Berman D.S., Buczak A.L., Chavis J.S., Corbett C.L. A survey of deep learning methods for cyber security // Information, 2019. Vol. 10. No. 4. P. 122.
6. Tuor A., Kaplan S., Hutchinson B., Nichols N., Robinson S. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams // Workshops at the Thirty-First AAAI Conference on Artificial Intelligence, 2017. P. 224-231.
7. Insider Threat Test Dataset. [Электронный ресурс]. URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508099 (дата обращения 29.04.2020).
8. Meng F., Lou F., Fu Y., Tian Z. Deep Learning Based Attribute Classification Insider Threat Detection for Data Security // 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, 2018. P. 576-581.

УДК 004.584

ОЦЕНКА УРОВНЯ ПОДГОТОВКИ СОТРУДНИКОВ ПРЕДПРИЯТИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гвоздков Игорь Вячеславович, Тюлейкина Анна Евгеньевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: gvozdkov@rambler.ru, atyuleykina@yandex.ru

Аннотация. В данной статье рассматривается статистика угроз информационной безопасности со стороны персонала, задача определения оценки уровня подготовки в области информационной безопасности сотрудников предприятия, улучшение качества подготовки сотрудников в данной области.

Ключевые слова: информационная безопасность, оценка, подготовка, методы защиты, международный стандарт.

EVALUATION OF THE LEVEL OF PREPARATION OF EMPLOYEES OF THE ENTERPRISE IN THE FIELD OF INFORMATION SECURITY

Gvozdkov Igor, Tyuleikina Anna
Bonch-Bruevich Saint-Petersburg state university of communication
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: gvozdkov@rambler.ru, atyuleykina@yandex.ru

Abstract. This article discusses statistics of threats to information security by personnel, the task of determining the assessment of the level of training in the field of information security of employees, improving the quality of training of employees in this area.

Keywords: information security, assessment, training, protection methods, international standard.

Введение. В результате широкого применения информационных систем с каждым годом возрастает количество атак на предприятия, которые наносят финансовые и материальные убытки. Атаки прежде всего могут происходить по причине незнаний элементарных правил сотрудников в области безопасности

информации. Тем самым формируются различные курсы по переподготовке, проводятся совещания для сотрудников. Но, как известно, это занимает длительное время. Следует отметить, что не все предприятия уделяют должного внимания на обеспечение безопасности информационных ресурсов, с которыми взаимодействуют сотрудники. Таким образом, необходимо проводить обучение в сфере информационной безопасности сотрудников.

Ключевые угрозы для информации в результате совершения противоправных действий сотрудников [1]:

- утечка конфиденциальной информации и коммерческой тайны;
- подмена или уничтожение данных необходимых для реализации бизнес-процессов предприятия;
- нарушение прав на объекты интеллектуальной собственности.

В результате этого может произойти прерывание бизнес-процессов и прямые и непрямые финансовые потери.

Чтобы противостоять угрозе, необходимо досконально ее изучить и принять определенные меры защиты для ее устранения. Именно поэтому проведено исследование угроз информационной безопасности. Среди более 5000 тысяч людей, прошедших опрос, присутствуют специалисты по безопасности, системные администраторы и руководители [2].

В результате проведенного опроса выяснилось, что более 92,6% предприятий сталкивалась с утечкой информации. В 55,2% случаев причиной утечек конфиденциальной информации являются целенаправленные действия сотрудников. Работники крадут данные по разным причинам: продажа конкурентам, для формирования портфолио или для развития собственного бизнеса. Из-за неосторожного поведения персонала, к примеру, отправки сообщений или важных документов не по нужному адресу, случайному предоставлению логинов и паролей третьим лицам и тому подобного происходит около 23,6% утечек конфиденциальной информации. И в 21% случаев информация оказывается за периметром предприятия из-за действий злоумышленников или вирусов.

Из-за злоумышленных действий инсайдеров предприятие теряет ценную информацию, составляющую коммерческую тайну, и новые разработки в 61,5% случаях.

В 37% случаев составляют сотрудники, желающие продать конфиденциальную информацию конкурентам. Самые хитрые сотрудники развивают собственный бизнес, используя ресурсы предприятия, таких случаев - 26%.

По мнению 59% опрошенных самой ведущей угрозой информации является внутренняя угроза, так как сотрудники предприятия могут легко получить доступ к информации, имеющую ценность, и легко воспользоваться ей в своих корыстных целях. 33% опрошенных предполагают, что наиболее опасны для сохранности данных неосторожные действия персонала, совершаемые без коварного умысла. И только 8% опасаются действий хакеров.

Три важные причины, по которым сотрудник предприятия может совершить хищение ценной информации:

- отсутствие системы контроля персонала и перемещения информации, что составляет 41,6%;
- отсутствие персональной ответственности на рабочем месте – 34,7%;
- большой круг лиц, имеющий доступ к конфиденциальной информации, что составляет 23,7%.

В 46% случаев инциденты с кражей информации ведут к полной потере данных. Причинами таких действий сотрудников:

- целенаправленное нанесения вреда – 36,3%;
- неосознанные действия персонала – 31,9%;
- действия третьих лиц – 31,3%.

Не удивительно, что при таких обстоятельствах доверяют персоналу 10,7% опрошенных.

Также в результате опроса с планомерной защитой информации сотрудники делают резервные копии информации несколько раз в месяц – 66,7%; 14,8% – один раз в месяц; 7,4% – раз в квартал, и 11,1% – раз в год или реже.

Большинство опрошенных достаточно серьезно относятся к обновлению логина и пароля для доступа к ценным данным, из них 10,7% – меняют логин и пароль чаще раза в месяц; 28,6% – один раз в месяц; 25% – раз в квартал; 14,3% – раз в полугодие; и 7,1% – пренебрегают этим на регулярной основе.

Для того, чтобы повысить показания, составляющие защиту и сохранность информации, необходимо оценивать уровень подготовки в области информационной безопасности сотрудников предприятия. Далее при определенных показаниях необходимо сделать вывод о дальнейших действиях, связанных с улучшение информационной безопасности предприятия.

Принцип решения задачи заключается в проверке знаний в области безопасности информации сотрудников предприятия при приеме на определенную должность. Так на основании полученной информации, сформированной по результатам прохождения тестирования, руководством предприятия самостоятельно могут быть приняты дополнительные меры по оценке или совершенствованию существующей системы информационной безопасности: совершенствование политики безопасности, формирование определенных инструкций и правил для персонала внутри организации, либо для самостоятельной подготовки персонала, поскольку проверочные тестирования должны быть основаны на существующих федеральных законах об информации и на международном стандарте в области информационной безопасности: ISO/IEC 27001 [3].

Тестирования должны отвечать требованиям, предъявляемым:

1. К формулировке тестовых заданий в закрытой форме с выбором одного правильного ответа.
2. Федеральным законом и Международным стандартам на предмет:

– соответствия изложенного в них материала;

– правдоподобности и правильности формулировки вопросов к проверяемым стандартами требований, правил и норм;

– полноты оценки состояния текущего уровня информационной безопасности на предприятии, проверяемых параметров и степени их соответствия международным стандартам.

На основании полученной информации, которая выдается по результатам пройденного тестирования, руководителем предприятия могут быть приняты дополнительные меры по совершенствованию существующей системы информационной безопасности.

Составленные рекомендации должны соответствовать международному стандарту ISO/IEC 27001, Федеральному закона «Об информации, информационных технологиях и защиты информации» или другим, к примеру, российским стандартам, таким образом могут использоваться руководством предприятия для совершенствования политики безопасности и формирования определенных инструкций и правил для персонала внутри предприятия.

Заключение. Система проверки уровня подготовки сотрудников предприятия в области информационной безопасности должно происходить на регулярной основе в зависимости от масштаба персонала, предприятия и от статуса информации, с которой работают сотрудники.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность предприятия: ключевые угрозы и средства защиты. [Электронный ресурс]. – Режим доступа: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (дата обращения: 02.07.2020).
2. Исследование: угрозы информационной безопасности. Часть 1: статистика [Электронный ресурс]. – Режим доступа: https://stakhanovets.ru/ (дата обращения: 05.07.2020).
3. ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/42103.html (дата обращения: 05.07.2020).

УДК 004.056.5

МЕТОДИКА ПРИМЕНЕНИЯ ПРОЦЕССА ВЫБОРА КОНТРМЕР НА ОСНОВЕ ИГРОВОГО ПОДХОДА

Десницкий Василий Алексеевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: desnitsky@comsec.spb.ru

Аннотация. В работе предложена методика применения процесса выбора контрмер против атак типа flood на основе коалиционной игры с пошаговой передачей хода.

Ключевые слова: выбор контрмер, теория игр, информационная безопасность.

A TECHNIQUE FOR APPLICATION OF THE PROCESS OF COUNTERMEASURE CHOICE ON THE BASE OF GAME THEORY APPROACH

Desnitsky Vasily
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: desnitsky@comsec.spb.ru

Abstract. The paper proposes a technique for applying the process of choosing of countermeasure against flood attacks on the base of a coalition game with turn-based progress.

Keywords: countermeasure choice, game theory, information security.

Разработанная методика направлена на осуществление процесса выбора контрмер при реагировании на сетевые атаки и построена на основе подхода к моделированию средств выбора контрмер для противодействия атакам усиления пропускной способности DNS [1]. Методика применима к более широкому классу атак – атакам типа flood, направленным на исчерпание пропускной способности сетевого канала узла. В качестве атакуемого узла рассматривается сервер, предоставляющий информационные сервисы неограниченному числу клиентов. Методика строится на базе математической коалиционной игры с пошаговой передачей хода. Выделяются две следующие коалиции, участники каждой из которых имеют общие интересы в рамках такой математической игры, а также могут быть логически и частично физически агрегированы в рамках одного игрока: атакующий хост и набор эксплуатируемых им ботов (нападающий); защищающий хост, сервер-жертва и легитимные клиенты (защитник).

Целевая характеристика нападающего – величина, определяющая число атакующих пакетов усредненного размера в секунду. Целевая характеристика защитника – величина, характеризующая число легитимных пакетов в секунду, поступающих на хост-жертву и обрабатываемых им. Данная величина на каждом ходе задается динамически в зависимости от суммарного запроса легитимных пользователей, отправляющих запросы на хост-

жертву. Предполагается, что эта величина всегда не превышает пропускной способности канала хоста-жертвы. Вместе с тем цель защитника состоит в том, чтобы в условиях атаки максимальное число легитимных пакетов было получено и обработано хостом-жертвой. Для нападающего и защитника определяются функции выигрыша, определяемые на каждом ходе и зависящие от выбранных параметров атаки и контрмер. Таким образом, нападающий и защитник имеют цели максимизации своей функции выигрыша на множестве действий атакующего и контрмер защитника, соответственно.

Предложенная методика состоит из следующих трех стадий. На стадии подготовки производится согласование между защитником и хостом-жертвой параметров входящего сетевого канала узла-жертвы. На стадии осведомления хост-жертва пересылает на хост-защитник текущие результаты анализа входящего трафика, включающие число принятых хостом-получателем легитимных и атакующих пакетов данных в единицу времени. На стадии оценивания и выбора контрмеры хост-защитник производит дискретный перебор возможных контрмер из имеющегося перечня с перебором допустимых значений параметров контрмер с максимизацией функции выигрыша, после чего выдает в качестве своих текущих выходных данных найденную контрмеру и ее параметры. Данная стадия организуется в виде цикла с заранее не ограниченным числом итераций, на которых осуществляются вычисления.

Работа выполнена при финансовой поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (уникальный идентификатор RFMEFI60719X0322).

СПИСОК ЛИТЕРАТУРЫ

1. Deshpande T., Katsaros P., Smolka S. A., Stoller S. D. Stochastic Game-Based Analysis of the DNS Bandwidth Amplification Attack Using Probabilistic Model Checking // 2014 Tenth European Dependable Computing Conference, Newcastle. 2014. P. 226-237, DOI: 10.1109/EDCC.2014.37.
2. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Monitoring and counteraction to malicious influences in the information space of social networks // 10th International Conference on Social Informatics (SocInfo). 2018. С. 159-167.
3. Balueva A., Desnitsky V., Ushakov I. Approach to detection of Denial-of-Sleep attacks in wireless sensor networks on the base of machine learning // Intelligent Distributed Computing XIII. 2019. С. 350-355.

УДК 004.056.5

ПОДХОД К АНАЛИЗУ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

Десницкий Василий Алексеевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: desnitsky@comsec.spb.ru

Аннотация. Предложен комплексный подход к анализу нарушений информационной безопасности в мобильных приложениях. Проводится анализ угроз информационной безопасности мобильных приложений, функционирующих в рамках мобильных устройств и беспроводных сенсорных сетей с учетом возможных видов программных и программно-аппаратных уязвимостей, которые способен успешно эксплуатировать потенциальный нарушитель информационной безопасности. Приведена характеристика основных направлений возможных атакующих воздействий. Кроме того, рассматриваются конкретные примеры известных видов атак. Предложенный подход применятся для оценки защищенности мобильных приложений на примере тестового коммуникационного приложения Мессенджер с использованием показателей критичности атак, их скрытности, а также организационно-технической сложности их выполнения. В процессе анализа используются существующие средства статического и динамического анализа кода мобильных приложений.

Ключевые слова: мобильное приложение, беспроводная сеть, информационная безопасность, нарушитель.

AN APPROACH TO ANALYSIS OF INFORMATION SECURITY VIOLATIONS IN MOBILE APPLICATIONS

Desnitsky Vasily
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: desnitsky@comsec.spb.ru

Abstract. A proposed complex approach comprises an analysis of information security violations in mobile applications. The analysis of the information security violations is performed on mobile applications operating within the framework of mobile devices and wireless sensor networks, taking into account possible types of software and hardware/software vulnerabilities that a potential information security violator can successfully exploit. Characteristics of the main directions of possible attacking influences are given. In addition, specific examples of known attack types are considered. The proposed approach is used to examine security of mobile applications by using an example of a test communication application Messenger by means of criticality indicators of attacks, their stealth, as well as organizational and technical complexity of their implementation. In the work, existing static and dynamic code analysis tools for mobile applications are used.

Keywords: mobile application, wireless network, information security, intruder.

В настоящее время мобильные вычисления широко используются в различных областях приложения. При этом стремительно возрастают как число, так и разнообразие угроз информационной безопасности мобильных устройств [1]. Большая часть мобильных атак используют уязвимости в мобильных приложениях и операционной системы, которые необходимо устранить на этапе разработки программного обеспечения для таких устройств. В результате разработка встраиваемых компонентов защиты является важной и неотъемлемой частью процесса построения мобильных приложений.

Используемые в настоящее время различные приложения зачастую подвергаются многочисленным атакам со стороны злоумышленников, основной целью которых является изменение отдельных особенностей или правил поведения программы. В частности, к целям несанкционированных воздействий относятся получение атакующим каких-либо дополнительных преимуществ, не предусмотренных разработчиком программы.

Подобные атаки могут основываться на изменении некоторого участка кода, позволяем открыть нарушителю какие-либо новые недокументированные возможности или снять заданные функциональные, ресурсные или иные ограничения. Так, например, это может быть попытка реализации неправомерного пользовательского доступа к интерфейсу приложения без наличия соответствующего легально приобретенного цифрового ключа, или же незаконное изменение установленного разработчиками периода действия лицензионного соглашения на данное программное приложение.

Согласно аналитическим оценкам, величина потерь от несанкционированного модификации программ и использования их злоумышленниками в своих целях приобретает все большие значения, что в свою очередь обуславливает необходимость разработки новых и дальнейшего повышения эффективности существующих методов защиты [2].

В работе проведен анализ существующих разновидностей атак на мобильные приложения и уязвимостей мобильных устройств и приложений, на которых базируются подобные атаки. К основным направлениям воздействий на мобильные устройства можно отнести деструкцию пользовательских или служебных данных, кода программных приложений или компонентов операционной системы. При этом объект воздействия может подвергаться искажениям, включающим осуществление модификаций, формирование помех и физическую деформацию носителей. Кроме того возможным становится некорректное уничтожение информации, способное привести приложение или устройство в целом к ошибкам несоответствия и неправильного конфигурирования.

Актуальным направлением воздействия является также дисфункция, предполагающая установку некорректных условий доступа, включающая несанкционированные перемещения фрагментов информации из защищенных в незащищенные модули хранения и модификации правил доступа к ним [3]. Кроме того, дисфункция может включать также нарушение установленных правил доступа, включающих устранение и обход применяемых алгоритмов защиты

Еще одним важным направлением воздействий является ухудшение условий использования мобильного приложения или устройства в целом, включающее, в том числе, несанкционированное внедрение на устройство злонамеренного кода, позволяющего удаленному нарушителю его использовать в качестве узла ботнета. Такая атака способна приводить к снижению производительности устройства и введению провайдерами ограничений на его сетевую активность. Кроме того, возможность выполнения не доверенного кода на мобильном устройстве может представлять опасность успешной реализации других видов атак на него.

К конкретным видам атак на мобильные устройства можно отнести декомпиляцию и деобфускацию бинарного кода приложения; перехват и подмену данных, передаваемых на устройство (MitM-атака); "рутование" устройства и атаки на приложение и применяемые в нем алгоритмы через внешние отладочные инструменты; атаки, эксплуатирующие уязвимости конкретных видов аппаратных интерфейсов мобильных устройств, таких как NFC, Bluetooth, включая атаки с использованием подключаемых физически скомпрометированных doc-станций, внешних накопителей и др. [4]; атаки на основе модифицированных обновлений приложений и компонентов операционной системы устройства; атаки методами социальной инженерии [5].

В работе также проводится ранжирование атакующих воздействий на мобильные приложения с использованием показателей критичности атак, их скрытности, а также организационно-технической сложности их выполнения.

Практическая часть работы выполняется на примере разработанного тестового программного приложения Мессенджер в рамках мобильной платформы Android с использованием инструментов статического и динамического анализ мобильных приложений, включающих средства декомпиляции байт-кода, деобфусикаторы и другие средства анализа [6].

К используемым инструментам статического анализа кода относятся Jadx, ApkTool, APKiD, Simplify, тогда как в качестве средств динамического анализа применяются Frida, Objection, Drozer, Inspeckage и др. [7-8]. В качестве одного из своих применений, данный подход может быть использован для верификации динамически формируемых беспроводных сенсорных сетей, состоящих из устройств современных мобильных платформ, а также для определения и ранжирования возможных атакующих воздействий в таких сетях.

Работа выполнена в СПИИРАН при финансовой поддержке Российский фонд фундаментальных исследований (РФФИ), проект 19-07-00953.

СПИСОК ЛИТЕРАТУРЫ

1. Nagarjun P., Ahamad S.S. Review of Mobile Security Problems and Defensive Methods // International Journal of Applied Engineering Research. Vol. 13. 2018. P. 10256-10259
2. Desnitsky V., Kotenko I., Rudavin N. Ensuring availability of wireless mesh networks for crisis management // Studies in Computational Intelligence. 2018. Vol. 798. P. 344-353.
3. Alin Z., Pocatilu P., Capisizu S. Mobile data vulnerabilities. 2019. P. 407-412. DOI: 10.12948/ie2019.06.10.
4. Hur J., Shamsi J. A survey on security issues, vulnerabilities and attacks in Android based smartphone // Proceedings of 2017 International Conference on Information and Communication Technologies (ICICT). 2017. P. 40-46. DOI: 10.1109/ICICT.2017.8320163.
5. Десницкий В.А., Котенко И.В. Модель защиты программного обеспечения на основе механизма "удаленного доверия" // Известия высших учебных заведений. Приборостроение. 2008. Т. 51. № 11. С. 26-31.
6. Sowndarajan K., Binu S. Android security issues and solutions // Proceedings of IEEE 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). 2017. 686-689. 10.1109/ICIMIA.2017.7975551. DOI: 10.1109/ICIMIA.2017.7975551.
7. Gao J., Li L., Kong P., Bissyandé T., Klein J. Understanding the Evolution of Android App Vulnerabilities // IEEE Transactions on Reliability. 2019. P. 1-19. DOI: 10.1109/TR.2019.2956690. ·
8. Taleby Ahvanooey M., Li Q., Rabbani M., Rajput A. A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks // International Journal of Advanced Computer Science and Applications. 2017. Vol. 8. No. 10. P. 30-45. DOI: 10.14569/IJACSA.2017.081005.

УДК 004.056

ОПРЕДЕЛЕНИЕ НАБОРА АТРИБУТОВ ДЛЯ ФОРМИРОВАНИЯ ПРОФИЛЯ АТАКУЮЩЕГО ПРИ АНАЛИЗЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дойникова Елена Владимировна, Новикова Евгения Сергеевна, Гайфулина Диана Альбертовна, Котенко Игорь Витальевич

Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: {doynikova, novikova, gaifulina, ivkote}@comsec.spb.ru

Аннотация. Рассматривается задача определения модели атакующего в форме профиля атакующего, то есть набора атрибутов, для применения в задачах анализа рисков. В исследовании используются методы интеллектуального анализа данных журналов событий информационных систем и сетевого трафика.

Ключевые слова: профиль атакующего; модель атакующего; атрибуты анализ рисков; анализ данных.

DETERMINING THE SET OF ATTRIBUTES FOR SPECIFICATION OF ATTACKER PROFILE IN RISK ANALYSIS TASKS

Doynikova Elena, Novikova Evgenia, Gaifulina Diana, Kotenko Igor

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: {doynikova, novikova, gaifulina, ivkote}@comsec.spb.ru

Abstract. The task of attacker model specification as an attacker profile, i.e. the set of attributes, is considered for application in risk analysis. The methods of data mining for event logs of information systems and network traffic are used.

Keywords: attacker profile; attacker model; attributes; risk analysis; data analysis.

Модель атакующего является одной из основных моделей в задачах анализа рисков и других задачах информационной безопасности. Целью исследования является определение модели атакующего в форме профиля атакующего, то есть набора атрибутов. В процессе исследования методов определения и применения модели атакующего [1] был сформулирован ряд вопросов, касающихся модели атакующего, в том числе, как определить данную модель, как вычислять параметры данной модели не экспертным путем, а на основе реальных данных, собираемых в процессе работы анализируемой системы, где взять подходящие исходные данные проведения экспериментов.

Для ответа на первые два вопроса в работе вводится формальная модель атакующего и выделяются атрибуты, составляющие предложенную модель. Были выделены низкоуровневые и высокоуровневые атрибуты. Низкоуровневые атрибуты вычисляются непосредственно на основе «сырых» данных, то есть сетевого трафика и журналов событий (например, частота атак или частот инцидентов безопасности). Высокоуровневые атрибуты являются метриками атакующего и вычисляются на основе низкоуровневых атрибутов (например, уровень навыков или мотивация атакующего). В работе вводится классификация низкоуровневых и высокоуровневых атрибутов, а также первичное сопоставление низкоуровневых атрибутов высокоуровневым. Для ответа на третий вопрос были сформулированы требования к набору данных, необходимому для проведения экспериментов, проанализированы существующие наборы данных и выбраны для экспериментов наборы данных с соревнований по захвату флага (capture the flag, CTF), а именно: сетевой трафик с соревнования DEFCON 26 CTF [2]; журналы событий с соревнований National CPTC 2019 [3]. Эти наборы данных были выбраны, т.к. содержат данные о множестве атакующих действий, осуществляемых разными типами атакующих против одной информационной системы.

В работе были проведены первые эксперименты с использованием набора данных DEFCON 26 CTF с выделенными атрибутами профиля атакующего, направленные на кластеризацию атакующих в зависимости от

уровня навыков с использованием методов t-SNE (стохастическое вложение соседей с t-распределением) [4], многомерного шкалирования (MDS) [5] и k-средних. Результаты показали, что большинство атакующих имеют примерно одинаковый высокий уровень навыков, что согласуется с тем, что в финал соревнований выходят команды высококвалифицированных атакующих и позволяет предположить, что выделенные атрибуты подходят для определения профиля атакующего.

В будущих исследованиях планируется расширить набор атрибутов и набор экспериментов для определения того, являются ли выделенные параметры эффективными для выявления разных типов атакующих, а также вписать предложенную модель в подход к анализу рисков.

Работа выполнена при финансовой поддержке стипендии президента РФ (СП-751.2018.5).

СПИСОК ЛИТЕРАТУРЫ

1. Doynikova, E., Novikova, E., Kotenko, I. Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects // Information. Vol. 11, 2020.
2. Официальная страница соревнований DEFCON 26 CTF [Электронный ресурс]. URL: https://media.defcon.org/DEF\%20CON\%2026/DEF\%20CON\%2026\%20ctf/ (дата обращения: 19.07.2020).
3. Официальная страница соревнований CPTC 2019 [Электронный ресурс]. URL: http://mirrors.rit.edu/cptc/2019/mirrors/ (дата обращения: 19.07.2020).
4. Laurens van der Maaten, Hinton, G. Visualizing Data using t-SNE // Journal of Machine Learning Research. Vol. 9, 2008, C. 2579-2605.
5. Torgerson, W.S. Multidimensional scaling I: Theory and method // Psychometrika. Vol. 17, 1952, C. 401-419.

УДК 004.056

МЕТОДИКА ВЫБОРА МЕР ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИИ МЕТРИК БЕЗОПАСНОСТИ

Дойникова Елена Владимировна, Федорченко Андрей Владимирович, Гайфулина Диана Альбертовна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: {doynikova, fedorchenko, gaifulina}@comsec.spb.ru

Аннотация. Предлагается методика выбора мер противодействия кибератакам с учетом обнаруженных событий безопасности и различных профилей атакующего. В основе методики лежит разработанная онтология метрик безопасности.

Ключевые слова: меры противодействия; кибератака; онтология; метрики безопасности.

TECHNIQUE FOR SELECTION OF COUNTERMEASURES AGAINST CYBER ATTACKS BASED ON THE ONTOLOGY OF SECURITY METRICS

Doynikova Elena, Fedorchenko Andrey, Gaifulina Diana
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: {doynikova, fedorchenko, gaifulina}@comsec.spb.ru

Abstract. The technique for counteraction against cyber attacks considering detected security incidents and different attacker profiles is proposed. The technique is based on the developed ontology of the security metrics.

Keywords: security measures; cyber attack; ontology; security metrics.

Выделяются превентивный и реактивный подходы к выбору мер защиты от кибератак. Статистика кибератак показывает, что зачастую они реализуются с использованием заранее неизвестных уязвимостей, поэтому превентивный подход не всегда работает. Современные системы защиты используют методы анализа поведения пользователей и устройств для своевременного выявления и реагирования на кибератаки. Для этого реализуется подробное журналирование всех происходящих в системе событий. На данный момент реальные инструменты в основном используют правило-ориентированные методы обнаружения кибератак на основе событий, в то время как интеллектуальные методы анализа событий представляются более перспективными, но еще недостаточно развиты. Целью данной работы является разработка методики выбора мер противодействия кибератакам с учетом обнаруженных событий безопасности и различных профилей атакующих, использующей методы интеллектуального анализа данных.

Данное исследование проводилось в несколько этапов. На первом этапе была разработана онтология метрик безопасности, связывающая различные объекты, взаимодействующие в процессе оценивания защищенности системы и выбора мер противодействия кибератакам (в том числе, атакующий, атака, мера противодействия), а также метрики безопасности, лежащие в основе методик оценивания защищенности (например, уровень навыков атакующего, риск безопасности) и выбора мер противодействия (например, эффективность меры противодействия) [1].

На втором этапе проводился анализ и корреляция событий, предшествовавших инциденту безопасности, и разработка методики прогнозирования инцидентов по происходящим в системе событиям, с использованием методов машинного обучения. Для анализа были выбраны журналы событий с соревнований по захвату флага (capture the flag, CTF), а именно, с соревнований National CPTC 2019 [2]. Эти журналы включают как журналы

событий различных объектов специально разработанной для соревнований информационной системы организации, имитирующей банк, так и журнал инцидентов, зафиксированных системой обнаружения вторжений Suricata [3] в процессе проведения кибератак различными командами, соответствующими разным профилям атакующих.

На третьем этапе проводилась разработка методики связывания обнаруженных событий и инцидентов с объектами инфраструктуры анализируемой системы, для последующего динамического обновления онтологии и выбора оптимальных мер противодействия. Для этого анализировались свойства событий и инцидентов.

Методика выбора мер противодействия работает на основе логического вывода с использованием связей разработанной онтологии, в том числе связей между обнаруженным инцидентом, объектом инфраструктуры, к которому относится инцидент, уязвимостями этого объекта инфраструктуры, кибератаками, применимыми к данному объекту и соответствующими выявленному инциденту, атакующими, и мерами противодействия, применимыми против соответствующей кибератаки и атакующего, и доступными для заданного объекта инфраструктуры. В результате формируется список доступных мер противодействия. Выбор оптимальной меры противодействия осуществляется за счет оптимизации коэффициента выбора мер противодействия, рассчитанного для доступных мер противодействия.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-01246).

СПИСОК ЛИТЕРАТУРЫ

1. Doynikova, E., Fedorchenko, A., Kotenko, I. A semantic model for security evaluation of information systems // Journal of Cyber Security and Mobility. 2020.
2. Официальная страница соревнований CPTC 2019 [Электронный ресурс]. URL: http://mirrors.rit.edu/cptc/2019/mirrors/ (дата обращения: 19.07.2020).
3. Официальная страница Suricata [Электронный ресурс]. URL: https://suricata-ids.org/ (дата обращения: 19.07.2020).

УДК 004.5

УПРАВЛЕНИЕ ДАННЫМИ ВИЗУАЛИЗАЦИИ МОБИЛЬНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ СЕНСОРНЫХ ЭКРАНОВ

Жернова Ксения Николаевна, Гайфулина Диана Альбертовна, Иванов Александр Юрьевич, Комашинский Владимир Ильич

Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: zhernova@comsec.spb.ru, gaifulina@comsec.spb.ru, vniira@yandex.ru, kama54@rambler.ru

Аннотация. Вместе с распространением интерфейсов, основанных на сенсорных экранах, появляются приложения для управления безопасностью, поддерживающие жестовое управление. Однако поддерживаемые модели взаимодействия всё ещё малофункциональны и практически не отвечают принципу прямого взаимодействия. Мобильные сети связи так же, как и другие области телекоммуникаций, подвержены сетевым атакам, поэтому для них тоже необходимо разрабатывать приложения безопасности. При этом для повышения эффективности принятия решений требуется разработка эффективных моделей человеко-компьютерного взаимодействия. В докладе будет рассмотрена модель взаимодействия с визуализацией данных мобильной сети.

Ключевые слова: пользовательский интерфейс, визуализация данных, сенсорный интерфейс, человеко-компьютерное взаимодействие, мобильные сети, компьютерная безопасность.

MOBILE NETWORK VISUALIZATION DATA MANAGEMENT USING TOUCH SCREENS

Zhernova Ksenia, Gaifulina Diana, Ivanov Alexander, Komashinskiy Vladimir

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: zhernova@comsec.spb.ru, gaifulina@comsec.spb.ru, vniira@yandex.ru, kama54@rambler.ru

Abstract. With the proliferation of touchscreen-based interfaces, security management applications that support gesture control are emerging. However, the supported interaction models are still poorly functional and practically do not meet the principle of direct manipulation. Mobile communication networks, like other areas of telecommunications, are susceptible to network attacks, so they also need to develop security applications. Moreover, to increase the efficiency of decision-making, the development of effective models of human-computer interaction is required. The report will consider a model of interaction with the visualization of mobile network data.

Keywords: user interface, data visualization, touch interface, human-computer interaction, mobile networks, computer security.

Несмотря на повсеместное распространение Интернет-технологий, мобильная связь всё ещё остаётся востребованной. По этой причине существует множество атак, направленных против пользователей мобильной сети. Кроме того, мобильные сети всё ещё содержат большое количество уязвимостей, которые могут быть использованы для сетевых атак на различных уровнях. Быстрое детектирование аномалий в сети позволяет предотвратить возможные действия злоумышленника.

Для выявления инцидентов безопасности требуется анализировать большие объёмы данных, передающихся по мобильной сети. При этом оператору удобнее всего работать с графической визуализацией обрабатываемых данных. Для эффективного анализа этих данных для модели визуализации необходимо разрабатывать адекватную модель взаимодействия, которая позволит повысить её эффективность: повысить количество отображаемых данных без перегрузки визуализации, взаимодействовать с данными на разных уровнях и т.п. В докладе предложена модель человеко-компьютерного взаимодействия с визуализацией данных мобильной сети связи.

Для анализа данных безопасности мобильной сети могут применяться различные модели визуализации. Чаще всего для подобных целей используются следующие модели [1, 2]: географические карты, тепловые карты, карты Вороного.

При этом такие модели могут совмещаться между собой для выполнения разных типов задач. Например, географические карты, которые используются для отображения географической позиции инцидента безопасности, часто комбинируются с тепловыми картами в целях отображения каких-либо количественных показателей. Карты Вороного можно накладывать поверх географических карт для обозначения местоположения базовых станций мобильной сети и зон их покрытия.

Поскольку в настоящее время распространены устройства с сенсорными экранами, а также появляются приложения безопасности с сенсорным интерфейсом управления, целесообразно разрабатывать модели взаимодействия с помощью жестов сенсорных экранов.

В целях увеличения эффективности работы оператора с моделями визуализации мобильной сети была разработана модель человеко-компьютерного взаимодействия на основе жестов. Жестовое взаимодействие с визуализацией мобильной сети выглядит следующим образом: сведение и разведение несколькими пальцами для перемещения между уровнями карты [3], вращение для поворота карты, листание несколькими пальцами влево-вправо для смены модели визуализации, касание одним пальцем – выбор нужной соты, долгое касание одним пальцем – вызов контекстного меню конкретной соты, долгое касание тремя пальцами – вызов фильтра, перемещение тремя пальцами – перемещение зоны фильтра.

Оценку моделей взаимодействия с визуализацией мобильных сетей связи планируется проводить экспериментально с помощью тестов на пользователях. Оцениваться будут формальные параметры, такие как скорость и точность выполнения заданий, также будут учтены субъективные впечатления пользователей от работы с разрабатываемым интерфейсом. Скорость будет измеряться как время прохождения каждого задания. Уровень точности будет выявляться как количество ошибок, допущенных при выполнении каждого задания. Субъективная оценка будет получена с помощью опросов.

В докладе рассмотрены сложные модели визуализации, пригодные для представления данных безопасности мобильных сетей связи. Представлены модели взаимодействия на основе сенсорных экранов, с помощью которых можно взаимодействовать с этими визуализациями. Разрабатываемая модель взаимодействия позволит управлять данными инцидентов безопасности как отдельной соты, так и группы сот, выбирать соответствующую ситуации модель визуализации и выбирать требуемый уровень абстракции, при этом модель будет соответствовать принципам прямого взаимодействия [4] и, таким образом, будет естественна для оператора.

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01488).

СПИСОК ЛИТЕРАТУРЫ

1. Kolomeets M. et al. Voronoi Maps for Planar Sensor Networks Visualization //International Symposium on Mobile Internet Security. – Springer, Singapore, 2017. – С. 96-109.
2. Коломеец М.В., Чечулин А.А., Дойникова Е.В., Котенко И.В. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение, Т.61, № 10, 2018, С.873-880. DOI: 10.17586/0021-3454-2018-61-10-873-880.
3. Котенко И.В., Коломеец М. В., Комашинский В. И., Бушуев С. Н., Гельфанд А. М. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. СПб.: СПОИСУ. 2018. С.143-144.
4. Shneiderman B. The eyes have it: A task by data type taxonomy for information visualizations //The Craft of Information Visualization. – 2003. – P. 364-371.

УДК 004.056

ОПРЕДЕЛЕНИЕ АТРИБУТОВ ДЛЯ УСТАНОВЛЕНИЯ АВТОРСТВА ВРЕДОНОСНОГО КОДА НА ОСНОВЕ АНАЛИЗА ГРАФА ПОТОКА УПРАВЛЕНИЯ

Картель Анастасия Владимировна[1], Новикова Евгения Сергеевна[1], Муренин Иван Николаевич[2], Дойникова Елена Владимировна[2]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mails: imurenin@gmail.com, elenadoynikova@mail.ru, anv.kartel@gmail.com, evgenia.novikova123@gmail.com

Аннотация. Атрибуция авторства исходного кода - это процесс идентификации авторства исходного кода на основе набора известных примеров кода, принадлежащих данному автору. Одним из практических

приложений атрибуции кода является анализ и обнаружение вредоносных программ. В статье мы исследуем проблему установления авторства приложений Android на основе классификации графа потока управления, предлагаются признаки, которые могут быть использованы для построения модели анализа.

Ключевые слова: атрибуция авторства программного кода, вредоносный код, Android приложения, граф потока управления

DEFINING ATTRIBUTES FOR MALWARE AUTHORSHIP ATTRIBUTING BASED ON CONTROL FLOW GRAPH ANALYSIS

Kartel Anastasia, Novikova Evgenia, Murenin Ivan, Doynikova Elena
[1] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: imurenin@gmail.com, elenadoynikova@mail.ru, anv.kartel@gmail.com, evgenia.novikova123@gmail.com

Abstract. Source attribution is the process of identifying authorship of source code based on a set of known code examples belonging to a given author. One of the practical applications of code attribution is malware analysis and detection. In this article, we explore attribution of Android apps based on analysis of control flow graph attributes, the possible set of attributes to construct analysis model is suggested.

Keywords: code authorship attribution, malware, Android applications, control flow graph.

Задача определения авторства кода связана со способностью определять авторов программного кода на основе их стиля кодирования. Эта задача имеет много практический приложений и используется в таких задачах как, определение наиболее вероятного автора работы, группировка авторов на основании сходства по какому-либо признаку, анализ эволюции авторских навыков программирования, предпочтений и стиля письма за определенный период времени, проверка авторства, т.е. определения автора данного примера кода [1]. Другое интересное практическое применение этого подхода - это криминалистическая экспертиза программного обеспечения, когда аналитик, имеющий набор образцов вредоносных программ, пытается определить возможного автора вредоносного ПО.

Одна из основных сложностей в атрибуции – работа со стилем автора. Установление авторства в значительной степени зависит от информации, которая позволяет проводить глубокий лингвистический анализ. В программном обеспечении акцент часто делается на именование переменных, интервалы, макет программы. При анализе вредоносного ПО исследователи зачастую работают с двоичным представлением, которое хранит малое число характеристик.

В общем случае, анализируемые атрибуты можно разделить на пять основных групп [2]: лексические, синтаксические и семантические, поведенческие и зависящие от приложения. Лексические атрибуты могут быть извлечены из исходного или двоичного файла и представляют собой длину строк, количество строк в программе, количество операндов, количество переменных, частоты слов, частоты токенов, символьную N-грамму, имена функций или методов и идентификаторы. Синтаксические атрибуты характеризуют внешнюю структурную организацию кода. В основе их использования лежит предположение, что разработчикам кода, склонным использовать процедуры кода бессознательно, удобно оставаться в сложившихся привычках, которые трудно изменить. Семантические параметры отражают логический поток кода и дают глубокое понимание его внутренней работы. Поведенческие особенности могут быть получены из динамической информации, генерируемой при выполнении двоичного файла программы. К ним относятся системные вызовы, доступ к файлам, сетевые подключения, созданный mutex, посещенные URL-адреса и сгенерированные динамические значения. И наконец, последняя группа атрибутов, зависящих от приложений, описывают связанные библиотеки, ресурсы (например, изображения и звуковые файлы), файлы свойств, файлы журнала и файлы разрешений.

В зависимости от типа используемых атрибутов можно выделить различную форму их представления: токены, строки, n-граммы, идиомы, графы.

В настоящей работе анализируются графы потоков программ, относящиеся к семантическим атрибутам установления авторства кода. В общем случае, графы - это набор узлов, представляющих основные блоки программы, связанные с направленными ребрами. Это представление используется для моделирования потока и структуры программы. Графы могут использоваться для атрибуции в различных формах и могут быть построены как из исходного кода, так и из двоичного кода.

В настоящей работе графы управления потоками строились для Android-приложений. Они извлекались с помощью утилит dexdump и androguard. Граф потоков CFG записывался в формате .dot. Пример описания графа представлен ниже:

- subgraph taken_edges {
- edge [color="#00FF00",weight=.3,len=3];
- node0:p0 -> node3:p4;
- node3:p10 -> node6:p19;

– node4:p14 -> node6:p19;
– node5:p18 -> node2:p3;
– node6:p24 -> node2:p3; }

Данный граф может быть отображен с помощью утилиты GraphViz. В этом случае блоки последовательно исполняемого кода отрисовываются в виде прямоугольников, а передача управления в виде стрелок разного цвета. Цвета имеют следующие обозначения: красный цвет обозначает исключения, зеленый – подграфы, из которых берутся данные ребра, черный – регулярные ребра.

В [3] для описания графов авторы используют 20 атрибутов, описывающих граф в целом. Среди признаков представлены такие как соотношение числа ребер и вершин графа, процент листовых, средних и изолированных вершин в графе, средняя степень вершин, средний коэффициент кластеризации, средняя длина путей в графе, количество и средний размер компонент связности, спектр матрицы смежности и ее след и др. В [4] для анализа вредоносного кода используются следующие атрибуты, извлеченные из графа потока управления: число маркированных ветвей, средняя глубина узла и т.д. Для установления авторства кода нами предложено использовать следующие атрибуты: 1) число подграфов – общее число подграфов; 2) число узлов – сумма всех узлов в файле; 3) среднее число узлов – отношение общего числа узлов к числу подграфов; 4) среднее число ребер – отношение общего числа ребер к числу подграфов; 5) средний вес узла – отношение суммы весов всех узлов на число узлов (вес узла – это число инструкций узла); 6) максимальный вес узла – максимальный вес узла на файл; 7) доля изолированных подграфов – доля подграфов, состоящих из одного узла и не имеющих входных или исходящих связей, состоящий только из последовательных инструкций; 8) изолированные точки внутри графа (nop) - это вершины внутри подграфа, не имеющих входные и исходящие связи.

Полученный набор был исследован методами визуального анализа, было показано, что точки, описываемые этими параметрами, образуют в некоторых случаях четко ограниченные кластеры, а в некоторых – рассеяны по плоскости. Это позволяет заключить, что ряд авторов имеют характерный аналитический подход к решению проблемы, который не изменяется от программы к программе.

Работа выполнена при финансовой поддержке Гранта Российского Фонда Фундаментальных Исследований (РФФИ) № 19-07-01246 а.

СПИСОК ЛИТЕРАТУРЫ

1. Caliskan-Islam, A., Harang, R., Liu, A., Narayanan, A., Voss, C., Yamaguchi, F., Greenstadt, R.: De-anonymizing programmers via code stylometry. In: Proceedings of the 24th USENIX Security Symposium (2015), pp 255-270.
2. Gonzalez, H., Stakhanova, N., Ghorbani, A.A.: Authorship attribution of android apps. In: CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy (2018). Pp 277-286. https://doi.org/10.1145/3176258.3176322.
3. Geng Li, Murat Semerci, Bulent Yener, and Mohammed J Zaki. Graph classification via topological and label attributes. In Proceedings of the 9th international workshop on mining and learning with graphs (MLG), San Diego, USA, volume 2, 2011.
4. Caliskan, A., Yamaguchi, F., Dauber, E., Harang, R., Rieck, K., Greenstadt, R., Narayanan, https , A.: When Coding Style Survives Compilation: De-anonymizing Programmers from Executable Binaries. In: Proc. of Network and Distributed Systems Security (NDSS) Symposium 2018. https://doi.org/10.14722/ndss.2018.23304.

УДК 004.5

ВИЗУАЛЬНЫЙ АНАЛИЗ БОТОВ СОЦИАЛЬНОЙ СЕТИ В ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Коломеец Максим Вадимович, Жернова Ксения Николаевна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: kolomeec@comsec.spb.ru, zhernova@comsec.spb.ru

Аннотация. Одним из основных инструментов оказания вредоносного влияния в социальных сетях являются боты. Однако, злоумышленники научились маскировать численные параметры ботов таким образом, чтобы средства защиты социальных сетей не смогли их распознать. В таких ситуациях одним из методов выявления может стать визуальная аналитика социальных графов, так как подделать социальную структуру намного сложнее. В докладе будет рассмотрен подход визуальной аналитики графов социальных сетей с использованием средств виртуальной и дополненной реальности.

Ключевые слова: обнаружение ботов, визуализация данных, анализ социальных сетей, социальные графы, визуальная аналитики, информационная безопасность.

VISUAL ANALYSIS OF SOCIAL NETWORK BOTS IN AUGMENTED REALITY

Kolomeets Maxim, Zhernova Ksenia
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: kolomeec@comsec.spb.ru, zhernova@comsec.spb.ru

Abstract. Bots are one of the main tools for exerting malicious influence on social networks. However, cybercriminals have learned to mask the numerical parameters of bots in such a way that the security tools of social networks could not recognize them. In such situations, visual analytics of social graphs can become one of the methods

of identification, since it is much more difficult to falsify the social structure. The thesis will consider an approach to visual analytics of social network graphs using virtual and augmented reality.

Keywords: bot detection, data visualization, social networks analysis, social graphs, visual analytics, information security.

Как правило, для распознавания ботов используются методы, основанные на статистике и машинном обучении [1]. Данные методы используют численные метрики, такие как количество друзей, фотографий и т.д. [2] Однако злоумышленники научились имитировать метрики ботов таким образом, чтобы их было сложно распознать. Тем не менее, для злоумышленников одним из наиболее сложных методов маскировки остается подделка социальный структуры.

Процесс подделки и защиты социальных структур был детально изучен исследователями из Facebook [3]. Все легальные пользователи социальной сети формируют граф с топологией малого мира. Это значит, что друзья одного конкретного пользователя в высокой долей вероятности также будут друзьями. Для того чтобы не быть обнаруженным, бот должен стать частью данного графа. Это является трудоемкой задачей, так как пользователи обычно не добавляют незнакомые им аккаунты. Таким образом, обычно боты используют следующие стратегии:

1. Боты посылают запросы на добавление в друзья множеству случайных пользователей, рассчитывая, что малая часть из них примет запрос. В таком случае, друзья одного конкретного бота с низкой долей вероятности также будут друзьями, а структура графа друзей бота не будет формировать малый мир.
2. Боты посылают запросы на добавление в друзья другим ботам, имитируя малый мир. В таком случае, структура ботов будет образовывать малый мир, но он будет слабо связан с основным графом – малым миром легальных пользователей.

Таким образом, распознать ботов можно по структуре, которую они образуют. Для этого был разработан метод визуальной аналитики на основе технологии виртуальной реальности и программный прототип. В виртуальной реальности формируется 3D изображение графа социальной сети. Оператор при помощи контроллеров может выделять отдельные вершины графа (аккаунты), которые образуют подозрительные структуры. Ключевым преимуществом такого подхода является эффективность навигации оператора в большом графе и точность проведения операций с отдельными вершинами, в сравнении с аналогичным анализом, использующим LCD-дисплей.

В докладе была продемонстрирована работа прототипа на примере анализа сообществ ВКонтакте.

Работа выполнена при финансовой поддержке РФФИ (проект № 18-37-20047 мол_а_вед).

СПИСОК ЛИТЕРАТУРЫ

1. Karataş A., Şahin S. A review on social bot detection techniques and research directions //Proc. Int. Security and Cryptology Conference Turkey. – 2017. – P. 156-161.
2. Dong G., Liu H. (ed.). Feature engineering for machine learning and data analytics. – CRC Press, 2018.
3. Stein T., Chen E., Mangla K. Facebook immune system // Proceedings of the 4th Workshop on Social Network Systems, SNS'11. 2011.

УДК 004.056.5

МЕТОДИКА РАСПРЕДЕЛЕННОГО ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АНОМАЛИЙ НА ОСНОВЕ АНАЛИЗА БОЛЬШИХ ДАННЫХ

Комашинский Николай Александрович, Котенко Игорь Витальевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: nckkm@yandex.ru, ivkote1@mail.ru

Аннотация. Рассматривается методика распределенного обнаружения компьютерных атак на основе анализа больших данных, использующая методы сигнатурного анализа. Методика состоит из последовательности этапов и их шагов, описывающих действия оператора и системы обнаружения атак. Применение данной методики в системах обнаружения атак, позволяет ускорить процесс выявления компьютерных аномалий, благодаря использованию инструментов распределенной обработки данных.

Ключевые слова: компьютерная аномалия; алгоритм; распределенная файловая система; MapReduce, анализ данных; оператор безопасности; информационная система.

A TECHNIQUE OF DISTRIBUTED DETECTION OF COMPUTER ANOMALIES BASED ON BIG DATA ANALYSIS

Komashinsky Nickola, Kotenko Igor
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: nckkm@yandex.ru, ivkote1@mail.ru

Abstract. The paper considers a technique of distributed detection of computer attacks based on big data analysis using signature analysis methods. It consists of a sequence of stages and their steps describing the actions of the operator

and the attack detection system. The use of this technique in intrusion detection systems makes it possible to speed up the process of detecting computer anomalies through the use of distributed data processing tools.

Keywords: computer anomaly; algorithm; distributed file system; MapReduce, data analysis; security operator; Information system.

Методика распределенного обнаружения компьютерных атак на основе анализа больших данных требует определения основных стадий использования конкретных моделей и алгоритмов. Цель методики – повышение скорости обработки данных и точности выявления компьютерных аномалий с помощью распараллеленной предварительной обработки данных с последующим анализом больших данных.

Методика основана на трех следующих этапах: (1) Этап сбора информации; (2) Этап применения алгоритма выявления атак; (3) Этап анализа выходных данных. Каждый элемент методики ассоциирован с действиями одного из ее участников: оператора или системы обнаружения. Также указаны соответствия действий системы с реализующими их компонентами.

Этап 1. Сбор информации.

На данном этапе происходит сбор информации о сетевом трафике с применением предварительной обработки с последующей настройкой параметров системы. Формально этап может быть поделен на следующие подэтапы:

– формирование задачи исследования источника данных и определение параметров, по которым она будет исследоваться;

– проведение нормализации входящего трафика (размерность данных должна быть уменьшена, а данные должны быть преобразованы для дальнейшей обработки, устранена избыточность и др.);

– запуск процесса балансировки для распределения нагрузки на узлы кластера;

– корректировка данных оператором, позволяющая внести некоторые корректировки в собранные данные для увеличения точности работы алгоритмов обнаружения аномалий;

– запуск процесса сбора информации о входящем трафике. Для сбора используются соответствующие агенты системы обнаружения, собирающие данные с распределенных сенсоров, сообщения системных журналов, информацию о загрузки сети, а также сообщения безопасности брандмауэра;

– выявление типа атаки сигнатурными методами, для последующего применения соответствующего алгоритма обработки событий;

– сохранение всех данных в распределенной файловой системе HDFS (Hadoop Distributed File System

Этап 2. Применение алгоритма выявления атак.

На этом этапе осуществляется выявление атак с помощью разработанного комплекса алгоритмов, реализованных в системе обнаружения. В качестве исходных данных используются данные, собранные на Этапе 1. Этап 2 может быть поделен на следующие подэтапы:

– построение среды для работы алгоритмов после ручного запуска процесса оператором;

– выполнение сигнатурного анализа и задач MapReduce для распараллеленной обработки на нескольких узлах кластера;

– вычисление результатов работы и сравнение работы алгоритмов для точного выявления вредоносного воздействия;

– во время работы этапа 2 для работы с MapReduce используются модуль анализа аномалий, а сигнатурные правила остаются актуальными, благодаря компоненту обновления сигнатур.

Этап 3. Анализ выходных данных.

На данном этапе происходит непосредственный вывод результатов оператору, который был получен на предыдущем этапе. Этап может быть поделен на следующие подэтапы:

– формирование оповещений об аномальной активности и компьютерных атаках для оператора;

– сохранение выявленных событий в виде журналов, для возможности ознакомления с ранее полученными результатами;

– на всем протяжении работы этапа для сохранения результатов используются компоненты работы с базой данных.

Предлагаемая методика распределенного обнаружения компьютерных атак на основе анализа больших данных позволяет:

1) проводить нормализацию и балансировку поступающего в систему обработки трафика;

2) выявлять основные пути распространения компьютерной атаки от источников до целевой категории;

3) проводить нормализацию трафика и балансировку нагрузки на сенсоры системы с целью ускорения обработки больших потоков данных;

4) получать основные данные о компьютерной атаке, своевременно формировать оповещения для оператора для возможности оперативного реагирования на инциденты информационной безопасности;

5) сформировать на основе полученных результатов наиболее эффективную схему контрмер для повышения безопасности информационной системы.

Одним из важнейших элементов методики является применение модели MapReduce, предназначенной для создания фреймворка для параллельных вычислений для обработки больших данных.

Таким образом, результатом методики является своевременное обнаружение компьютерных атак, позволяющее оператору оперативно реагировать на события в сетях с большими скоростями передачи данных и большими объемами передаваемой информации. Данная методика, способствует выявлению специфицированных типов атак, и, благодаря распределенной обработке, позволяет существенно ускорить работу целевой системы обнаружения атак.

Работа выполнена при финансовой поддержке Гранта РФФИ № 18-07-01488 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Saenko I., Branitskiy A. Improving the Performance of Manufacturing Technologies for Advanced Material Processing Using a Big Data and Machine Learning Framework // Materials Today: Proceedings. 2019. vol. 11. part 1. pp. 380-385. DOI: 10.1016/j.matpr.2018.12.162.
2. Kotenko I., Komashinsky N. Combining Spark and Snort Technologies for Detection of Network Attacks and Anomalies: Assessment of Performance for the Big Data Framework // 12th International Conference on Security of Information and Networks (SIN 2019). September 12th-15th, 2019 - Sochi, Russia. Proceedings by ACM International Conference Proceeding Series (ICPS). ACM, New York, NY, USA, 2019. Article No. 16. 8 p.
3. Kotenko I., Saenko I., Branitskiy A. Detection of Distributed Cyber Attacks Based on Weighted Ensembles of Classifiers and Big Data Processing Architecture // IEEE INFOCOM19 Workshop of BigSecurity, Paris, France, 2019. IEEE Xplore. 6 p.
4. Котенко И.В., Саенко И.Б., Авраменко В.С. Концептуальный подход к обеспечению информационной безопасности системы распределенных ситуационных центров // Информатизация и связь. 2019. № 3. С. 37-42.
5. Котенко И.В., Пелёвин Д.В., Ушаков И.А. Общая методика обнаружения инсайдера компьютерной сети на основе технологий больших данных // VIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2019). 2019. Т. 1. С. 572-576.

УДК 004.056.5

ТЕОРЕТИКО-МНОЖЕСТВЕННАЯ МОДЕЛЬ РАСПРЕДЕЛЕННОГО ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК С ПРИМЕНЕНИЕМ СИГНАТУРНОГО АНАЛИЗА

Комашинский Николай Александрович, Котенко Игорь Витальевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: nckkm@yandex.ru, ivkote1@mail.ru

Аннотация. Рассматривается модель экспертной системы обнаружения вторжений в режиме реального времени. Модель включает спецификацию профилей для представления поведения субъектов по отношению к объектам с помощью метрик и статистических моделей, а также определение правил получения знаний об этом поведении из записей аудита и правил обнаружения аномальной активности. Модель не зависит от какой-либо конкретной системы, среды, уязвимости системы или типа вторжения, тем самым обеспечивая основу для экспертной системы обнаружения вторжения общего назначения.

Ключевые слова: компьютерная атака; сигнатура; аномалия; несанкционированный доступ; Hadoop; оператор безопасности; информационная система.

THEORETICAL-MULTIPLE MODEL OF DISTRIBUTED DETECTION OF COMPUTER ATTACKS USING SIGNATURE ANALYSIS

Komashinsky Nickola, Kotenko Igor
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: nckkm@yandex.ru, ivkote1@mail.ru

Abstract. A model of an expert real-time intrusion detection system is considered. The model includes specification of profiles for representing the behavior of subjects in relation to objects using metrics and statistical models, as well as rules for obtaining knowledge about this behavior from audit records and for detecting anomalous activity. The model is independent of any specific system, application environment, system vulnerability, or intrusion type, thus providing the basis for a general purpose intrusion detection expert system.

Keywords: computer attack; signature; anomaly; unauthorized access; Hadoop; security operator; information system.

Рассматриваемая модель основана на гипотезе о том, что использование уязвимостей информационной системы влечет за собой некорректную работу некоторых элементов системы; следовательно, нарушения безопасности могут быть обнаружены по отклонениям в работе системы. В качестве примеров можно привести следующие представленные ниже действия.

(1) Попытка взлома. Злоумышленник, пытающийся взломать систему, может генерировать аномально высокую частоту отказов пароля по отношению к одной учетной записи или системе в целом.

(2) Маскарад или успешная попытка взлома. Злоумышленник, входящий в систему, используя неавторизованную учетную запись и пароль, имеет такие атрибуты как время входа в систему, местоположение или тип подключения, отличные от тех, что у легитимного пользователя учетной записи. Кроме того, поведение злоумышленника может значительно отличаться от поведения легитимного пользователя; в частности, он может проводить большую часть времени, просматривая каталоги и выполняя команды состояния системы, в отличие

от законного пользователя, который, скорее всего, сосредоточится на редактировании или компиляции и компоновке стандартных программ.

(3) Несанкционированный доступ легитимным пользователем. Авторизованный пользователь, пытающийся проникнуть через механизмы безопасности в операционной системе, может запускать различные программы или вызывать нарушения защиты попытками доступа к вредоносным файлам или программам. Если его попытка увенчается успехом, он получит доступ к командам и файлам, которые ему обычно не разрешены.

(4) Утечка данных легитимным пользователем. Авторизованный пользователь, пытающийся похитить конфиденциальные документы, может войти в систему в необычное время или направить данные на удаленные принтеры, которые обычно не используются.

(5) Троянский конь. Поведение троянского коня, установленного в программе, может отличаться от легитимной программы, например, с точки зрения времени использования процессора.

(6) Вирус. Вирус, установленный в системе, может привести к увеличению частоты перезаписи исполняемых файлов, памяти, используемой исполняемыми файлами или к запуску определенной программы по мере распространения вируса.

(7) Отказ в обслуживании - злоумышленник, способный монополизировать ресурс (например, сеть), может иметь аномально высокую активность по отношению к ресурсу, в то время как активность всех остальных пользователей является аномально низкой.

Конечно, вышеуказанные формы аномального проявления также могут определять действия, не связанные с безопасностью. Они могут быть признаком того, что пользователь меняет рабочие задачи, приобретает новые навыки или делает ошибки при наборе текста; программные обновления; или изменение рабочей нагрузки в системе. Важной целью текущего исследования является определение того, какие виды деятельности и статистические показатели обеспечивают наилучшую дискриминационную способность; то есть имеют высокий уровень обнаружения и низкий уровень ложных срабатываний. В связи с гибкой настройкой конфигурационных файлов, сведением к минимуму ложных срабатываний предлагается использовать сигнатурный анализ.

Теоретико-множественная модель распределенного обнаружения компьютерных атак включает семь основных компонентов: (1) Субъекты – инициаторы активности на целевой системе - обычно это пользователи. (2) Объекты - ресурсы, управляемые системой - файлы, команды, устройства и т.п. (3) Записи аудита – генерируются целевой системой в ответ на действия, выполняемые или предпринимаемые субъектами над объектами, - вход пользователя в систему, выполнение команд, доступ к файлу и т. п. (4) Профили – структуры, которые характеризуют поведение субъектов относительно объектов с точки зрения статистических метрик и моделей наблюдаемой активности. Профили автоматически генерируются и инициализируются из шаблонов. (5) Записи аномалий – генерируются при обнаружении подозрительной активности. (6) Правила действий – действия, выполняемые при реализации определенного условия, которые обновляют профили, обнаруживают аномальное поведение, связывают аномалии с предполагаемыми вторжениями и создают отчеты. (7) Файловая система – организация распределенного хранилища данных для возможности параллельной обработки. В качестве таковой можно использовать HDFS (Hadoop Distributed File System) – распределенную файловую систему Hadoop для хранения файлов больших размеров с возможностью потокового доступа к информации, поблочно распределенной по узлам вычислительного кластера.

Рассматриваемая модель не зависит от какой-либо конкретной системы, среды, уязвимости системы или типа вторжения, тем самым обеспечивая основу для универсальной экспертной системы обнаружения вторжений.

Модель можно рассматривать как систему подбора сигнатур на основе заданных правил. Когда создается запись аудита, она сопоставляется с профилями. Вводится информация в соответствующие профили, а затем определяется, какие правила следует применять для обновления профилей, проверки аномального поведения и предупреждения об обнаруженных аномалиях. Оператор безопасности помогает в создании шаблонов профилей для деятельности, подлежащей мониторингу, но правила и структуры профилей в значительной степени независимы от системы.

Основная идея состоит в том, чтобы контролировать стандартные операции в целевой системе: входы в систему, выполнение команд и программ, доступ к файлам и устройствам и т. д., обнаруживая только отклонения в работе. Модель не содержит каких-либо специальных функций для решения сложных действий, которые используют известный или предполагаемый недостаток безопасности в целевой системе; более того, она не имеет никакого представления о механизмах безопасности целевой системы или ее недостатках. Хотя механизм обнаружения недостатков может иметь определенную ценность, он будет значительно более сложным и не сможет справиться с вторжениями, использующими недостатки, которые не идентифицированы, или с уязвимостями, связанными с персоналом. Однако, обнаружив вторжение, оператор безопасности сможет выявить уязвимые места.

Таким образом, предлагаемая модель обеспечивает основу для разработки системы обнаружения вторжений в реальном времени, способной обнаруживать широкий спектр вторжений, связанных с попытками взлома, маскарадом, проникновением в систему, троянскими конями, вирусами, утечкой и другими злоупотреблениями со стороны легитимных пользователей, а также некоторыми скрытыми каналами. Кроме того, модель позволяет обнаруживать вторжения, не зная об уязвимостях в целевой системе, которые позволили вторжению иметь место, без обязательного изучения конкретного действия, которое использует определенную уязвимость.

Работа выполнена при финансовой поддержке Гранта РНФ № 18-11-00302 в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Komashinsky N. Combining Spark and Snort Technologies for Detection of Network Attacks and Anomalies: Assessment of Performance for the Big Data Framework // 12th International Conference on Security of Information and Networks (SIN 2019). September 12th-15th, 2019 - Sochi, Russia. Proceedings by ACM International Conference Proceeding Series (ICPS). ACM, New York, NY, USA, 2019. Article No. 16. 8 p.
2. Desnitsky V., Rudavin N., Kotenko I. Modeling and Evaluation of Battery Depletion Attacks on Unmanned Aerial Vehicles in Crisis Management Systems // Intelligent Distributed Computing XIII. IDC 2019. Studies in Computational Intelligence, vol 868. Springer, Cham, 2020. p. 323-332.
3. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011, № 3, С.68-75.
4. Левшун Д.С., Чечулин А.А., Котенко И.В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 113–122. DOI:10.31854/1813-324X-2019-5-4-113-122 (ВАК, РИНЦ).

УДК 003.26

ПОСТКВАНТОВЫЕ ПРОТОКОЛЫ СЛЕПОЙ ЦИФРОВОЙ ПОДПИСИ

Костина Анна Александровна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: anna-kostina1805@mail.ru

Аннотация. Обсуждается проблема разработки постквантовых протоколов слепой подписи, лежащих в основе информационных технологий, применение связано с решением задачи обеспечения неотслеживаемости пользователей. В качестве перспективного подхода к разработке практичных протоколов данного типа отмечено использование скрытой задачи дискретного логарифмирования, задаваемой в конечных некоммутативных ассоциативных алгебр. Основными ожидаемыми преимуществами протоколов слепой подписи, основанных на данной вычислительно трудной задачи по сравнению с известными аналогами являются следующие: более высокая производительность, малый размер подписи и открытого ключа.

Ключевые слова: постквантовая криптография; цифровая подпись; слепая подпись; вычислительно трудная задача; конечная ассоциативная алгебра; некоммутативная алгебра.

OST-QUANTUM DIGITAL SIGNATURE PROTOCOLS

Kostina Anna
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: anna-kostina1805@mail.ru

Abstract. There is discussed the problem of developing post-quantum blind signature protocols, which are the basis of information technologies connected with solving the problem of providing untraceability of users. As a promising approach to the development of practical protocols of this type, the use of a hidden discrete logarithm problem set in finite non-commutative associative algebras is noted. The main expected advantages of blind signature protocols based on this computationally difficult problem compared to known analogues are the following: higher performance, smaller size of the signature and public key.

Keywords: post-quantum cryptography; digital signature; blind signature; computationally difficult problem; finite associative algebra; non-commutative algebra.

Протоколы слепой электронной цифровой подписи (ЭЦП) предложены для решения задач обеспечения неотслеживаемости (анонимности) пользователей в ряде специальных приложений информационных технологий, например, в системах электронных денег и тайного голосования через Интернет. Слепая ЭЦП генерируется подписантом в ходе протокола по своему личному секретному ключу и передает ее клиенту. Последний вычисляет по слепой подписи подлинную подпись подписанта к некоторому документу, к которому подписант не имеет доступа в процессе осуществления протокола слепой подписи. В настоящее наиболее интересными для практическог применения являются протоколы, основанные на вычислительной трудности задачи факторизации и задачи дискретного логарифмирования. В обоих случаях анонимность клиента реализуется за счет того, что в процессе выполнения протокола клиент вносит в слепую подпись один или два случайных ослепляющих множителя в параметры, по которым вычисляется подпись. Затем после получения значения слепой подписи от подписанта клиент устраняет вклад ослепляющих множителей и получает значение подлинной ЭЦП.

Однако, как задача факторизации, так и задача дискретного логарифмирования могут быть решены за полиномиальное время на квантовом компьютере [1], поэтому в настоящее время актуальной является задача разработки постквантовых протоколов ЭЦП наряду с постквантовыми версиями двухключевых криптосхем других типов. Изучение различных подходов к построению постквантовых протоколов слепой ЭЦП показало, что наиболее интересными с практической точки зрения являются протоколы слепой ЭЦП, основанные на так называемой скрытой задаче дискретного логарифмирования (СЗДЛ). Использование СЗДЛ позволяет выполнить построение протокола слепой ЭЦП по аналогии с известными протоколами слепой ЭЦП, основанными на вычислительной трудности обычной задачи дискретного логарифмирования.

Однако при построении протоколов, основанных на СЗДЛ, в качестве алгебраического носителя используются конечные некоммутативные ассоциативные алгебры, в которых левосторонние и правосторонние умножения дают существенно различные результаты [2, 3]. Поэтому внесение ослепляющих множителей должно учитывать эту важную особенность. С учетом этого вносятся два типа ослепляющих множителя – левосторонний и правосторонний. Ряд описанных в литературе протоколов ЭЦП, основанных на СЗДЛ, при использовании ослепляющих множителей указанного типа позволяют реализовать преобразование процедуры генерации ЭЦП в протокол слепой подписи. При этом сохраняются преимущества исходного протокола ЭЦП, основанного на СЗДЛ, по сравнению с другими постквантовыми схемами ЭЦП, включая кандидаты на постквантовый стандарт ЭЦП, например, Falcon [https://falcon-sign.info/], Dilithium [https://pq-crystals.org/dilithium/index.shtml] и qTESLA [https://qtesla.org/].

Основными преимуществами протоколов слепой ЭЦП, основанных на СЗДЛ, по сравнению с другими известными постквантовыми протоколами слепой ЭЦП являются существенно более высокая производительность процедур формирования слепой подписи и проверки подлинности подписи, существенно меньший суммарный размер подписи и открытого ключа.

При разработке известных протоколов слепой ЭЦП, основанных на СЗДЛ, был использован критерий обеспечения стойкости к известным квантовым атакам. Разработка протоколов слепой подписи, отвечающих усиленному критерию постквантовой стойкости и ориентированных на обеспечение стойкости к расширенному классу потенциальных квантовых атак, остается открытой исследовательской проблемой.

СПИСОК ЛИТЕРАТУРЫ

1. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. Vol. 26. P. 1484-1509.
2. Молдовян Н.А., Абросимов И.К. Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23–32.
3. Moldovyan D.N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. V.27, No.1(79). P. 56-72.

УДК 003.26

СХЕМЫ ЭЦП НА ОСНОВЕ СКРЫТОЙ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ И УСИЛЕННЫЙ КРИПТЕРИЙ ПОСТКВАНТОВОЙ СТОЙКОСТИ

Костина Анна Александровна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: anna-kostina1805@mail.ru

Аннотация. Рассмотрены новые формы задания скрытой задачи дискретного логарифмирования, позволяющие обеспечить выполнимость усиленного критерия постквантовой стойкости при разработке алгоритмов ЭЦП. Особенностью новых форм является использование коммутативной группы с двухмерной цикличностью в качестве скрытой группы. Рассмотрен вопрос выбора алгебраических носителей схем ЭЦП, содержащих достаточно большое число коммутативных групп с двухмерной цикличностью. Показано, что матрицы размерности 2x2, заданные над полем $GF(p)$, являются примером таких носителей.

Ключевые слова: постквантовая криптография; криптографический примитив; цифровая подпись; вычислительно трудная задача; конечные некоммутативные алгебры; ассоциативные алгебры.

SIGNATURE SCHEMES BASED ON THE HIDDEN DISCRETE LOGARITHM PROBLEM AND ENHANCED CRITERION OF POST-QUANTUM RESISTANCE

Kostina Anna
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: anna-kostina1805@mail.ru

Abstract. New forms of defining the hidden discrete logarithm problem are considered, which allow implementation of the enhanced criterion of post-quantum resistance. The novel forms are characterized in using a commutative group with two dimensional cyclicity as a hidden group. Selection of the algebraic supports containing sufficiently large number of the finite groups possessing two-dimensional cyclicity is considered. It is shown that the matrices of the dimension 2x2 defined over the field GF(p) represent examples of such algebraic supports.

Keywords: post-quantum cryptography; cryptographic primitive; digital signature; computationally difficult problem; finite non-commutative associative algebras.

Скрытая задача дискретного логарифмирования (СЗДЛ) является перспективным примитивом постквантовых двухключевых криптосхем: протоколов открытого согласования ключа [1]; электронной цифровой подписи (ЭЦП) [2], алгоритмов открытого и коммутативного шифрования [3]. Для задания СЗДЛ обычно используются маскирующие операции, обладающие свойством взаимной коммутативности с операцией возведения в степень. Последняя является базовой и вносит основной вклад в обеспечение стойкости

разрабатываемых на основе СЗДЛ криптосхем. В качестве алгебраического носителя СЗДЛ служат в конечные некоммутативные ассоциативные алгебры (КНАА) различных типов. Наиболее разнообразные формы СЗДЛ предложены для разработки постквантовых схем ЭЦП. Общим для всех форм является выработка открытого ключа в виде двух и более элементов КНАА, которые лежат в разных циклических группах, содержащихся в алгебре, но являются образами некоторых элементов КНАА, лежащими в другой циклической группе, называемой скрытой группой. Прообразы элементов открытого ключа связаны друг с другом, а именно, один из них выражается в виде степени другого прообраза. Эта связь проверяется в ходе выполнение процедуры проверки подлинности ЭЦП как выполнимость проверочного уравнения. В данной схеме построения схемы ЭЦП сохраняется возможность построении периодических функций на основе открытых параметров криптосхемы, причем таких, которые содержат период, зависящий от значения неизвестного логарифма, заданного в скрытой группе. Стойкость к квантовым атакам (атакам с использованием квантовых компьютеров) обеспечивается за счет того, что значения, принимаемые такой периодической функцией, рассеиваются примерно равномерно по достаточно многочисленным циклическим группам, содержащимся в алгебраическом носителе.

С целью предвосхищения новых потенциальных кантовых атак, основанных на предположительно возможных квантовых алгоритмах вычисления длин периодов периодических функций, принимающих значения в конечных алгебраических структурах более общего вида, чем циклические группы, например в конечных алгебрах, недавно было предложено использование коммутативных групп с двухмерной цикличностью в качестве скрытой группы и вычисление элементов открытого ключа как образов элементов, лежащих в разных циклических группах. Однако вопрос о выборе КНАА, подходящих для построения схем ЭЦП на основе этой идеи остался незавершенным. Кроме того, для предложенных частных случаев алгебр не было дано формального доказательства существования подмножеств элементов, образующих коммутативную группу с двухмерной цикличностью. В настоящем сообщении приводятся результаты, показывающие, что 4-мерные КНАА с глобальной двухсторонней единицей содержат достаточно большое число указанных коммутативных групп и могут быть использованы для построения криптосхем со скрытой группой в виде коммутативной группы с двухмерной цикличностью, удовлетворяющие требованию усиленнго критерия постквантовой стойкости – вычислительно невозможности построения на снове открытых параметров схемы ЭЦП периодических функций, свободных от периодов, длина которых зависит от значения дискретного логарифма. Для трех частных 4-мерных КНАА, заданных по прореженным таблицам умножения базисных векторов, дано формальное доказательство существования коммутативных групп с двухмерной цикличностью.

Значение полученных результатов состоит в том, что они показывают достаточность использования 4-мерных КНАА для реализации алгоритмов ЭЦП отвечающих усиленному критерию постквантовой стойкости, в том числе алгебр, в которых операция векторного умножения задается по прореженным таблицам умножения базисных векторов, и матриц размерности 2x2. Это дает возможность предложить постквантовые схемы ЭЦП, превосходящие в 3 и более раз по производительности, предложенные в рамках конкурса НИСТ кандидаты на постквантовый стандарт ЭЦП при существенно меньших размерах подписи и открытого ключа.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan D.N. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem // Computer Science Journal of Moldova. 2019. V.27, No.1(79). P. 56-72.
2. Молдовян Н.А., Абросимов И.К. Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23–32.
3. Moldovyan D.N. , Moldovyan N.A., Moldovyan A.A. Commutative encryption method based on hidden logarithm problem // Bulletin of the South Ural StateUniversity. Ser. Mathematical Modelling, Programming & ComputerSoftware // 2020. Vol. 13. No. 2. P. 54–68.

УДК 004.5

МЕТОДИКА ПРОЕКТИРОВАНИЯ КОМПЛЕКСА ВИЗУАЛИЗАЦИИ СЕТЕВОЙ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ДАННЫМИ ПОСРЕДСТВОМ СЕНСОРНЫХ ЭКРАНОВ

Котенко Игорь Витальевич, Бахтин Юрий Евгеньевич, Бушуев Сергей Николаевич, Комашинский Николай Александрович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ivkote@comsec.spb.ru, bakhtin@comsec.spb.ru, s.bushuev@telda.ru, nckkm@ya.ru

Аннотация. При решении различных задач компьютерной безопасности структура обрабатываемых данных может сильно различаться. По этой причине разрабатываются различные модели визуализации для визуального анализа инцидентов безопасности. Однако, несмотря на большие возможности современных интерфейсов, модели взаимодействия между оператором и системой всё ещё ограничены. В докладе будет рассмотрен подход к разработке человеко-компьютерного интерфейса на сенсорных экранах в зависимости от структуры данных.

Ключевые слова: пользовательский интерфейс, графический интерфейс пользователя, сенсорный интерфейс, человеко-компьютерное взаимодействие, компьютерная безопасность.

METHODOLOGY FOR DESIGNING A NETWORK SECURITY VISUALIZATION AND DATA MANAGEMENT COMPLEX BY MEANS OF TOUCH SCREENS

Kotenko Igor, Bakhtin Yuriy, Bushuyev Sergey, Komashinskiy Nikolay
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ivkote@comsec.spb.ru, bakhtin@comsec.spb.ru, s.bushuev@telda.ru, nckkm@ya.ru

Abstract. When solving various problems of computer security, the structure of the processed data can vary greatly. For this reason, various visualization models are being developed for the visual analysis of security incidents. However, despite the great possibilities of modern interfaces, the models of interaction between the operator and the system are still limited. The report will consider an approach to the development of a human-computer interface on touch screens, depending on the data structure.

Keywords: user interface, graphical user interface, touch interface, human-computer interaction, computer security.

Поскольку сетевой трафик обладает большими объёмами разнородных данных, для принятия решения оператором процессы в сети требуется визуализировать. Для повышения качества визуального анализа разрабатываются различные модели визуализации. Все эти модели содержат различные метрики, через которые можно передать данные информационной безопасности. Вид модели визуализации зависит от того, какие именно задачи информационной и компьютерной безопасности выполняются, и какую именно информацию нужно передать оператору [1].

Модели визуализации могут быть достаточно простыми и отображать несвязанные данные (такие как обычные линейные графики, гистограммы, круговые диаграммы). Также отображаемые данные могут быть связанными между собой или представлять собой иерархическую структуру (например, графы, деревья и т.п.). Кроме того, модели могут объединять в себе несколько других моделей для выполнения различных задач (sunburst включает в себя деревья и круговые диаграммы, упаковка шаров объединяет деревья и пузырьковую диаграмму, и т.п.).

Таким образом, для решения различных проблем безопасности должны выбираться различные модели визуализации. Выбор модели визуализации может зависеть от ряда параметров:

– структура данных: связанные или несвязанные данные, иерархические, планарные или неструктурированные и т.д.;

– задачи, которые стоят перед оператором: имеет ли визуализация исключительно демонстрационную функцию, предполагается ли дальнейший анализ инцидента безопасности.

– направление работы: данные антивирусного ПО или систем контроля доступа будут иметь разные модели.

Очевидно, что такое разнообразие моделей визуализации не может управляться одним и тем же способом. Для различных моделей визуализации требуется разрабатывать различные модели взаимодействия [2]. Поскольку технологии человеко-компьютерных интерфейсов стремительно развиваются, в том числе технологии, основанные на сенсорных экранах, они постепенно внедряются и в системы информационной и компьютерной безопасности. Это позволяет разрабатывать новые, более эффективные модели человеко-компьютерного взаимодействия с системами безопасности. Так, разрабатываются жестовые модели взаимодействия с визуализацией систем безопасности.

Для разработки более эффективных моделей взаимодействия следует подбирать наиболее удобные для данной конкретной визуализации и конкретной задачи жесты на сенсорных экранах. Например:

– сведение и разведение трёх пальцев для использования фильтра [3];

– пролистывание тремя пальцами влево-вправо для перехода к следующей модели визуализации;

– провести тремя пальцами вверх для того, чтобы отдалить от себя все окна приложения с возможностью выбора.

Так, предлагается разработка жестовых моделей взаимодействия в зависимости от типа визуализации (которая, в свою очередь, зависит от ряда параметров: тип данных, связанность данных и т.п.).

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01488).

СПИСОК ЛИТЕРАТУРЫ

1. Коломеец М.В., Чечулин А.А., Дойникова Е.В., Котенко И.В. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение, Т.61, № 10, 2018, С.873-880. DOI: 10.17586/0021-3454-2018-61-10-873-880.
2. Коломеец М. В., Чечулин А. А., Котенко И. В. Методы человеко-машинного взаимодействия для повышения эффективности принятия решений в процессах информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. Том 1. С. 479-483.
3. Котенко И.В., Коломеец М. В., Комашинский В. И., Бушуев С. Н., Гельфанд А. М. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. СПб.: СПОИСУ. 2018. С.143-144.

УДК 004.056

ОЦЕНКА КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ АППАРАТА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Крундышев Василий Михайлович, Калинин Максим Олегович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

Аннотация. В докладе рассмотрены методы искусственного интеллекта, которые пригодны для решения актуальной задачи оценки кибербезопасности современных динамических промышленных систем.

Ключевые слова: искусственный интеллект; кибербезопасность; машинное обучение; нейронные сети; нечеткая логика; промышленные системы.

ASSESSMENT OF THE CYBERSECURITY OF INDUSTRIAL FACILITIES USING THE APPARATUS OF ARTIFICIAL INTELLIGENT

Krundyshev Vasiliy, Kalinin Maxim
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

Abstract. The report discusses artificial intelligence methods that are suitable for solving the urgent problem of assessing the cybersecurity of modern dynamic industrial systems.

Keywords: artificial intelligence; cybersecurity; machine learning; neural networks; fuzzy logic; industrial systems.

Введение. При построении современных промышленных систем пристальное внимание необходимо уделить формированию и постоянному совершенствованию системы кибербезопасности, состоящей из комплекса технических и организационных защитных мер. Однако существует ряд проблем, которые препятствуют практической реализации оценки защищенности динамических промышленных систем:

– недостаточная формализация правил оценки кибербезопасности и, как следствие, необходимость постоянного привлечения экспертов;

– сложность детальной оценки защищенности в условиях ограниченной осведомленности сетевых узлов о текущем уровне киберугроз;

– неопределенность правил использования статистических данных для оценки вероятности возникновения киберугроз.

Традиционные стратегии оценки кибербезопасности, разработанные для статических компьютерных сетей, не могут использоваться для формирования рационального набора защитных мер при построении и оценке неоднородных, реконфигурируемых промышленных систем. Методы оценки защищенности (метод Дельфи, мозговой штурм, SWIFT и т.д.), основанные на экспертных оценках и требующие активного участия человека, не могут быть применены в динамичных инфраструктурах. Методы, использующие анализ сценариев (анализ первопричины, анализ дерева неисправностей, анализ дерева событий и т.д.) и функциональный анализ (анализ уровней защиты, анализ скрытых дефектов, анализ видов и последствий отказов и т.д.), специфичны для промышленных областей и плохо адаптируемы для решения задач кибербезопасности [1]. Применению статистических методов (метод Монте-Карло, сети Байеса и т.д.) препятствует сложность сбора статистических данных для моделирования расчетов результирующих показателей в сетях с одноранговой архитектурой, а также зависимость точности решений от количества итераций [2]. Для решения перечисленных проблем предлагается использовать методы искусственного интеллекта, такие как машинное обучение, искусственные нейронные сети и нечеткую логику.

Способность работать с большими данными, высокая скорость классификации, обнаружение скрытых закономерностей и высокая точность - все эти преимущества машинного обучения особенно актуальны в рассматриваемой прикладной области в условиях большого количества устройств, взаимодействия и влияния устройств друг на друга. Количественный подход, используемый в методах машинного обучения, устанавливает точные значения вероятности угроз и возможных последствий, а также риска для каждого типа активов. Численные значения удобны для анализа и сравнения результатов.

Использование искусственных нейронных сетей (ИНС) целесообразно в тех случаях, когда формализация процесса принятия решений затруднена или даже невозможна [3]. Искусственные нейронные сети позволяют реализовать эффективную обработку интенсивно поступающих неструктурированных данных сверхвысокого объема и извлечение из них знаний.

Среди основных преимуществ ИНС можно выделить следующие: способность обучаться автоматически и в процессе работы, вероятность обнаружения неизвестных киберугроз и возможность распараллеливания работы.

Особенностью математического аппарата нечеткой логики является то, что он использует «нечеткие множества» с неполными, отсутствующими или вероятностными данными [4]. Нечеткая логика работает не

столько с понятиями, которые имеют четкие семантико-количественные границы, сколько с множеством вероятностных данных внутри границ. В логические связи при нечеткой логике вступают не конкретные величины, а области данных с возможной актуализацией любого значения в границах данной области.

Заключение. Указанные методы искусственного интеллекта позволяют обрабатывать большие объемы данных, динамически адаптировать свою конфигурацию под изменяющиеся условия задачи и строить отображения с высокой нелинейностью, и за счет этого учитывать такую особенность кибербезопасности в промышленных системах как большое количество устройств и их постоянное взаимодействие.

Исследование выполнено в рамках Государственного задания на проведение фундаментальных исследований (код темы 0784-2020-0026).

СПИСОК ЛИТЕРАТУРЫ

1. Valis D., Koucky M. Selected overview of risk assessment techniques // Problemy Eksploatacji. – 2009. – № 75 (4). –P. 19–32.
2. Platon V., Constantinescu A. Monte Carlo Method in Risk Analysis for Investment Projects // Procedia Economics and Finance. – 2014. – № 15. –P. 393–400.
3. Зегжда П.Д., Малышев Е.В., Павленко Е.Ю. Использование искусственной нейронной сети для определения автоматически управляемых аккаунтов в социальных сетях // Проблемы информационной безопасности. Компьютерные системы. – 2016. – №4. –С. 9 – 15.
4. Овасапян Т.Д. Применение аппарата нечеткой логики для противодействия атакам внутренних нарушителей в WSN-сетях // Проблемы информационной безопасности. Компьютерные системы. – 2019. – №2. –С. 65 – 72.

УДК 004.05

ЗАЩИТА ПРОМЫШЛЕННЫХ СИСТЕМ ОТ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ АДАПТИВНОГО ПРОГНОЗИРОВАНИЯ И САМОРЕГУЛЯЦИИ

Лаврова Дарья Сергеевна
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mail: lavrova@ibks.spbstu.ru

Аннотация. Предложены методы прогнозирования аномалий в работе промышленных систем и саморегуляции их сетевой инфраструктуры для сохранения целевой функции в условиях реализации компьютерных атак.

Ключевые слова: обнаружение аномалий; адаптивное прогнозирование; саморегуляция; граф де Брёйна.

PROTECTING INDUSTRIAL SYSTEMS FROM COMPUTER ATTACKS BASED ON ADAPTIVE PREDICTION AND SELF-REGULATION

Lavrova Daria
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mail: lavrova@ibks.spbstu.ru

Abstract. Methods of prediction anomalies in the operation of industrial systems and self-regulation of their network infrastructure to preserve the target function in the implementation of computer attacks are proposed.

Keywords: anomaly detection; adaptive prediction; self-regulation; de Bruijn graph.

Современные промышленные системы (ПС) обладают спецификой с точки зрения обеспечения информационной безопасности: критичность нарушения безопасности таких систем связана с возможными катастрофическими последствиями из-за выхода физических процессов из-под контроля. В таких условиях необходимо обеспечивать предотвращение компьютерных атак на ПС, заключающееся в сочетании методов прогнозирования, обнаружения компьютерных атак и противодействия им [1, 2].

Предотвращение компьютерных атак на промышленные системы (ПС), позволяющее не допустить выхода необратимых физических процессов из-под контроля, затруднено ввиду роста числа новых типов компьютерных атак, ограниченного времени на противодействие атакам и отсутствия единой методологии, сочетающей раннее обнаружение атак и противодействие им.

Предлагаются методы прогнозирования состояния компонентов ПС и саморегуляции сетевой структуры ПС, в совокупности позволяющие обнаружить на ранней стадии нарушения в работе ПС, вызванные компьютерной атакой, и нейтрализовать их влияние на целевую функцию системы.

Метод адаптивного прогнозирования основан на анализе временных рядов, сформированных из значений, поступающих от компонентов ПС. Такое математическое представление позволяет универсализировать данные и следить за динамикой значений. Значения временных рядов могут отражать как реализацию компьютерной атаки на систему, так и различные физические процессы, которые не являются аномалией и проявляются в резком изменении нескольких значений во временном ряде (например, скачки напряжения в сети).

Для прогнозирования значений показателей временных рядов необходимо, чтобы прогнозная модель была способна адаптироваться к изменениям в данных, – тогда разовые изменения какого-либо параметра не

будут распознаны как компьютерная атака, и напротив, постепенное изменение значения показателя будет свидетельствовать о наличии нежелательной тенденции во временном ряде. Таким образом, для предотвращения компьютерных атак целесообразно использовать адаптивное прогнозирование, модель которого будет корректироваться с учетом вычисленной ошибки прогнозирования – разницы между предсказанным и реальным значениями [3].

Предложенный метод адаптивного прогнозирования базируется на сочетании рекурсивного алгоритма фильтра Калмана с алгоритмом машинного обучения Random Forest. Использование машинного обучения позволяет автоматически классифицировать спрогнозированные значения на нормальные и аномальные и, при необходимости, генерировать уведомление о возможной компьютерной атаке.

Сложность применения фильтра Калмана для ПС заключается в том, что для построения необходимых матриц и векторов требуется информация о физической модели ПС, которая не всегда доступна. Для решения этой проблемы показания каждого компонента ПС представлены как хаотичная траектория движения некоторого тела в одномерном пространстве. Тело характеризуется координатой Y, переменной скоростью движения V и ускорением a.

Экспериментальные исследования метода продемонстрировали высокую точность верного распознавания компьютерных атак на ранней стадии: значения метрик оценки качества классификации находились в пределах 0,93–0,98, время обучения занимало 1–6 секунд, время расчета прогноза на одно наблюдение вперед составило около 0,0001 секунды. К преимуществам метода также относятся низкие требования к объему предоставляемых данных и вычислительных ресурсов.

Нейтрализация деструктивного влияния компьютерных атак на целевую функцию ПС достигается за счет автоматической саморегуляции сетевой структуры ПС. Саморегуляция возможна за счет избыточности состава компонентов ПС, а также за счет возможности перераспределения функций между различными компонентами системы.

Последствия компьютерной атаки в терминах графовой модели представлены в виде «разрывов» в функциональной последовательности целевой функции ПС. Такое представление целевой функции позволило провести аналогию между ее восстановлением и биоинформатической задачей сборки генома. Разработанный метод саморегуляции реализует перенос и адаптацию принципов сборки генома на ПС с использованием математического аппарата графов де Брёйна и графов перекрытий, обеспечивая повышение скорости саморегуляции [4].

При нарушении одной функции, входящей в целевую, или нескольких невзаимосвязанных функций предлагается использовать заранее сформированные сценарии саморегуляции, представляемые в терминах графовой модели как унарные преобразования графа. В случае с нарушением нескольких взаимосвязанных функций потребуется перестроение одной или нескольких частей целевой функции, для повышения скорости соединения этих частей друг с другом целесообразно использовать графы де Брёйна или графы перекрытий.

Важным аспектом при описании и реализации метода саморегуляции является тип сетевой инфраструктуры ПС. Именно посредством внесения изменений в сетевую инфраструктуру и будет выполняться предотвращение компьютерных атак, реализуемых на ПС. О

днако алгоритмы саморегуляции будут существенно отличаться в случае централизованной и децентрализованной сетевой инфраструктуры.

Если компьютерная атака затрагивает одно из конечных устройств (датчик), управляемый промышленным контроллером, тогда решение о том, каким образом будет выполнена саморегуляция (например, какой датчик активировать вместо подвергнувшегося атаке), будет принято централизованно – контроллером. Если деструктивному воздействию подвергается один из управляющих контроллеров, то его задачи должны быть распределены между собой аналогичными ему узлами. В таком случае решение о саморегуляции должно приниматься децентрализованно.

Таким образом, перечисленные методы могут быть эффективно использованы для обеспечения информационной безопасности сложной сетевой инфраструктуры современных промышленных систем, отличающихся высокой степенью автоматизации и наличием большого числа интеллектуальных устройств.

Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1932.2019.5.

СПИСОК ЛИТЕРАТУРЫ

1. Sadiku, N. Cyber-physical systems: a literature review / N. Sadiku, Y. Wang, S. Cui, M. Musa // European Scientific Journal, 2017, Vol. 13, № 36, P. 52-58.
2. Зегжда Д. П., Павленко Е. Ю. Показатели безопасности Цифрового Производства. Проблемы информационной безопасности. Компьютерные системы, №2, 2018, с. 118-130.
3. Зокаев Т. Н. Методика адаптивного прогнозирования результатов деятельности предпринимательских структур Ставропольского края по производству минеральной воды / Т.Н. Зокаев, О.И. Шаталова // Terra Economicus, 2008, Т. 6, № 3-3, С. 329-331.
4. Сергушичев, А. А. Совместное применение графа де Брёйна, графа перекрытий и микросборки для de novo сборки генома / А. А. Сергушичев, А. В. Александров, С. В. Казаков, Ф. Н. Царев, А. А. Шалыто // Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика, 2013, Т. 13, № 2-2, С. 51-57.

УДК 004.056

ТРЕБОВАНИЯ К МЕТОДИКЕ ПРОЕКТИРОВАНИЯ И ВЕРИФИКАЦИИ ЗАЩИЩЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Левшун Дмитрий Сергеевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: levshun@comsec.spb.ru

Аннотация. В данной работе рассмотрены современные подходы к проектированию и верификации защищенных киберфизических системы. Сформулированы ключевые недостатки данных решений. Сформулированы требования к единой методике проектирования и верификации. Предполагается, что построение методики в соответствии с данными требованиями избежать ошибок проектирования, тем самым значительно снизив количество уязвимостей в разрабатываемых системах. В свою очередь, это позволит снизить риски, связанные с финансовыми потерями, потерями времени, а также безопасностью людей, что и обеспечивает актуальность и высокую значимость данного исследования.

Ключевые слова: безопасность в соответствии с проектом, киберфизическая система, проектирование безопасности, верификация безопасности, моделирование систем.

REQUIREMENTS TO THE METHODOLOGY FOR DESIGN AND VERIFICATION OF SECURE CYBER-PHYSICAL SYSTEMS

Levshun Dmitry
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: levshun@itmo.ru

Abstract. This work discusses modern approaches to the design and verification of secure cyber-physical systems. Key disadvantages of these solutions are formulated. Requirements for a unified design and verification methodology are formulated. It is assumed that the implementation of a methodology in accordance with these requirements will allow one to avoid design errors, thereby significantly reducing the number of vulnerabilities in the developed systems. This will reduce the security risks that can lead to financial losses, loss of time as well as the safety of people, and that is ensures the relevance and high significance of this investigation.

Keywords: security by design, cyber-physical system, security design, security verification, system modeling**.**

Киберфизические системы теперь – это неотъемлемая часть любой сферы нашей жизнедеятельности: от электроэнергетики, производства и транспорта, до медицины, торговли и личного использования. Данный факт обуславливает критическую важность обеспечения их защищенности, а также высокий ущерб от эксплуатации уязвимостей в них. Наличие уязвимостей в киберфизических системах обусловлено различными факторами: ошибками реализации используемых устройств, аппаратного и программного обеспечения, применением данных систем в несвойственной им окружающей среде, отсутствием или несовершенством стандартов, ошибками проектирования.

Уязвимости, внесенные из-за ошибок на этапе проектирования, являются наиболее опасными, т.к. после завершения разработки киберфизической системы, их устранение может представлять собой трудно решаемую задачу. Особенно когда устранение ошибки подразумевает изменения в аппаратной составляющей отдельных устройств или обновление программного обеспечения устройств, фирм-производителей которых уже не существует. Распространенность таких уязвимостей связана с тем, что зачастую, киберфизические системы проектируются без участия специалистов в области безопасности с применением слабозащищенных или незащищенных протоколов передачи данных, выходом в сеть Интернет и использованием непроверенного на наличие ошибок кода. Решение данной проблемы является важной задачей, именно поэтому были разработаны и применяются на практике различные методики проектирования. Данные методики могут быть направлены на аппаратные и программные элементы [1, 2], протоколы и интерфейсы [3, 4], программно-аппаратные элементы [5, 6], сеть передачи данных [7, 8] и киберфизическую систему в целом [9, 10].

Ключевой недостаток подобных решений заключается в том, что они сфокусированы на обеспечении только отдельных аспектов безопасности, а не безопасности системы в целом. К примеру, подходы, направленные на разработку безопасного программного обеспечения, не учитывают, что функциональность отдельных компонентов киберфизических системы определяется не только программной, но и аппаратной составляющей. Это особенно актуально для устройств на основе микроконтроллеров, для которых характерна сильная связь между аппаратным и программным обеспечением. Данная особенность имеет сильное влияние на процесс их проектирования, верификации и разработки.

Важным недостатком подходов, направленных на программно-аппаратные элементы, является тот факт, что безопасность проектируемых устройства рассматривается отдельно от системы, в которой им предстоит работать. Это означает, что не все аспекты безопасности будут приняты во внимание, а, значит,

безопасность системы в целом не будет обеспечена. При этом существуют подходы, рассматривающие не только отдельные устройства, но и обеспечивающие защищенное взаимодействие между ними. Недостатком подобных решений является тот факт, что безопасность сети передачи данных рассматривается только со стороны устройств, что может стать проблемой при проектировании сложных многоуровневых систем.

В рамках подходов, направленных на среду передачи данных, наибольшее распространение получили решения, применимые только в рамках определенной платформы и архитектуры. Подобные решения направлены на адаптацию широко используемых безопасных протоколов сети Интернет и их использования при взаимодействии устройств на основе микроконтроллеров. Необходимость адаптации связана с ограниченностью вычислительных ресурсов подобных устройств, максимальным размером полезной нагрузки, возможным к передаче в канале, а также возможности хранения только небольших объемов данных.

При этом объединение отдельных решений в рамках единого подхода представляет собой сложную задачу ввиду их несовместимости. Это связано с тем, что каждый подход используем свою собственную модель системы, представленную во внутреннем формате. Именно поэтому преобразование одной модели в другую практически невозможно без потери значимых данных. С другой стороны, существует ряд экосистем для индустриального интернета вещей, которые частично решают проблему проектирования, верификации и разработки защищенных киберфизических систем. Однако область их применения ограничена. Данные решения ориентированы на конкретное оборудование, программное обеспечение и платформы. При этом обеспечивается безопасность только на уровне шлюза и его соединения с облачными сервисами. Данные экосистемы решения не рассматривают оптимизацию предлагаемых решений на основе вычислительной мощности, потребляемой энергии и стоимости. Это означает, что предлагаемые решения могут не быть рациональными с точки зрения компромисса между безопасностью и доступными ресурсами.

Проведенный анализ показывает, что на данный момент не существует единого подхода для проектирования, верификации и разработки защищенных киберфизических систем. Требования к подобному подходу могут быть сформулированы следующим образом:

1. Новый подход должен быть основан на уже существующих решениях, их адаптации и доработке.
2. В основе нового подхода должен лежать компромисс между доступными ресурсами и обеспечением безопасности системы.
3. В основе нового подхода должна лежать интегрированная модель защищенной киберфизической системы, а также модели ее элементов, представляющие проекции данной модели.
4. Интегрированная модель должна предоставлять возможность как прямого (от проекций к модели), так и обратного (от модели к проекциям) преобразования.
5. Процесс верификации должен быть неотъемлемой частью нового решения, обеспечивая формальную проверку потенциальной возможности создания киберфизической системы, а также ее защищенности системы от злоумышленника.

Предполагается, что построение методики в соответствии с данными требованиями избежать ошибок проектирования, тем самым значительно снизив количество уязвимостей в разрабатываемых системах. В свою очередь, это позволит снизить риски, связанные с финансовыми потерями, потерями времени, а также безопасностью людей, что и обеспечивает актуальность и высокую значимость данного исследования.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90082.

СПИСОК ЛИТЕРАТУРЫ

1. Faily S. Further Applications of CAIRIS for Usable and Secure Software Design //Designing Usable and Secure Software with IRIS and CAIRIS. Springer, Cham, 2018. P. 239-254.
2. Kobashi T., Washizaki H., Yoshioka N., Kaiya H., Okubo T. and Fukazawa Y. Designing Secure Software by Testing Application of Security Patterns. Exploring Security in Software Architecture and Design. IGI Global, 2019. P. 136-169.
3. Xu X., He B., Yang W., Zhou X. and Cai Y. Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers. IEEE Transactions on Information Forensics and Security. 2015. Vol. 11. No. 2. P. 373-387.
4. Wang B., Zhong S.M. and Dong X.C. On the novel chaotic secure communication scheme design. Communications in Nonlinear Science and Numerical Simulation. 2016. Vol. 39. P. 108-117.
5. Wang Z., Karpovsky M., Bu L. Design of reliable and secure devices realizing Shamir's secret sharing. IEEE Transactions on Computers. 2015. Vol. 65. No. 8. P. 2443-2455.
6. Desnitsky V., Levshun D., Chechulin A. and Kotenko I.V. Design Technique for Secure Embedded Devices: Application for Creation of Integrated Cyber-Physical Security System. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 2016. Vol. 7. No. 2. P. 60-80.
7. Saleem K., Derhab A., Al-Muhtadi J. and Shahzad, B. Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society. Computers in Human Behavior. 2015. Vol. 51. P. 977-985.
8. Huang J. and Huang C.T. Design and verification of secure mutual authentication protocols for mobile multihop relay WiMAX networks against rogue base/relay stations. Journal of Electrical and Computer Engineering. 2016. Vol. 2016. P. 1-12.
9. Penas O., Plateaux R., Patalano S. and Hammadi M. Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of manufacturing systems. Computers in Industry. 2017. Vol. 86. P. 52-69.
10. Lin Z., Yu S., Lü J., Cai S. and Chen G. Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system. IEEE Transactions on circuits and systems for video technology. 2014. Vol. 25. No. 7. P. 1203-1216.

УДК 70

ИНФОРМАЦИООНОЕ РЕГУЛИРОВАНИЕ МАССОВЫХ ИНЦИДЕНТОВ В КИТАЕ

Лю Янь
Педагогический университет Центрального Китая
Луаю ул., 152, Ухань, провинция Хубэй, 430079, КНР
e-mail: karenly_62@mail.ru

Аннотация. Доклад посвящен определению и характеристике информационно-пропагандистской политики в Китае, и описанию ее функционирования в медиа-освещении социальных конфликтов.

Ключевые слова: медиа-политика, массовые инциденты, медиа-образ, конфликт, Китай.

INFORMATION REGULATION OF MASS INCIDENTS IN CHINA

Liu Yan
Central China Normal University
152 Luoyu Road, Wuhan, Province Hubei, 430079, China
e-mail: karenly_62@mail.ru

Abstract. The report is dedicated to the definition and characterization of informational-advocacy policy in China, and a description of its functioning in media coverage of social conflicts.

Keywords: media policy, mass incidents, media image, conflict, China.

«Массовые инциденты» – официальный эвфемизм для обозначения протестных действий обездоленных социальных групп в Китае [1]. Государственная информационно-пропагандистская политика определяет «видимость» массовых инцидентов в медиа.

В рамках провозглашенного предыдущим правительством Ху Цзиньтао – Вэнь Цзябяо (2003-2012 гг.) курса на построение гармоничного общества и создания благожелательной администрации ослабление управления массовой информацией и примирительное стиль центрального руководства в отношении протестов дали СМИ больше возможности опубликовать материалы об острых социальных конфликтах и демонстрациях [2].

Тем не менее протесты все еще были темой на грани допущенных цензурой и на практике существовало немало ограничений для публикации подобных новостей. На региональном уровне реальные препятствия журналистам чинят местные власти в очагах выступлений.

Однако, взаимный антагонизм и недоверие между журналистами и властями на местах способствует продвижению медиа-образов в пользу протестующих. В рамках информационно-пропагандистской политики создана, и информационная система управления обостряющимися конфликтами, где ведущая роль отводится центральным СМИ. Они активизируют вмешательство центральных властей по каналам изданий для внутреннего пользования, выполняя функции надзора за местными властями.

СПИСОК ЛИТЕРАТУРЫ

1. O'Brien K., Li L. Rightful Resistance in Rural China. – N. Y.: Cambridge University Press, 2006. – 200 p
2. Чжэн Вэнь, Хуан Жунгуи, Куй Юн. 郑雯,黄荣贵,桂勇. 中国抗争行动的"文化框架"——基于拆迁抗争案例的类型学分析(2003–2012). 新闻与传播研究, 2015, 02: 5-26+126. Культурный фрейминг действий сопротивления в Китае: типологический анализ протестов против сноса дома (2003–2012гг.) // Журналистика и коммуникации. – 2015. – No 2. – С. 5–26+126.

УДК 004.056

АНАЛИЗ ЗАЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ АТАК ОТКАЗА В ОБСЛУЖИВАНИИ

Мелешко Алексей Викторович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: meleshko.a@iias.spb.su

Аннотация. В работе анализируются некоторые существующие научные работы по тематике защиты компьютерных сетей от атак типа отказ в обслуживании и выработки контрмер для реагирования на подобные атаки. Атаки отказа в обслуживании являются опасными, так как нацелены на снижение пропускной способности коммуникационных каналов сервера, что в свою очередь может привести к нарушению доступности предоставляемых им сервисов. Поэтому важно заблаговременно выявлять такие атаки и им противодействовать. В качестве основного результата настоящей работы были выявлены и проанализированы некоторые виды контрмер, которые целесообразно применять против атак отказа в обслуживании в компьютерных сетях, а также возможные подходы оценки их эффективности.

Ключевые слова: компьютерные сети, атака отказ в обслуживании, информационная безопасность.

ANALYSIS OF SECURITY OF COMPUTER NETWORKS FROM ATTACKS OF FAILURE TO SERVICE

Meleshko Aleksei
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The paper analyzes some existing scientific works on the topic of protecting computer networks from denial of service attacks and developing countermeasures to respond to such attacks. Denial of service attacks are dangerous because they are aimed at reducing the throughput of the server's communication channels, which in turn can lead to a violation of the availability of the services it provides. Therefore, it is important to identify such attacks in advance and counteract them. As the main result of this work, we identified and analyzed some types of countermeasures that should be used against denial of service attacks in computer networks, as well as possible approaches to assess their effectiveness.

Keywords: computer networks, denial of service attack, information security.

В настоящее время существует множество видов атак на компьютерные сети. Среди них можно выделить отдельный вид атак – это атаки отказа в обслуживании (DoS). Подобные атаки, исходя из названия, нацелены на снижение пропускной способности сети жертвы или сервера, что, в свою очередь, приводит к нарушению работы сети. Например, во время действия атаки пользователи не могут получить доступ к нужному сервису или же передать информацию друг другу. К таким атакам можно отнести TCP-Flood (SYN, ACK и другие), UDP-Flood, SMTP-Flood, DNS Bandwidth Amplification Attack (атака усиления полосы пропускания DNS) и другие. Для того, чтобы минимизировать влияние атак на сеть, необходимо вовремя её обнаружить, а также адекватно реагировать на её появление. Для реагирования важно грамотно подобрать контрмеры для каждой из атак. Проанализируем некоторые работы по обнаружению подобных атак и выбору мер к их противодействию.

В статье [1] авторы приводят обзор работ по тематике контрмер против кибератак за несколько лет (2012-2016 годы). Исследование авторов направлено на анализ работ в этой области и на углубленное их изучение и сравнение по семи критериям. Также предлагается обсуждение перспектив и дальнейших исследований с области выработки контрмер против кибератак. Авторы дают определение понятию контрмеры как общий набор методологий, процедур и процессов, направленных на реагирование на нарушения безопасности в конкретной системе и их искоренение. Представленная авторами работа дает понятие о состоянии предметной области в течении многих лет, и рассматривает недостатки уже имеющихся подходов. Кроме того, приводится ряд критериев, на которые следует обратить внимание при дальнейших работах.

В статье [2] авторы описывают контрмеры, применяемые для минимизации атак распределенного отказа в обслуживании (DDoS) на основе кластера. По мнению авторов DDoS считается одной из основных угроз безопасности сегодня в Интернете. В контексте данной работы, DoS-атаки пытаются исчерпать пропускную способность жертвы или способность сервера. В DDoS атак, злоумышленник компрометирует большое количество хостов в Интернете и предписывает им проводить скоординированную атаку. Авторы анализируют и эксперимент с фильтрацией DDoS защиты, организованной на основе кластера. В фильтрации кластера используется неконтролируемое обучение для создания профиля сетевого трафика. Затем профилированный трафик пропускается через фильтры различной мощности и фильтруется несанкционированный трафик, то есть получаем лучшую пропускную способность нормального трафика, нежели вредоносного трафик.

Статья [3] посвящена описанию контрмер против атаки усиления полосы пропускания DNS. Это распределенная атака типа отказ в обслуживании, при которой сеть компьютеров загружает DNS-сервер ответами на запросы, которые никогда не были сделаны. Авторы в статье используют средство проверки вероятностной модели PRISM, чтобы моделировать и анализировать атаки DNS, а также три контрмеры: фильтрацию пакетов, случайные отбрасывания пакетов и агрессивные попытки получения легитимных пакетов. Фильтрация пытается идентифицировать источники атак и блокировать трафик, исходящий от них. Случайные отбрасывания пакетов регулируют входящий трафик путем случайного отбрасывания пакетов UDP.

Оценивать контрмеры авторы [3] предлагают несколькими способами. Например, в качестве оценки можно использовать вычислительные затраты, которые отражаются в количестве вычислительных ресурсов (например, процессоров), необходимых для контрмеры. Также авторы утверждают, что возможно анализировать эффективность контрмер путем расчета вероятности атаки и используя метрики «затраты-выгоды».

В статье [4] авторы представляют свою платформу FlowIDS для обнаружения атак SMTP-Flood. Данная платформа опирается на метод дерева решений и методы глубокого обучения. Работает платформа на сетях, которые основаны на SDN (программно-определяемая сеть). Такая архитектура представляет абстракцию мониторинга и контроля сетевой безопасности в обеспечении централизованного органа управления для кластерных сетей. Это позволяет интегрировать различные параметры безопасности, такие как брандмауэр, система обнаружения вторжений, антивирусные и другие инструменты. Авторы в работе в качестве системы обнаружения вторжений авторы используют Suricata.

FlowIDS проверяет все неопознанные аномалии трафика. Сначала идет проверка трафика SMTP на основе существующих признаков для известной атаки потока трафика SMTP. FlowIDS опирается на классификацию дерева решений (DT), или на алгоритм глубокого обучения (DL) для обнаружения потока SMTP. Авторы в работе тестировали FlowIDS с DT и DL в среде SDN. Для этого проводилось моделирование сети. Представленные

авторами [4] результаты показали, алгоритм DL обеспечивает лучшую пропускную способность сети по сравнению с алгоритмом DT.

Подводя итог проведенному анализу, можно сделать вывод, что универсального набора контрмер подобрать сложно, необходимо опираться на специфику определенной компьютерной сети. А в плане оценки подобранных контрмер существует несколько путей, оценка с помощью вероятностных характеристик появления атаки, оценка метриками «затраты-выгоды» или же оценка, которая использует такие параметры как вычислительные ресурсы. Обнаружение подобных атак может быть реализовано как с использованием различных систем обнаружения вторжений или же с использованием предложенного авторами [4] подхода, который опирается на архитектуру SDN и на алгоритмы машинного обучения.

Работа выполнена при финансовой поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (уникальный идентификатор RFMEFI60719X0322).

СПИСОК ЛИТЕРАТУРЫ

1. Nespoli P., Papamartzivanos D., Marmol F.G., Kambourakis G. Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks / IEEE Communications Surveys & Tutorials, 2017. P 1-37.
2. Bachani M., Memon A., Shaikh F.K. Sensors Network: In Regard with the Security Aspect and Counter Measures / Network Security Attacks and Countermeasures, 2016. P 176-196.
3. Deshpande T., Katsaros P., Basagiannis S., Smolka S.A. Formal analysis of the DNS bandwidth amplification attack and its countermeasures using probabilistic model checking / IEEE 13th International Symposium on High-Assurance Systems Engineering. IEEE, 2011. P 360-367.
4. Aziz M. Z. A., Okamura K. Leveraging SDN for detection and mitigation SMTP flood attack through deep learning analysis techniques / International Journal of Computer Science and Network Security, 2017. vol. 17. no. 10. P 166-172.

УДК 004.056

ПРОГРАММНАЯ МОДЕЛЬ ДЛЯ ГЕНЕРАЦИИ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ

Мелешко Алексей Викторович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: meleshko.a@iias.spb.su

Аннотация. В работе предлагается программная модель киберфизической системы управления водоснабжением, построенной на базе беспроводной сенсорной сети. Данная модель необходима для исследования различных состояний системы, моделирования некоторых видов атакующих воздействий на нее, а также для построения эффективных моделей и средств обнаружения атак на стадии эксплуатации системы. Разработанная модель системы управления водоснабжением представляет собой уменьшенную в размере натурную модели дамбы. Аппаратная часть мели базируется на микроконтроллерах Arduino и соответствующей элементной базе, включающей управляемые электроприводные шаровые краны, датчики уровня и потока воды и др., тогда как программная часть модели разработана с использованием языка программирования Python. Результатом настоящей работы на текущей стадии исследований являются сгенерированные наборы данных, содержащие логи нормальной работы системы, а также логи системы, находящиеся под несколькими видами атак. Полученные наборы данных предназначены для дальнейшего анализа с использованием методов машинного обучения.

Ключевые слова: киберфизические системы, система управления водоснабжением, информационная безопасность.

SOFTWARE MODEL FOR GENERATING WATER SUPPLY MANAGEMENT SYSTEM SECURITY INCIDENTS

Meleshko Aleksei
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The paper proposes a program model of a cyberphysical water management system based on a wireless sensor network. This model aimed at studying various states of the system, modeling some types of attacking influences on it, as well as for constructing effective models and means of detecting attacks at the stage of operation of the system. The developed model of the water supply management system is a smaller full-scale model of the dam. The hardware part of the chalk is based on Arduino microcontrollers and the due element base, including controlled electric ball valves, water level and flow sensors, etc., while the model software was developed using the Python programming language. The result of this work at the current stage of research is the generated data sets containing the logs of the normal operation of the system, as well as the logs of the system that are under several types of attacks. The obtained data sets are intended for further analysis using machine learning methods.

Keywords: cyberphysical systems, water supply management system, information security.

Безопасность киберфизических систем сейчас довольно актуальна, в частности для систем, которые носят критический характер. Различного рода атаки могут привести к непредсказуемым последствиям, как в плане работы самой системы, так и в плане безопасности окружающих её физических объектов. Поскольку киберфизические системы включают набор некоторого числа сенсоров и исполнительных устройств (актуаторов), то поиск вмешательства в работу системы возможно путем анализа данных, которые формируются системой.

С помощью набора логов нормальной работы системы, а также логов системы, находящейся под действием атаки можно, используя методы машинного обучения, научиться детектировать атаки по показаниям сенсоров. Это позволит оперативно выявлять атаки на систему и своевременно на них реагировать для предотвращения негативных последствий. Однако встает вопрос о наличии тех самых наборов данных для обучения в свободном доступе. Важно, чтобы наборы содержали как разное количество атак, так и нормальные состояния системы.

Статьи [1] и [2] описывают аппаратные прототипы для системы газопровода и водонапорной башни, а также собранные с них наборы данных. Однако, авторы [1] и [2] замечают, что собранные наборы некорректны потому, что они содержат некоторые шаблоны, которые заставляют алгоритмы машинного обучения легко детектировать атаки.

Поэтому целью данной работы является разработка программной модели киберфизической системы управления водоснабжением, с помощью которой можно будет за приемлемое время сгенерировать требуемые наборы данных содержащие нужные атаки. Под системой управления водоснабжением понимается натурная модель системы управления водоснабжением (дамбы). Описание реализации данной натурной модели в виде работающего программно-аппаратного прототипа киберфизической системы управления водоснабжением, приведено в статье [3].

Алгоритм работы натурной модели системы управления водоснабжением описан в статье [3]: есть два резервуара (верхний и нижний), вода перетекает из верхнего резервуара в нижний под действием силы тяжести, управляемый кран играет роль затвора дамбы, после наполнения второго резервуара закрывается кран и вода посредством насоса перекачивается в первый резервуар (вода по одну сторону дамбы уходит, а с другой стороны прибавляется). Сенсоры контролируют уровень воды в резервуарах, а также потоки воды. В каждом резервуаре три сенсора уровня воды и один сенсор, показывающий наполненность резервуара. Во втором резервуаре расположен управляемый насос и сенсор потока воды от насоса. Между резервуарами находится управляемый кран и сенсор потока воды между резервуарами.

Для возможности генерации большего количества состояний системы, а также различных атак был разработан программный эмулятор данной системы. С его помощью возможно получить набор данных, описывающих состояния системы, а также встроить в набор атакующие ситуации разных типов. Например, в случае необходимости генерации набора данных, содержащего несколько часов работы системы, необходимо запускать прототип на требуемое время и постоянно имитировать атаки, а в случае использования программного эмулятора данный процесс автоматизирован и занимает меньше времени. Эмулятор работает следующим образом: задается начальное состояние сенсоров и актуаторов системы, далее происходит имитация работы системы, а именно изменение показаний одних сенсоров с течением определенного времени, например пол секунды, и корректировка показаний других.

В определенный момент времени при генерации набора записей на несколько минут или секунд в них встраивается атака определённого класса и записывается в выходной файл. Конкретные значения времени, за которое опустошаются резервуары или меняются показания конкретных сенсоров были получены эмпирически, используя натурный прототип. Таким образом, можно задать любое начальное состояние системы и имитировать воздействия большого числа атаки и получить требуемый набор записей состояний системы с определенным промежутком времени за относительно небольшое время.

Набор данных представляет собой файл, формата *.csv, в котором содержатся записи состояний сенсоров и актуаторов прототипа в определенные моменты времени. Каждому моменту времени работы прототипа соответствует строка записей значений сенсоров, записанных через запятую или через символ, точка с запятой. Интервал времени между записями фиксирован и равен половине секунды.

В отличие от предыдущей версии набора данных, описанных в статье [3], настоящий набор содержит записи, включающие расширенный набор сенсоров и актуаторов прототипа, генерирующих данные по обновленной системе правил.

На данном этапе были реализованы пять классов атак. Все атакующие ситуации можно разделить на следующие пять классов: атака на двоичные сенсоры уровня воды; атака, направленная на искажение общего объема воды в резервуарах; два вида атак на сенсор потока воды между резервуарами и на сенсор потока воды от насоса; последний класс является смесью предыдущих атак, а именно заключается в подмене показателя потока воды между резервуарами, относительно от степени открытия управляемого крана. Можно выделить еще один класс – отсутствие атаки.

В итоге предложена программная модель киберфизической системы управления водоснабжением. Данная модель позволяет моделировать различные состояния системы в разные моменты времени, а также моделировать пять видов атакующих ситуаций. Суммарно было сгенерировано семь наборов данных, содержащих как записи нормального состояния системы, так и атакующих ситуаций. Поскольку имеется пять классов атак, то наборы данных делятся следующим образом: набор данных, содержащий только нормальные

состояния системы, пять наборов, в которых содержатся нормальные состояния совместно с атакующими ситуациями каждого класса, набор, содержащий все классы атак и нормальное состояние.

В дальнейшем сгенерированные наборы данных планируется подать на вход различным методам машинного обучения и обучить классификатор распознавать каждый класс атаки, что в свою очередь позволит своевременно их выявлять, анализируя данные в реальном времени с реального прототипа системы. После выявления атаки можно своевременно отреагировать на её появления и предотвратить негативные последствия или снизить величину причиненного ущерба.

Также можно использовать полученные наборы данных для тестирования других методов детектирования атак, например, основанных на статистике.

Работа выполнена в СПИИРАН при финансовой поддержке РФФИ (проект № 19-07-00953).

СПИСОК ЛИТЕРАТУРЫ

1. Morris, T. Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., Reddi, R. A. Control System Testbed to Validate Critical Infrastructure Protection Concepts / International Journal of Critical Infrastructure Protection, 2011. vol. 4. P 88-103.
2. Morris, T., Gao, W. Industrial Control System Network Traffic Data sets to Facilitate Intrusion Detection System Research / 8th IFIP WG 11.10 International Conference Critical Infrastructure Protection VIII (ICCIP 2014), 2014. P 65-78.
3. Meleshko A., Desnitsky V., Kotenko I. Machine learning based approach to detection of anomalous data from sensors in cyber-physical water supply systems / IOP Conference Series: Materials Science and Engineering, 2019. vol. 709. P 1-7.

УДК 003.26

ПОСТКВАНТОВЫЕ ВЕРСИИ КОММУТАТИВНОГО ШИФРА И ПРОТОКОЛА БЕСКЛЮЧЕВОГО ШИФРОВАНИЯ

Молдовян Александр Андреевич, Молдовян Дмитрий Николаевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: maa1305@yandex.ru, mdn.spectr@mail.ru

Аннотация. Обсуждаются проблема разработки постквантовых алгоритмов коммутативного шифрования и протоколов бесключевого шифрования на их основе. Представлены основные типы алгебраических носителей, используемых для построения постквантовых версий коммутативных шифров. Рассмотрены основные типы маскирующих операций, дополняющих базовую операцию экспоненцирования и являющихся взаимно коммутативными с последней. Отмечено существование недетерминированных коммутативных шифров, что показывает ограниченность общепринятого определения коммутативного шифра.

Ключевые слова: постквантовая криптосхема; коммутативный шифр; вычислительно трудная задача; дискретный логарифм; конечные некоммутативные алгебры; ассоциативные алгебры.

POST-QUANTUM VERSIONS OF THE COMMUTATIVE CIPHER AND NO-KEY ENCRYPTION PROTOCOL

Moldovyan Alexandr, Moldovyan Dmitriy
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: maa1305@yandex.ru, mdn.spectr@mail.ru

Abstract. There is discussed the problem of developing post-quantum commutative encryption algorithms and no-key encryption protocols based on them. The main types of algebraic carriers used for constructing post-quantum versions of commutative ciphers are presented. The main types of masking operations that complement the basic exponentiation operation and are mutually commutative with the latter are considered. The existence of non-deterministic commutative ciphers is noted, which shows the limitations of the generally accepted definition of a commutative cipher.

Keywords: post-quantum cryptoscheme; commutative cipher; computationally difficult problem; discrete logarithm; finite non-commutative algebras; associative algebras.

В настоящее время основное внимание в области разработки постквантовых криптографических алгоритмов и протоколов со стороны криптографического сообщества уделяется криптосхемам с открытым ключом. Сравнительно мало внимания уделяется проблеме разработке постквантовых коммутативных шифров. Несмотря на то, что их практические приложения не столь широки по сравнению с протоколами цифровой подписи и открытого распределения ключей, коммутативные шифры имеют уникальное применение в рамках протокола бесключевого шифрования для решения класса задач известных как «честная раздача карт». основным примитивом протоколов указанного типа является коммутативный шифр, стойкий к атакам на основе известного исходного текста.

Известные протоколы бесключевого шифрования основаны на вычислительной сложности задачи дискретного логарифмирования, для которой известны квантовые алгоритмы, имеющие полиномиальную временную сложность. В литературе известно весьма ограниченное число кандидатов на постквантовые коммутативные шифры, основанные на вычислительной сложности скрытой задачи дискретного логарифмирования (СЗДЛ) [1,2]. Данный примитив реализуется в достаточно разнообразных формах при построении постквантовых схем цифровой подписи, однако в

случае разработки постквантовых коммутативных шифров имеется возможность использования сравнительно ограниченного числа вариантов задания СЗДЛ [3].

Общая схема построения коммутативного шифра на основе СЗДЛ включает следующие элементы: 1) входное шифруемое сообщение встраивается в некоторый элемент конечной некоммутативной ассоциативной алгебры (КНАА), являющейся алгебраическим носителем алгоритма шифрования, 2) выполняется операция экспоненцирования, вносящая основной вклад в стойкость коммутативного алгоритма шифрования, 3) выполняется маскирующая операция, обладающая взаимной коммутативностью с базовой операцией экспоненциирования. При этом параметры маскирующей операцией являются элементами ключа шифрования и должны удовлетворять дополнительному требованию – взаимной коммутативности с маскирующими операциями, соответствующими другому независимому ключу шифрования. Последнее требование является ограничивающим фактором в выборе маскирующих операций, вид которых и определяет конкретную форму возникающей СЗДЛ, связанной с анализом стойкости разрабатываемого коммутативного шифра.

Разные формы СЗДЛ возникают при использовании в качестве алгебраического носителя коммутативных шифров КНАА различных типов, в частности некоммутативных алгебр с глобальной двухсторонней единицей и алгебр с большим множеством глобальных односторонних (правосторонних или левосторонних) единиц. При использовании алгебр первого типа имеются два варианта отображения входного сообщения элементом алгебры: 1) сообщение встраивается в обратимый элемент алгебры и в качестве маскирующей операции используется операция автоморфного отображения; 2) сообщение встраивается в необратимый элемент алгебры и в качестве маскирующей операции используются операция локального отображения, обладающие свойством взаимной коммутативности только в рамках подмножества необратимых элементов алгебраического носителя. В последнем случае возможны построения коммутативных шифров с «двойным» маскированием базовой операции экспоненцирования. При использовании в качестве алгебраического носителя КНАА с множеством глобальных односторонних единиц реализуются коммутативные алгоритмы шифрования вероятностного типа, что требует расширения общепринятого определения коммутативного алгоритма шифрования, как алгоритма генерирующего один и тот же шифртекст при выполнении шифрования на двух разных ключах, независимо от очередности их использования.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. Vol. 26. No. 3(78). P. 301-313.
2. Молдовян Н.А., Абросимов И.К. Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2019. Т. 15. № 2. С. 212-220.
3. Молдовян Н.А., Абросимов И.К., Ковалева И.В. Постквантовый протокол бесключевого шифрования // Вопросы защиты информации. 2017. № 3. С. 3-13.

УДК 003.26

КРИТЕРИИ РАЗРАБОТКИ ПОСТКВАНТОВЫХ ДВУХКЛЮЧЕВЫХ КРИПТОСХЕМ НА КОНЕЧНЫХ АССОЦИАТИВНЫХ АЛГЕБРАХ

Молдовян Александр Андреевич, Молдовян Дмитрий Николаевич, Молдовян Николай Андреевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: maa1305@yandex.ru, mdn.spectr@mail.ru, nmold@mail.ru

Аннотация. Обсуждаются критерии построения постквантовых криптосхем на основе скрытой задачи дискретного логарифмирования в конечных некоммутативные ассоциативных алгебрах, заданных над конечным полем $GF(p)$. Выделены два типа критериев: 1) ориентированные на обеспечение стойкости к квантовым атакам, использующим известные квантовые алгоритмы дискретного логарифмирования и 2) ориентированные на обеспечение стойкости к атакам на основе предположительно возможных новых квантовых алгоритмах вычисления длины периода периодической функции, принимающей значения, выходящие за рамки какой-то одной фиксированной циклической группы. Рассмотрены способы построения схем цифровой подписи, удовлетворяющих указанным критериям.

Ключевые слова: постквантовая криптосхема; открытый ключ; цифровая подпись; вычислительно трудная задача; дискретный логарифм; конечные некоммутативные алгебры; ассоциативные алгебры.

DESIGN CRITERIA OF THE DEVELOPMENT OF THE PUBLIC-KEY CRYPTOSCHEMES ON FINITE ASSOCIATIVE ALGEBRAS

Moldovyan Alexandr, Moldovyan Dmitriy, Moldovyan Nikolay
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: maa1305@yandex.ru, mdn.spectr@mail.ru, nmold@mail.ru

Abstract. Design criteria for development of the cryptoschemes based on the hidden discrete logarithm problem in finite non-commutative associative algebras defined over the finite field GF(p) are considered. The following two types of the criteria are highlighted: i) focused on ensuring the resistance to quantum attacks using the known quantum

algorithms for finding discrete logarithms and ii) focused on ensuring the resistance to quantum attacks using potentially possible quantum algorithms for finding the period length of a periodic function which takes on values that go beyond a single fixed cyclic group. Methods of developing digital signature schemes that meet the specified criteria are considered.

Keywords: post-quantum cryptoschemes; public key; digital signature; computationally difficult problem; discrete logarithm; finite non-commutative algebras; associative algebras.

Известные полиномиальные алгоритмы решения задачи дискретного логарифмирования (ЗДЛ) на квантовом компьютере [1] основаны на ее сведении к задаче нахождения длины периода периодической функции. По заданным параметрам ЗДЛ строится периодическая функция, содержащая период, зависящий от значения логарифма. Достаточно быстрое вычисление длины периода обеспечивается тем, что в случае функций, принимающих значения в конечной циклической группе, квантовый компьютер очень эффективно выполняет дискретное преобразование Фурье.

Прогнозируемое появление в достаточно близком будущем квантового компьютера, способного решать за полиномиальное время ЗДЛ и задачу факторизации, обусловило высокую степень актуальности проблемы разработки постквантовых двухключевых криптосхем, к которым относятся криптографические алгоритмы и протоколы с открытым ключом, являющиеся стойкими к квантовым атакам, т. е. к атакам с использованием вычислений на квантовом компьютере. Национальный институт стандартов и технологий США (НИСТ) в конце 2016 г. анонсировал программу по разработке к 2024 г. проекта на постквантовые стандарты открытого согласования ключей и электронной цифровой подписи (ЭЦП) и всемирный конкурс по разработке постквантовых криптосхем с открытым ключом. Из 69 предложенных кандидатов на постквантовые криптосхемы на участие во втором этапе конкурса были отобраны 17 схем открытого согласования ключа и 9 схем ЭЦП. Все эти криптосхемы основаны на вычислительно трудных задачах, отличных от ЗДЛ и задачи факторизации.

Главным недостатком предложенных кандидатов на постквантовые стандарты ЭЦП является большой суммарный размер открытого ключа и цифровой подписи, превышающий значение 2400 байт. Подход к разработке постквантовых схем ЭЦП, основанный на использовании вычислительной сложности скрытой задачи дискретного логарифмирования (СЗДЛ) [2, 3], оказался вне внимания участников конкурса, хотя в рамках этого подхода потенциально могут быть разработаны более практичные постквантовые криптосхемы.

Известные формы СЗДЛ формулируются в конечных некоммутативных ассоциативных алгебрах (КНАА), заданных над простым конечным полем GF(p). Расширение класса алгебраических носителей СЗДЛ и разработка новых ее форм представляет существенный интерес для разработки новых практичных постквантовых криптосхем. Важным моментов процесса разработки криптосхем является выбор критериев построения. В случае разработки постквантовых криптосхем на первый план выдвигаются критерий обеспечения постквантовой стойкости, т.е. стойкости к квантовым атакам. В критериях данного типа предполагается формулировка общего способа обеспечения постквантовой стойкости. Ряд известных схем ЭЦП, основанных на соответствуют следующему критерию: задание периодических функций на основе открытых параметров двухключевой криптосхемы должно приводить к тому, что значения каждой из этих функций являются достаточно равномерно рассеянными по достаточно большому числу различных циклических групп, содержащихся в алгебраическом носителе криптосхемы.

Этот критерий ориентирован на обеспечение стойкости к известным в настоящее время квантовым атакам. Однако возникает вопрос о потенциальной возможности появления в будущем квантовых алгоритмов нахождения длины периода для более широкого класса периодических функций. Возможность сохранения высокой стойкости схем ЭЦП при появлении таких квантовых алгоритмов потенциально может быть обеспечена вычислительной сложностью построения периодических функций с длиной периода, зависящей от значения дискретного логарифма.

Таким образом, усиленный критерий обеспечения стойкости к квантовым атакам может быть сформулирован следующим образом: криптосхема должна быть построена таким образом, что построение периодических функций на основе публичных параметров криптосхемы должно приводить к тому, что эти функции будут свободны от периода, зависящего от значения дискретного логарифма, хотя будут обладать периодами, длины которых задаются простым порядком скрытой циклической группы**.**

Для реализации криптосхем, отвечающих усиленному критерию, наиболее интересным общим подходом является использование коммутативных групп с двухмерной или многомерной цикличностью в качестве скрытой группы. Разработка криптосхем на основе этого общего подхода требует использования алгебраических носителей, содержащих достаточно большое число групп данного вида и новых форм задания СЗДЛ.

СПИСОК ЛИТЕРАТУРЫ

1. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. Vol. 26. P. 1484-1509.
2. Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science Journal of Moldova. 2018. Vol. 26. No. 3(78). P. 301-313.
3. Молдовян Н.А., Абросимов И.К. Схема постквантовой электронной цифровой подписи на основе усиленной формы скрытой задачи дискретного логарифмирования // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2019. Т. 15. № 2. С. 212-220.

УДК №004.056

ПРИМЕНЕНИЕ ЧЕСНОЧНОЙ МАРШРУТИЗАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОГО ВЗАИМОДЕЙСТВИЯ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

Москвин Дмитрий Андреевич, Дахнович Андрей Дмитриевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: moskvin@spbstu.ru, andrei_dahnovich@mail.ru

Аннотация. Рассматриваются особенности обеспечения кибербезопасности промышленного Интернета Вещей. На основе проведенного анализа выдвигаются требования киберустойчивости промышленного Интернета Вещей к сетевым угрозам, а также описывается подход к реализации киберустойчивости на основе механизма чесночной маршрутизации.

Ключевые слова: интернет вещей, цифровое производство, кибербезопасность, индустрия 4.0, киберфизические системы, чесночная маршрутизация.

USING GARLIC ROUTING FOR MAKING OF CYBER RESILIENT COMMUNICATION IN INDUSTRIAL INTERNET OF THINGS

Moskvin Dmitriy, Dakhnovich Andrey
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: moskvin@spbstu.ru, andrei_dahnovich@mail.ru

Abstract. The features of ensuring cybersecurity of the IIoT are considered. Based on the analysis, the requirements for the cyber resistance of the IIoT to network threats are put forward, and an approach to the implementation of cyber resistance based on the garlic routing mechanism is described.

Keywords: internet of things, digital manufacturing, cybersecurity, industry 4.0, cyber-physical systems.

Концепция цифрового производства (ЦП) («промышленный интернет вещей», Индустрия 4.0) активно внедряется в инфраструктуру современных компаний. При этом происходит цифровая трансформация технологической сети, что означает ее переход на стек технологий и сетей передачи данных, на которых до этого функционировал корпоративный сегмент сети предприятия, а также образование новых сегментов сети и появление стыков между ними. Например, хранение данных на стороне провайдера облачных услуг приводит к связям между объектами технологической сети и сетью провайдера.

В большинстве работающих на сегодняшний день систем ЦП производственные процессы и данные изолированы друг от друга по отдельным сегментам, что упрощает обеспечение их безопасности и уменьшает риски, связанные с компрометацией одного из компонентов или сегмента в целом. При переходе к ЦП происходит интеграция различных сегментом друг с другом, что позволяет злоумышленнику получить доступ ко всем процессам производства. Сети ЦП обладают несколькими свойствами, обеспечивающих их особенность при построении и сложности применения известных подходов к обеспечению безопасности:

1. Гетерогенность – разнородность инфраструктуры и протоколов взаимодействия.
2. Уникальность – невозможность применение универсального решения систем «из коробки», для каждого предприятия необходима индивидуальная настройка инфраструктуры.
3. Сегментированность – взаимодействие происходит между различными по архитектуре и функциям сегментами сети (корпоративной, технической и т.д.).
4. Связность – отсутствие строгой иерархии потоков данных от верхних к нижним уровням сети, так как появляются новые типы взаимодействий как между, так и внутри сегментов сети.

В связи с этим возникают новые угрозы информационной безопасности, связанные с недостатками аутентификации объектов и поступающих на них данных; некорректными правами доступа к объектам и между сегментами сети; воздействием на управляющие потоки информации. Для устранения данных угроз необходимо решить задачи кибербезопасности цифрового производства, сводящиеся к обеспечению:

- аутентификации данных, передаваемых между сегментами сети;
- контролю доступа к объектам;
- конфиденциальности передаваемых данных;
- устойчивости к атакам и способности самовосстановления работоспособности системы.

Для решения данных задач безопасности цифрового производства предлагается применить концепцию чесночной маршрутизации, позволяющую создавать безопасные каналы передачи данных, проводить аутентификацию полученных данных, а также передавать данные по нескольким маршрутам для обеспечения гарантии доставки.

СПИСОК ЛИТЕРАТУРЫ

1. Stouffer K., Pillitteri V., Lightman S. Guide to Industrial Control Systems (ICS) Security // NIST Special Publication 800-82 rev.2. 2015.
2. Васильев Ю.С., Зегжда П.Д., Зегжда Д.П. Обеспечение безопасности автоматизированных систем управления технологическими процессами на объектах гидроэнергетики // Известия Российской академии наук. Энергетика. 2016. № 3. С. 49-61
3. Voas J. Network of ‘Things’ // NIST Special Publication 800-183. 2016.

4. Степанова Т.В., Зегжда Д.П., Васильев Ю.С., Зегжда П.Д. Обеспечение технологической независимости РФ в области кибербезопасности // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 17-29.
5. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. №2. С. 2-15

УДК 004.056

АНАЛИЗ МЕТОДОВ ОЦЕНКИ САМОПОДОБИЯ СЕТЕВОГО ТРАФИКА СВЕРХВЫСОКИХ ОБЪЕМОВ

Муренин Иван Николаевич, Новикова Евгения Сергеевна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: imurenin@gmail.com, evgenia.novikova123@gmail.com

Аннотация. Работа представляет анализ подходов к поиску самоподобия в сетевом трафике сверхвысоких объемов. Представлены различные методы оценки показателя Херста, который широко используется в качестве меры долговременной памяти временных рядов. Показаны особенности использования обобщений модели авторегрессии скользящего среднего для обнаружения нелинейных зависимостей в сетевом трафике и поиска долгосрочной зависимости. Проведен сравнительный анализ методов обнаружения самоподобия сетевого трафика на основе подходов, представленных в литературе, сделаны обобщения и рекомендации по их дальнейшему использованию.

Ключевые слова: анализ сетевого трафика; самоподобие сетевого трафика; долгосрочная зависимость, параметр Херста.

ANALYSIS OF SELF-SIMILARITY ASSESSMENT TECHNIQUES FOR NETWORK TRAFFIC OF SUPER-HIGH VOLUMES

Murenin Ivan, Novikova Evgenia
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: imurenin@gmail.com, evgenia.novikova123@gmail.com

Abstract. The work presents an analysis of approaches to the self-similarity assessment of network traffic of super-high volumes. Various methods for estimating the Hurst exponent, which is widely used as a measure of long-term memory of time series, are presented. The main features of using generalized autoregressive models for detecting non-linear dependencies in network traffic and searching for long-term dependencies. A comparative analysis of the methods for detecting self-similar network traffic based on the approaches presented in the literature is proceed, explanations and recommendations for their further use are made.

Keywords: analysis of network traffic; self-similarity of network traffic; long range dependency, Hurst exponent.

Прогнозирование трафика является одной из основных задач анализа производительности сети. На основе полученных прогнозов может осуществляться оценка проектирования и планирования сети. Разработка эффективной и точной модели для прогнозирования сетевого трафика может снизить частоту перегрузки сети и улучшить качество связи. Краткосрочное или долгосрочное прогнозирование выгодно для управления сетью и корректировки ресурсов. Анализируя и прогнозируя исторические данные сетевого трафика и соответственно корректируя распределение сетевых ресурсов, операторы могут быть в курсе будущей ситуации в сети заранее. Это оказывает глубокое влияние на развитие ключевых технологий, таких как планирование архитектуры, распределение ресурсов и безопасность сети. Тем не менее, большинство моделей фокусируются на нелинейности данных трафика для повышения точности прогнозирования, но игнорируют важность самоподобия [1]. Самоподобие сетевого трафика требует оценки стохастическими методами и должно учитывается при его прогнозировании. Выполнение оценки самоподобия крайне важно при построении моделей выявления аномалий в сетевом трафика в режиме реального времени, поскольку изменение его характера обуславливает запуск переобучения моделей анализа, что позволяет строить гибкие адаптивные системы защиты информационных систем.

Самоподобие трафика означает, что его локальная структура частично соответствует общей структуре. Самоподобный процесс - это случайный процесс, который является статистически постоянным. Сетевой трафик имеет долгосрочную зависимость (long-range-dependancy) в отличие от процессов с краткосрочной зависимостью (short-range-dependancy), таких как процесс Пуассона. С физической точки зрения, долгосрочная зависимость является феноменом анализа самоподобия сетевого трафика, то есть устойчивость и неопределенность процесса самоподобия, также известные как многомасштабные поведенческие особенности, существуют на всех измерениях шкалы времени.

Наиболее общепринятые и широко используемые определения связаны с самоподобием первого и второго порядка. Самоподобие первого порядка основано на автокорреляции путей сетевого трафика. Поведение, характеризующее самоподобие, проявляется в том, что автокорреляционная функция не затухает

экспоненциально со временем, как в случае временных рядов с краткосрочной зависимостью, а скорее демонстрирует поведение степенного закона.

Самоподобие второго порядка определяется как воссоздание исходного временного ряда для различных временных «окон» *m*, где все значения, соответствующе времени в рамках одного окна длины *m* усредняются. Самоподобие второго порядка, также известное как агрегированный дисперсионный анализ, формально определяется как принятие нового временного ряда.

Для каждого определения самоподобия можно вывести показатель Херста H [1-4]. Параметр самоподобия (также называемый параметром Херста) является простейшей числовой характеристикой стохастического самоподобия и долгосрочной зависимости. Цель определения параметра Херста для случайных процессов состоит в том, чтобы проанализировать свойство самоподобия, которое ограничивает показатель значениями от 1/2 до 1 для самоподобной системы. Показатель H = 1/2 идентичен показателю случайного броуновского движения, а H = 1 отражает полное самоподобие. По оценкам, во многих исследованиях H составляет около 0,8 для большинства типов интернет-трафика. Авторы [5] предполагают, что параметр Херста очень эффективен для обнаружения повторяющихся шаблонов в сетевом трафике по сравнению с широко используемыми показателями, применяющимися для анализа временных рядов, такими как индекс дисперсии, отношение пика к среднему и коэффициенты вариации. Существует несколько групп методов для оценки параметра Херста. R/S метод и дисперсионно-временной анализ предложены в [1,4,6]. Метод R/S - нормализованная, безразмерная мера, предложенная самим Херстом для характеристики изменчивости данных. Дисперсионно-временной анализ основан на свойстве медленно уменьшать дисперсию самоподобного агрегатного процесса. Они оба являются статистическими методами и дают первичную оценку параметра H. Проблемы могут возникнуть с тем, что при расчете агрегированной дисперсии выбирается определенный диапазон *m* для размеров блоков, и выбор значений *m*, которые слишком малы, приводит к доминированию краткосрочных корреляций, в то время как больший *m* имеет меньше блоков и дает менее точную оценку H.

Метод периодограммы для оценки самоподобия трафика представлен в работах [1,6]. Он основан на оценке спектральной плотности случайного процесса на множестве дискретных временных интервалов. Оценка на основе периодограммы является более достоверной, чем оценка, основанная на агрегации, но при этом априори должна быть известна математическая параметризованная модель процесса. Основным недостатком этого метода является необходимость высокой вычислительной мощности

Оценка Уиттла [1,3] выводится из периодограммы и также рассчитывается на основе спектральной плотности. И периодограмма, и оценка Уиттла получены из оценки максимального правдоподобия (MLE) и предлагают хорошие статистические свойства, но могут давать ошибки, если модель спектральной плотности составлена неправильно.

В [7] описывается такие методы как броуновское движение (FBM) и фрактальный гауссов шум (FGN), основанные на оценке параметра автокорреляционной функции для соответствующих случайных процессов второго порядка. Авторы показывают, что они широко используются при оценке самоподобия сетевого трафика. При расчете параметра Херста оценки с помощью этих двух моделей могут быть получены относительно просто и будут иметь фундаментальные математические основания, но при этом они строго самоподобны и не могут хорошо анализировать трафик краткосрочной корреляционной структуры.

ON/OFF модель распределения тяжелых хвостов представлена в [3] В рамках этого подхода самоподобный процесс рассматривается как результат многочисленных наложений пользовательских данных. Модель определяется большим объемом источников данных. Каждый источник имеет два состояния: включенное и выключенное. Каждый источник данных независим, а длительность состояний соответствует распределению тяжелых хвостов. Когда источник данных находится во включенном состоянии, он генерирует данные с постоянной скоростью, но когда он находится в выключенном состоянии, он не производит никаких воздействий. Когда количество источников данных стремится к бесконечности, общий сетевой трафик имеет асимптотически самоподобный характер. Авторы [3] полагают, что существующие оценки не являются точными для отражения характеристик распределения тяжелых хвостов, поскольку они имеют идеализированные предположения, такие как стационарность и независимость.

DFA (Detrended fluctuation analysis) представляет собой модифицированную среднеквадратичную величину (RMS), которая рассчитывает отклонение от тренда и корреляцию на большие расстояния в нестационарных временных рядах. Полученная оценка аналогична показателю Херста, за исключением того, что DFA может также применяться к сигналам, базовая статистика (например, среднее значение и дисперсия) или динамика которых являются нестационарными (изменяющимися со временем). Авторы [4] считают, что оценки показателя Херста, использующих метод DFA, следует рассматривать со скептицизмом и проверять на соответствие другим методам.

Применение вейвлет-методов для анализа сетевого трафика на самоподобие представлено в работах [1,4]. Логарифмическая диаграмма создается с использованием дискретного вейвлет-анализа сигнала, где исходный сигнал представляется как отфильтрованный через вейвлет, определенный с учетом временной шкалы и определенного момента времени. Метод оценки самоподобия с использованием вейвлетов - это масштабирование функции разделения для каждого момента порядка q по каждой октаве. Часто предпочтительный метод анализа для нестационарных временных рядов.

ARIMA, сокращение от «Auto Regressive Integrated Moving Average» представляет собой класс моделей, которые «объясняют» данный временной ряд на основе своих собственных прошлых значений, то есть собственных лагов и лаговых ошибок прогноза, так что подобные модели можно использовать для прогнозирования будущих значений временного ряда. Любые «несезонные» временные ряды, которые демонстрируют закономерности и не являются случайным белым шумом, можно моделировать с помощью моделей ARIMA. Модель ARIMA характеризуется 3 членами: p, d, q, где, p - порядок члена AR, q - порядок члена MA, d - число разностей, необходимых для того, чтобы сделать временной ряд стационарным. FARIMA - это расширение традиционной модели авторегрессии скользящего среднего. В работах [1, 5, 7] представлены примеры использования данной модели для оценки самоподобия сетевого трафика. FARIMA (p, d, q) - прогрессивный самоподобный процесс второго порядка. Параметр Херста для данной модели можно найти как H=0.5+d, чтобы в дальнейшем с его помощью оценить степень самоподобия. Данная модель позволяет эффективно описать характеристики зависимости сетевого трафика в контексте долгосрочной зависимости.

В [1, 5] предлагается комбинированный ARIMA + GARCH [1, 5], использующий различные характеристики сети, такие как краткосрочная зависимость, долгосрочная зависимость и самоподобие. Используя возможности ARIMA в линейном трафике и модели GARCH для изменения дисперсии, авторы [8] разрабатывают одношаговую прогнозную модель, которая может быть расширена для создания многоканальных (или многошаговых) предсказаний. Этот метод демонстрирует лучшую производительность, чем FARIMA, с точки зрения отношения сигнал / ошибка (SER) в различных временных масштабах, а также экспериментальных прогнозов, кроме того, такая модель позволяет находить нелинейные зависимости во временных рядах.

Таким образом, представленные в литературе подходы позволяют оценить самоподобие сетевого трафика. Для трафика сверхвысоких объемов рекомендуется применять модели, имеющие не слишком высокую вычислительную сложность и позволяющие находить зависимости на больших расстояниях. Кроме того, такие модели не должны основываться на каких-либо предположениях о исходном распределении сетевого трафика, учитывая возможность обработки нестационарных временных рядов. Таким образом, для решения поставленной задачи наиболее подходящими можно считать вейвлет-анализ и модели на основе ARIMA. Также, возможно использование более простых методов, таких как R/S метод и дисперсионно-временной анализ, при условии выбора нескольких различных временных диапазонов для агрегации при получении похожих результатов для разных диапазонов.

Работа выполнена при финансовой поддержке Гранта Российского Фонда Фундаментальных Исследований (РФФИ) № № 19-07-00953 а.

СПИСОК ЛИТЕРАТУРЫ

1. Y. Xu, Q. Li, S. Meng. Self-similarity Analysis and Application of Network Traffic. MobiCASE 2019: Mobile Computing, Applications, and Servicesm, 112-125, 2019.
2. H. Jeong., W. Ahn, H. Kim, J. Lee. Anomalous Traffic Detection and Self-Similarity Analysis in the Environment of ATMSim, 10th IEEE International Conference, Innovative Mobile and Internet Services in Ubiquitous Computing, 2017. DOI: 10.3390/cryptography1030024
3. H. Larijani. Local Area Networks and Self-similar Traffic, Network Performance Engineering, 2011.
4. R. Smith. The Dynamics of Internet Traffic: Self-Similarity, Self-Organization, and Complex Phenomena, Advances in Complex Systems, 14, 6 p. 905-949, 2011. DOI: 10.1142/S0219525911003451
5. D. Ergenc, E. Onur. On Network Traffic Forecasting using Autoregressive Models, 2019.
6. R. Dobrescu, D. Hossu, R. Ulrich. Self-similarity Tests for Internet Traffic, Control Engineering and Applied Informatics 11(4), 11-17, 2009
7. X. An, L. Qu, H. Yan. A Study Based on Self-similar Network Traffic Model, Sixth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA), 2015. DOI: 10.1109/ISDEA.2015.28
8. B. Zhou, D. He, Z. Sun, W. Ng. Network traffic modeling and prediction with ARIMA/GARCH, 2008

УДК 004.056

ОПТИМИЗАЦИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С ПРИМЕНЕНИЕМ МЕТОДОВ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

Мясников Алексей Владимирович, Москвин Дмитрий Андреевич, Овасапян Тигран Джаникович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: myasnikov@ibks.spbstu.ru.com, moskvin@ibks.spbstu.ru, otd@ibks.spbstu.ru

Аннотация. Рассматриваются методы и средства машинного обучения, используемые для оптимизации процесса тестирования на проникновения

Ключевые слова: тестирование на проникновение; аудит безопасности; BAS-системы; машинное обучение, обучение с подкреплением.

PENETRATION TEST OPTIMIZATION METHODS USING REINFORCEMENT MACHINE LEARNING METHODS

Myasnikov Alexey, Moskvin Dmitriy, Ovasapyan Tigran
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: myasnikovalexey@gmail.com, moskvin@ibks.spbstu.ru, otd@ibks.spbstu.ru

Abstract. Methods and machine learning tools used to optimize the penetration testing process are considered.

Keywords: penetration testing; security audit; BAS systems; machine learning, reinforcement learning.

Тестирование на проникновение – метод практической оценки безопасности ИТ-инфраструктуры, применимый в среде цифрового производства. Процесс тестирования на проникновение связан с выполнением ряда технических задач: анализ ИТ-инфраструктуры, реализация сетевых атак, обнаружение уязвимостей в программном обеспечении ИТ-инфраструктуры, документирование результатов тестирования и подготовка рекомендаций.

Часть из этих этапов, а именно анализ и разведка, поддаются автоматизации, поскольку состоят из операций, выполнение которых возможно без непосредственного участия человека: сканирование портов, получение баннеров сервисов, построение карты внешнего периметра ИТ-инфраструктуры и карты локальной сети. Этапы, связанные с проведением атак, требуют непосредственного контроля специалиста. Возможны сценарии, когда специалист, проводящий тестирование на проникновение, использует все публично-доступные эксплоиты, однако, это недопустимо в корпоративных и производственных сетях, т.к. может привести к неконтролируемым последствиям, либо приведет к блокированию любых попыток эксплуатации из-за срабатывания средств защиты информации, установленных на испытуемом объекте. Таким образом, автоматизация процесса эксплуатации должна происходить с применением средств интеллектуального анализа, например, машинного обучения.

Прототип подобной системы может быть реализован, используя связку, состоящую из Metasploit Framework в качестве основного средства для эксплуатации и A3C (Asynchronous Advantage Actor-Critic) модели обучения от Keras и TensorFlow.

A3C является алгоритмом обучения с подкреплением. Функционирование происходит на основе нейронных сетей, которые обучаются на множестве уязвимых серверов. В качестве входных данных используется информация, полученная на этапе разведки (тип ОС, название ПО, версия, модуль эксплуатации, уязвимый хост). В зависимости от успешности или неудачи исполнения эксплоита обновляются показатели весов в нейронной сети.

Применение машинного обучения для задач тестирования на проникновение помогает повысить эффективность путем автоматизации процесса эксплуатации. Заведомо неверные варианты не проходят валидацию, таким образом снижается количество атак, что позволяет специалисту оставаться незаметным для средств защиты и не тратить время на заведомо неуспешные пути получения контроля над ИТ-инфраструктурой. Эффективность системы повышается с каждым применением из-за дообучения, кроме того, данный подход пригоден для использования в системах постоянного мониторинга безопасности сети.

В рамках доклада рассмотрены существующие системы, позволяющие проводить тестирование на проникновение с использованием машинного обучения. Рассмотрена их архитектура и применяемые методы машинного обучения. На основе проведенного анализа предложены решения по совершенствованию существующих систем.

Исследование выполнено в рамках Государственного задания на проведение фундаментальных исследований (код темы 0784-2020-0026).

СПИСОК ЛИТЕРАТУРЫ

1. Greenwald L., Shanley R. Automated Planning for remote penetration testing [Электронный ресурс]. URL: https://pdfs.semanticscholar.org/73d6/4e60473f5c788a965683c9e63796428993b8.pdf (Дата обращения: 01.07.2020)
2. Joseph A., Laskov P., Roli F., Nelson B. Machine Learning Methods for Computer Security // Dagstuhl Manifestos, Germany, 2013.
3. Seymour J., Tully P. Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter // Black Hat USA, 2016
4. Godefroid P., Peleg H., Singh R. Learn&Fuzz: machine learning for input fuzzing // Urbana-Champaign, IL, USA — October 30 - November 03, 2017

УДК 004.056.5

ОСОБЕННОСТИ ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ПРОГРАММНО-АППАРАТНЫХ КОМПОНЕНТОВ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Паращук Игорь Борисович, Десницкий Василий Алексеевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: desnitsky@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Рассматривается подход к анализу особенностей и формулировке содержания этапов оценивания защищенности программно-аппаратных компонентов беспроводных сенсорных сетей от компьютерных атак. Этапы содержат процедуры моделирования процессов функционирования беспроводных сенсорных сетей и поведения нарушителя, способного применять многошаговые атакующие воздействия, как физического, так и программно-информационного характера. Реализация этих этапов призвана повысить достоверность и оперативность оценивания защищенности сетей такого класса, их базовые механизмы построены на основе применения современных технологий больших данных и нейронных сетей.

Ключевые слова: беспроводная сенсорная сеть, защищенность, атака, данные, угроза, оценивание, моделирование, нарушитель, ресурс.

FEATURES OF SECURITY ASSESSMENT SOFTWARE AND HARDWARE COMPONENTS OF WIRELESS SENSOR NETWORKS

Parashchuk Igor, Desnitsky Vasily
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: desnitsky@comsec.spb.ru, shchuk@rambler.ru

Abstract. The approach to the analysis of features and the formulation of the content of the stages of assessing the security of software and hardware components of wireless sensor networks from computer attacks is considered. The stages contain procedures for modeling the processes of functioning of wireless sensor networks and the behavior of an intruder capable of applying multistep attack effects, both physical and software-informational. The implementation of these stages is designed to increase the reliability and efficiency of assessing the security of networks of this class, their basic mechanisms are based on the use of modern technologies of big data and neural networks.

Keywords: wireless sensor network, security, attack, data, threat, assessment, modeling, intruder, resource.

Введение. Беспроводные сенсорные сети (БСС) и проблемы их защищенности, безусловно, относятся к перечню приоритетных направлений развития науки и техники, как в Российской Федерации, так и в развитых зарубежных странах [1]. Повышение роли и стремительное распространение БСС, возрастание совокупной стоимости активов устройств, программного обеспечения и критически важных данных, циркулирующих в сетях такого класса, а также рост числа их уязвимостей и компьютерных атак объективно обусловливают актуальность исследования данной тематики. Вне всяких сомнений, все это подчеркивает насущную необходимость решения ряда теоретических и практических задач: задач анализа защищенности программно-аппаратного обеспечения БСС; контроля корректности предоставляемых ими сервисов с последующим принятием контрмер на основе результатов анализа защищенности, а также задач выработки рекомендаций по повышению защищенности сетей такого класса.

С точки зрения технологий, БСС находятся на стыке предметных областей сетей встроенных устройств и систем Интернета вещей [1]. Они объединяют распределенные множества встроенных устройств, сенсоров и представляют собой сравнительно новый вид информационно-телекоммуникационных инфраструктур. Сети такого класса включают разнообразные электронные устройства, физические объекты и пользователей с возникающими между ними коммуникационными соединениями и семантическими связями, потребностями в обработке, хранении, отображении и защите разнородной информации. Это самоорганизующиеся беспроводные системы специализированного назначения, включающие в свой состав различные встроенные устройства, программно-аппаратные сенсоры, исполнительные элементы, созданные на основе современных микросхем, в т.ч. на основе одноплатных компьютеров.

Особенности и наличие как традиционных, так и нетрадиционных угроз информационной безопасности БСС, обусловлены спецификой их построения и применения. Угрозы связаны с появлением новых классов программно-информационных и физических атакующих воздействий, осуществляемых на БСС, и требуют новых путей и механизмов защиты [2]. Методологической основой выбора и обоснования путей и механизмов защиты являются результаты оценивания защищенности программно-аппаратных компонентов БСС. Оценивание защищенности программно-аппаратных компонентов БСС – сложная, нетрадиционная задача, поскольку имеют место важные особенности таких систем. Сложность заключается в ограниченности аппаратных ресурсов БСС, задействованных программно-аппаратных модулей и их относительно низкой производительности по сравнению с другими видами вычислительных систем и телекоммуникационных сетей. Кроме того, существуют специфические возможности потенциального нарушителя в БСС, он способен совершать действия одновременно, как на физическом уровне, так и на программно-информационном. Важной особенностью является изменчивость программно-аппаратного окружения БСС и способов коммуникации между устройствами сети, а также наличие уникальных семантических связей между ее программно-аппаратными компонентами. Оценивание защищенности программно-аппаратных компонентов БСС может и должно быть организовано с использованием принципов обработки данных и событий информационной безопасности на основе технологии Больших Данных и нейронных сетей для выявления аномальных данных от сенсоров, на основе анализа возможных видов нарушителей в системах Интернета вещей, а также с учетом специфичных многошаговых атак на программно-информационном и аппаратно-физическом уровнях представления [3].

Механизмы оценивания защищенности программно-аппаратных компонентов БСС от компьютерных атак должны быть ориентированы на моделирование, анализ и практическую реализацию, на анализ защищенности сетей такого класса в условиях наличия разнородных и, взаимодействующих между собой, устройств, использующих беспроводные протоколы передачи данных, и с учетом повышенных требований к защищенности таких систем (сетей).

К основным этапам оценивания защищенности программно-аппаратных компонентов БСС можно отнести: этап моделирования БСС, специфицирующего физические и логические связи между узлами сети, их типы, роли, процессы динамической маршрутизации; этап моделирования поведения нарушителя в БСС; этап верификации атак на БСС с определением системы основных показателей для оценки таких воздействий; этап контроля БСС на предмет выполнимости условий осуществления атак нарушителем; этап распределенных сбора, обработки и анализа больших массивов данных от программных и аппаратных сенсоров БСС в режиме, близком к режиму реального времени, с использованием вычислительного кластера; этап выявления аномальных данных от сенсоров БСС на основе применения аппарата нейронных сетей с учетом классификации атак и их признаков; этап окончательного анализа

защищенности программно-аппаратных компонентов БСС беспроводных сенсорных сетей, а также этап выработки предложений по повышению защищенности БСС на основе полученных результатов.

Особого внимания, на наш взгляд, заслуживают первый и второй этапы – этапы моделирования БСС и поведения нарушителя. На первом этапе строятся динамические модели, отображающие физические и логические связи между узлами сети, определяются типов узлов сети и их роли в контексте свойств самоорганизации БСС и процессов маршрутизации в ней. Эти модели также отображают динамические характеристики и потоки данных в сети, позволяют создавать профили по настройке параметров узлов БСС, отправке, получению и распознаванию тестовых и сервисных команд в сети такого класса. Модели, предлагаемые к использованию на первом этапе оценивания защищенности программно-аппаратных компонентов БСС от компьютерных атак, строятся с учетом наличия обратных связей от моделей к объектам программно-аппаратной инфраструктуры сети. На втором этапе строится комбинированная модель нарушителя БСС с учетом возможных многошаговых атак и семантики внутрисетевого взаимодействия узлов сети. В рамках комбинированной модели нарушителя приведена классификация атак на беспроводные сенсорные сети, включающая несанкционированную модификацию конфигурационных настроек узлов сети, атаку перехвата данных в сети, атаку модификации данных, атаку внедрения ложного узла сети, DoS-атаку и атаку нарушения процесса маршрутизации в сети.

Особенностями и достоинствами предлагаемого подхода к формулировке и содержанию этапов оценивания защищенности программно-аппаратных компонентов БСС являются комбинирование и учет различных моделей нарушителя, осуществляющего многошаговые воздействия, как физического, так и программно-информационного характера, с использованием предлагаемой системы показателей нарушителя. Кроме того, моделирование компонентов БСС, различных видов нарушителей и атак реализуется с возможностью формирования обратных связей от моделируемых программно-аппаратных компонентов сети к киберфизическим модулям прототипа конкретной сети. Этапы оценивания защищенности программно-аппаратных компонентов БСС предполагают применение нейросетевого подхода к выявлению аномальных данных от сенсоров БСС с использованием признаков распознавания аномалий.

Заключение. Предложенный подход к построению и содержанию этапов оценивания защищенности программно-аппаратных компонентов БСС, по мнению авторов, позволит повысить достоверность и оперативность анализа защищенности сетей такого класса от компьютерных атак, что, в свою очередь, позволит улучшить качество принимаемых решений по управлению защитой их информационных ресурсов.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-00953) в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Ghildiyal S., Gupta A., Vaqur M., Semwal A. Analysis of wireless sensor networks: security, attacks and challenges // IJRET: International Journal of Research in Engineering and Technology. Volume 03. Issue 03. 2014. pp. 160-164.
2. Desnitsky V.A., Kotenko I.V. Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network // XX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg. 2017. pp. 500-502.
3. Десницкий В.А., Паращук И. Б. Показатели доступности, целостности и конфиденциальности данных пользователей беспроводных сенсорных сетей в интересах анализа и обеспечения их защищенности. // Информационная безопасность регионов России (ИБРР-2019): материалы XI Межрегиональной конференции, Санкт-Петербург, 23-25 октября 2019 г. СПб.: СПОИСУ, 2019. С. 114-116.

УДК 004.056.5

МОДЕЛЬ СИСТЕМЫ РОДИТЕЛЬСКОГО КОНТРОЛЯ ЦИФРОВОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ

Паращук Игорь Борисович, Десницкий Василий Алексеевич, Тушканова Ольга Николаевна
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: shchuk@rambler.ru, vasily.desnitsky@mail.ru, tushkanova.on@gmail.com

Аннотация. Предложен подход к определению базовых понятий родительского контроля, формулировке и систематизации уровней и взаимосвязанных задач такого контроля цифрового контента в сети Интернет. Совокупность этих понятий, уровней и задач, в сущности, является моделью (функциональной моделью) системы родительского контроля, поскольку отражает структуру, функциональные взаимосвязи и ограничения, реализуемые объектом такого класса в интересах защиты детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности. Рассмотрены роль и место этой модели в задачах оценки качества и эффективного управления мерами родительского контроля для защиты детей от информации, причиняющей вред их здоровью и развитию.

Ключевые слова: родительский контроль, модель, система, уровень, цифровой контент, функции, блокировка доступа, фильтрация, информация.

MODEL OF THE DIGITAL CONTENT PARENTAL CONTROL SYSTEM ON THE INTERNET

Parashchuk Igor, Desnitsky Vasily, Tushkanova Olga
St. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: shchuk@rambler.ru, vasily.desnitsky@mail.ru, tushkanova.on@gmail.com

Abstract. An approach is proposed to define the basic concepts of parental control, formulate and systematize the levels and interrelated tasks of such control of digital content on the Internet. The totality of these concepts, levels and tasks, in essence, is a model (functional model) of the parental control system, since it reflects the structure, functional relationships and restrictions implemented by an object of this class in the interests of protecting children from the destructive, traumatic impact of information on their psyche, as well as from information that can develop vicious tendencies in a child. The role and place of this model in the tasks of assessing the quality and effective management of parental control measures to protect children from information that harms their health and development are considered.

Keywords: parental control, model, system, level, digital content, functions, access blocking, filtering, information.

Введение. В последнее десятилетие все активнее внедряются программные, аппаратные и комплексные меры по фильтрации нежелательного цифрового контента, приложений и носителей, направленные на минимизацию вредоносного воздействия сети Интернет на ребенка. Эти меры принято называть родительским контролем [1]. Родительский контроль ставит целью повышение эффективности отслеживания действий ребенка в сети Интернет и призван решить ряд проблем: неспособность современного ребенка к самоуглублению, к концентрации на каком-либо занятии, отсутствие заинтересованности делом; снижение фантазии и творческой активности детей; повышение детской жестокости и агрессивности; дети не общаются со взрослыми, сверстниками; отрицательное влияние на физическое здоровье ребенка (даже на зрение ребенка), а также невозможность контролировать и защищать ребенка от вредной информации [2].

Вместе с тем, существует несколько наиболее распространенных определений понятия «родительский контроль», например. Родительский контроль (РК) – комплекс мер, предпринимаемых родителями (учителями, воспитателями) для ограничения детям времени работы за компьютером, доступа к определенной информации (сайтам) или запуску выбранных программ и игр [3]. Родительский контроль – комплекс правил и мер по предотвращению предполагаемого негативного воздействия сети Интернет и компьютера на опекаемого человека (обычно ребенка) [4]. Родительский контроль – это комплекс приложений и программ, которые помогают родителям защитить детей от вредного контента. Это инструменты для того, чтобы сделать работу в Интернете продуктивной, полезной и обезопасить ребенка от всего, что может ему навредить. К инструментам РК относятся компьютерное обеспечение, приложения для смартфонов, программы для телевидения, «умные» устройства и многое другое. Родительский контроль (parental control) – функция для семей с несовершеннолетними детьми, дающая возможность пользователю управлять просмотрами в Интернете, обеспечить безопасное и продуктивное общение ребенка с виртуальным миром.

Системы родительского контроля (СРК) – программно и технически реализованные наборы взаимоувязанных правил, мер, комплексов приложений и специальных программ, настроек браузера и/или штатных возможностей современных операционных систем, выполняющие базовые функции родительского контроля. Данные системы позволяют выполнять функции: по блокировке сайтов (как вариант, создание списка разрешенных сайтов), установка/снятие запретов на запуск приложений на компьютерах и смартфонах, а также времени взаимодействия с ними. Зачастую такие системы имеют также функции логирования действия ребенка: перемещение по Web-сайтам, какие приложения он запускал и во сколько, какие звонки и SMS отправлял, какую информацию искал в сети Интернет [3-5].

Функциональная модель СРК цифрового контента в сети Интернет включает взаимосвязанный набор (схему) реализуемых функций, к которым можно отнести [5]:

1. Ограничение времени, проводимого ребенком за компьютером. Можно определить время, в течение которого детям разрешен вход в систему. В частности, определить дни недели и разрешенные часы доступа в соответствующий день недели. Это не позволит детям входить в систему в течение определенного периода времени. Если в момент окончания разрешенного периода времени ребенок работает за компьютером, происходит автоматический выход из системы.

2. Установка запрета на доступ детей к отдельным играм. Запрет можно устанавливать исходя из допустимой возрастной оценки, выбора типа содержимого или запрещая доступ к определенным играм.

3. Ограничение активности детей в Интернете. Ограничить детей можно с помощью установки круга допустимых Web-узлов, исходя из возрастной оценки, запрета или разрешения загрузки файлов, определения условий фильтрации содержимого (т.е. мы должны определить, какое содержимое фильтры должны разрешать или блокировать). Можно разрешить или блокировать доступ к определенным Web-узлам.

4. Установка запретов на использование детьми отдельных программ. Можно запретить детям доступ к определенным программам.

5. Ведение отчетов о работе ребенка за компьютером.

6. Определение игр, доступных детям.

В рамках модели (функциональной модели) СРК цифрового контента в сети Интернет самыми распространенными являются два варианта ограничений:

создание «белых» и «черных» перечней Web-сайтов. «Черный» перечень должен регулярно обновляться, иначе появление новых ресурсов приведет к тому, что защита станет неактуальной. «Белый» перечень – вид более жесткого контроля – ребенок может просматривать только те Web-сайты, которые ему разрешили родители, нет необходимости обновлять перечень, актуальность со временем практически не теряется;

фильтрация сайтов по их содержимому. Пользователь задает набор ключевых слов, и если что-либо из их списка обнаруживается на Web-странице, то она не открывается.

Одним из базовых принципов работы функциональной модели СРК цифрового контента в сети Интернет является контентная фильтрация (КФ) – она обеспечивает поиск и выявление контента, содержащего нежелательную или опасную информацию, как правило, по списку «плохих» и «запрещенных» слов. Данная информация корректируется или ресурсы, содержащие такую информацию, блокируются. В подходе на основе КФ (как способа реализации функциональной модели СРК) есть ряд недостатков: необходима отдельная учетная запись для ребенка, иначе программу РК можно легко отключить; родители не всегда могут справиться с настройкой программ РК; обновление списков «плохих» и «запрещенных» слов всегда «запаздывает», КФ требует больших ресурсов компьютера или быстрого Интернет-соединения.

Таким образом, реализация модели (функциональной модели) СРК цифрового контента в сети Интернет подразумевает: настройку отдельной учетной записи; защиту паролем; контроль (времени использования компьютера; запускаемых программ; скачиваемых файлов; общения ребенка через мессенжеры и социальные сети; передачи личных данных; поиска в социальных сетях по видео); ограничение доступа к конкретным программам и конкретным сайтам.

Заключение. Предложенный подход к определению базовых понятий РК, формулировке и систематизации уровней и взаимосвязанных задач контроля цифрового контента в сети Интернет, является моделью (функциональной моделью) СРК, поскольку отражает структуру, функциональные взаимосвязи и ограничения, реализуемые системой такого класса в интересах защиты детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности. Эта модель, при ее использовании на практике, позволит улучшить достоверность и оперативность оценки качества РК, позволит повысить качество моделирования и качество принимаемых решений по эффективному управлению мерами такого контроля для защиты детей от информации, причиняющей вред их здоровью и развитию.

Работа выполнена при финансовой поддержке РНФ (проект РНФ 18-11-00302) в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный Закон «О защите детей от информации, причиняющей вред их здоровью и развитию» № 436-ФЗ (одобрен Советом Федерации 24 декабря 2010 г.).
2. Богатырева Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения // Известия ТулГУ. Гуманитарные науки. 2013. № 3-2, С. 14-26.
3. Зеленко А.П., Пьянкова В.В., Тетерина Е.В. Информационный мусор: проблема XXI века // Актуальные проблемы авиации и космонавтики. 2014. № 10. С. 240-241.
4. Макушкина Л.А. Разработка автоматизированной системы интернет тестирования школьников с целью родительского контроля посещаемости и успеваемости учеников// Макушкина Л.А., Лемякина Л.В. Вестник магистратуры. 2013. № 5 (20). С. 49-52.
5. Григорьян Н.В. Анализ существующих возможностей систем для осуществления родительского контроля / NovaInfo. № 61-2. 12.03.2017. [Электронный ресурс]. URL: https://novainfo.ru/article/11717 (дата обращения: 26.06.2020).

УДК 004.056

ПРИМЕНЕНИЕ СИСТЕМНОГО АНАЛИЗА К ОЦЕНКЕ ОБЪЕКТА ЗАЩИТЫ ПРИ МОНИТОРИНГЕ БЕЗОПАСНОСТИ КФС

Полтавцева Мария Анатольевна
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mail: poltavtseva@ibks.spbstu.ru

Аннотация. Рассматривается объект защиты при мониторинге безопасности в крупномасштабных промышленных системах с развитой сетевой инфраструктурой (киберфизических системах – КФС) с точки зрения системного анализа и современных требований к SOC (Security Operation Center).

Ключевые слова: информационная безопасность; кибербезопасность; моделирование; киберфизические системы; мониторинг безопасности.

APPLICATION OF SYSTEM ANALYSIS TO THE ASSESSMENT OF THE PROTECTION OBJECT IN THE CPS SECURITY MONITORING

Poltavtseva Maria
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mail: poltavtseva@ibks.spbstu.ru

Abstract. The object of protection when monitoring security in large-scale industrial systems with a developed network infrastructure (cyber physical systems-CFS) is considered from the point of view of system analysis and modern requirements for SOC (Security Operation Center).

Keywords: information security; cybersecurity; modeling; cyberphysical systems; security monitoring.

Современные системы мониторинга безопасности прошли большой путь от систем поиска нарушений на основе правил и сигнатур до интегральных комплексов центов управления безопасностью (SOC – Security Operation Senter) [1-2]. По мере эволюционного развития взрастала сложность такого рода систем, также, как и самих промышленных систем. Сегодня основными тенденциями являются: рост автоматизации и все большая необходимость автоматизации высокоуровневых функций анализа и управления безопасностью, интеграция систем безопасности, поддержка гетерогенной структуры объектов защиты. Особенно это актуально для промышленных киберфизических систем [3]. Их особенностями являются необратимость физического процесса, разнородность компонентов и протоколов, повышенные риски от атак злоумышленников и низкая степень защищенности, по сравнению с рядом других сегментов [4].

В области промышленных киберфизических систем тенденциями безопасности являются: рассмотрение как данных физического процесса так и коммуникаций (трафика); комплексные оценки параметров; разработка решений безопасности на базе подходов теории управления и концепции устойчивости [5-6]. Для реализации этих подходов и направлений должна проводиться комплексная системная оценка объекта защиты, а не только отдельных его аспектов.

Системный анализ является основным направлениям комплексной оценки сложных систем. Подход на базе системного анализа [7] определяет несколько важных характеристик при оценке объекта защиты:

Рассмотрение объекта защиты от отдельных компонентов до целостного представления, а также оценка его взаимосвязи с внешней средой (с точки зрения безопасности).

Акцентирование на функциональном представлении КФС и его отображение в систему мониторинга безопасности.

Интеграция различных целей и методов мониторинга безопасности через общие математические методы и гармонизацию сбора и предварительной обработки данных.

Эти аспекты приводят к построению многоуровневой адаптивной системы мониторинга безопасности, включающей все уровни рассмотрения объекта и взаимное отображение этих уровней с подсистемами обработки и анализа данных, а также интеллектуальным функционалом комплексного анализа объекта защиты и управления собственно процессом мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Лебедь С. Security opertions в условиях цифрового хаоса // Материалы SOC-форум 2019 https://ib-bank.ru/soc-forum/materials2019
2. Даренский Д. Industrial Cybersecurity Awareness. Подход Positive Technologies // Материалы SOC-форум 2019 https://ib-bank.ru/soc-forum/materials2019
3. Зегжда П.Д., Полтавцева М.А., Лаврова Д.С. Систематизация киберфизических систем и оценка их безопасности // Проблемы информационной безопасности. Компьютерные системы, - СПб: Изд-во Политехн. Ун-та, 2017. № 2. С. 127-138.
4. Павленко Е.Ю. Модель кибератак на системы цифрового производства // Проблемы информационной безопасности. Компьютерные системы, - СПб: Изд-во Политехн. Ун-та, 2019. № 4. с.72-75
5. Coletta A., Armando A. Security Monitoring for Industrial Control Systems //) Security of Industrial Control Systems and Cyber Physical Systems. CyberICS 2015, WOS-CPS 2015. – LNCS, Springer, 2015. Vol. 9588. P. 48–62.
6. Зегжда, П. Д. Тебекин А.В., Анисимов В. Г., Анисимов Е. Г., Супрун А.Ф. Методический подход к построению моделей прогнозирования показателей свойств систем информационной безопасности Проблемы информационной безопасности. Компьютерные системы - СПб: Изд-во Политехн. Ун-та, 2019. № 4. с.45-49
7. Романов В.Н. Системный анализ для инженеров. – СПб: СЗГТУ, 2006, 186 с.

УДК 004.422

МОДЕЛЬ ДАННЫХ СИСТЕМЫ МОДЕЛИРОВАНИЯ ДВИЖУЩИХСЯ ОБЪЕКТОВ

Проничев Алексей Петрович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: pronichevAP@gmail.com

Аннотация. Работа посвящена разработке модели данных для хранения информации о железнодорожных участках, подвижных составов и др. элементов железнодорожного транспорта. Предложенная модель предназначена для использования в узле управления системы моделирования движущихся объектов.

Ключевые слова: модель данных, система управления.

A DATA MODEL OF THE SYSTEM FOR MOVING OBJECTS SIMULATION

Pronichev Aleksei
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: pronichevAP@gmail.com

Abstract. The work is devoted to the development of a data model for storing information on railway sections, rolling stock, and other elements. The proposed model is intended for use in the control unit of a system for moving objects simulation.

Keywords data model, control system**.**

Интеллектуальные системы плотно вошли в нашу жизнь. Различные виды общественного и индивидуального транспорта уже не существую сами по себе, а объединены в транспортные сети, и используют общую инфраструктуру, в том числе пути (дороги, железнодорожные (ж/д) пути, воздушные коридоры, водные каналы и др.), транспортные узлы и терминалы, где производится погрузка груза и пересадка пассажиров (автобусные остановки, аэропорты, железнодорожные станции и др.). Управление такими сетями производится через системы контроля светофорами, переключения стрелок ж/д путей и др. Управление транспортной системой с каждым днем становится все более сложной задачей, большое внимание уделяется безопасности транспортной инфраструктуры [1]. Особое внимание уделяется развитию полуавтоматизированных и автоматизированных систем управления транспортом.

При рассмотрении событий, происходящих в таких системах, в том числе ситуаций, выходящих за рамки работы в нормальном режиме, таких как: поломки оборудования, стихийные бедствия, аварии, умышленные повреждения коммуникаций и др., требуется использование специализированных систем, имитирующих работу узлов управления для моделирования различных событий. Проблема оценки безопасности в таких системах заключается в отсутствии возможности отработки различных ситуаций на реальных объектах. Необходима выработка моделей для реализации данной возможности

В данной работе предлагается модель данных для узла управления системой моделирования железнодорожного транспорта и путей ж/д сообщения. В системе управления предполагается построение гибридных моделей железнодорожного транспорта и путей ж/д сообщения.

В предлагаемой модели данных железнодорожное полотно представляется как множество однонаправленных графов, вершины которых являются началами и концами отрезков путей. Привязка вершин к реальным физическим координатам на карте местности (или координатами на макете) обеспечивает связь между абстрактной моделью и ее полунатурным и натурным представлениями.

Разработанная модель данных может использоваться в системах моделирования как на имитационном уровне, так и на полунатурном, так как она может представлять из себя описание как физических объектов, так и тех, которые не существуют. Данная модель представляет собой элемент общего комплекса моделирования движущихся объектов.

Предполагается, что данный комплекс может быть использован для моделирования стихийный бедствий, аварий, а также для оценки защищенности транспортных инфраструктур по отношению к целенаправленным вредоносным действиям. В дальнейшей работе планируется проведение экспериментов с использованием предложенной модели данных на разработанном полунатурном стенде с сегментной железнодорожной инфраструктуры.

Работа выполнена при частичной поддержке бюджетной темы № 0060-2019-0010.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон "О транспортной безопасности" от 09.02.2007 N 16-ФЗ (последнее изменение от 02.12.2019 N 415-ФЗ)
2. Котенко И.В., Чечулин А.А., Левшун Д.С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд, № 6(78), 2017. С.48-57.
3. Ахмедзянов Г.Г., Старков И. Н., Поляков В. В. Проблемы обеспечения комплексной безопасности на железнодорожных переездах России //Инновационные проекты и технологии в образовании, промышленности и на транспорте. – 2019. – С. 463-469

УДК 004.422

АНАЛИЗ ПОДХОДОВ К ПРОЕКТИРОВАНИЮ И ОЦЕНКЕ РАСПРЕДЕЛЕННЫХ СИСТЕМ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Проничев Алексей Петрович, Котенко Игорь Витальевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: pronichevAP@gmail.com, ivkote@comsec.spb.ru

Аннотация. Работа является обзором существующих проблем при проектировании распределенных систем больших данных. В работе также проведен анализ решений, применяемых для проектирования и установки таких систем.

Ключевые слова: распределенные системы, обработка больших данных, проектирование.

OVERVIEW OF APPROACHES TO DESIGN AND EVALUATION OF DISTRIBUTED BIG DATA PROCESSING SYSTEMS

Pronichev Aleksei, Kotenko Igor
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: pronichevAP@gmail.com, ivkote@comsec.spb.ru

Abstract. The work is an overview of the existing problems in the design of distributed big data systems. The work also analyzes the solutions used for the design and installation of such systems.

Keywords distributed systems, big data processing, design.

В современном мире рост объемов собираемой информации делает актуальным исследования по разработке и внедрению систем хранения и обработки больших данных. В данных системах акцент делается на производительности, масштабируемости, доступности и целостности [1]. Системы хранения и обработки данных должны уметь адаптироваться к возрастающим объемам данных, эффективно их обрабатывать [2].

Несмотря на большое количество существующих решений, часто возникают проблемы, связанные с ошибками проектирования на начальных этапах использования системы. Наблюдается не соответствие используемых решений, ресурсов и задач, для которых предполагалось использование системы. Не учитывается взаимодействие узлов, потоков, мощности оборудования и др факторы, что приводит к неоптимальному использованию ресурсов. Актуальной задачей является разработка автоматизированных подходов по оценке предполагаемых систем, выработке подходов к планированию на ранних этапах.

В настоящей работе представлен анализ решений, которые применяются для проектирования распределенных систем, систем для автоматической развертки и настройки готовых решений. Особое внимание в обзоре уделено решениям по обработке больших данных, подходам используемых в данных системах, возможностям моделированиях при проектировании предполагаемой системы.

Отдельное внимание уделяется модели данных и способу хранения информации в системе, файловым системам для распределенного хранения (HDFS, GFS, Amazon S3). От выбранной подсистемы хранения зависят характеристики обработки и логическая структура хранения данных и метаданных. Можно выделить такие структуры как документные, колоночные, ключ-значение, графовые хранилища. Необходимо учитывать стратегию распределения метаданных на серверах (ручной, алгоритмы случайного доступа, хеш таблицы и др.), доступности этой информации и географического распределения. От выбранной подсистемы хранения в дальнейшем также будут зависеть характеристики системы обработки данных (MapReduce, Spark, Hadoop, Pig, Hive, Cassandra, Kafka и др.)

Особенности построения каждой системы, сложность реализации, выбор систем хранения, связи между узлами и др. аспекты требуют тщательного анализа при разработке, отладке и внедрении. Моделирование систем и процессов, протекающих в данных системах, вызывают множество трудностей. Процесс моделирования должен учитывать не только рассмотренные аспекты, но и возможность масштабирования, увеличения нагрузки. В дальнейшей работе предполагается разработка системы для проектирования систем обработки больших объемов данных, основанных на таких подходах моделирования как аналитический, имитационный, натурный и полунатурный. Используя различные подходы, предполагается добиться гибкости процесса моделирования, возможность рассмотрения системы под различными углами, снижения трудозатрат

Работа выполнена при частичной поддержке бюджетной темы № 0060-2019-0010.

СПИСОК ЛИТЕРАТУРЫ

1. Kotenko I., Saenko I., Branitskiy A. Improving the Performance of Manufacturing Technologies for Advanced Material Processing Using a Big Data and Machine Learning Framework // Materials Today: Proceedings. 2019. vol. 11. part 1. pp. 380-385.
2. Kotenko I., Saenko I., Kushnerevich A. Parallel big data processing system for security monitoring in Internet of Things networks // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.8, No.4 (December 2017).

УДК 004.056.5

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ABAC-МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА В ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Саенко Игорь Борисович, Иванов Александр Юрьевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ibsaen@comsec.spb.ru, alexandr.y@mail.ru

Аннотация. Рассмотрены особенности реализации модели разграничения доступа, основанной на атрибутах, применительно к построению перспективной системы разграничения доступа в территориально-распределенной телекоммуникационной системе. Обоснованы требования к системе хранения данных в этой системе. Предложены уровни архитектуры системы хранения. Определены взаимодействующие компоненты в системе разграничения доступа. Обсуждаются результаты программной реализации системы.

Ключевые слова: ролевое разграничение доступа, разграничение доступа, основанное на атрибутах, телекоммуникационная система, информационная система.

FEATURES OF IMPLEMENTATION OF THE ABAC ACCESS CONTROL MODEL IN THE TERRITORIAL DISTRIBUTED TELECOMMUNICATION SYSTEM

Saenko Igor, Ivanov Alexander
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ibsaen@comsec.spb.ru, alexandr.y@mail.ru

Abstract. The features of the implementation of the access control model based on attributes are considered in relation to the construction of a promising access control system in a geographically distributed telecommunication

system. The requirements for the data storage system in this system are substantiated. The levels of storage architecture are proposed. The interacting components in the access control system are defined. The results of the software implementation of the system are discussed.

Keywords: role-based access control, attribute-based access control, telecommunication system, information system, information system.

Введение. Современные территориально-распределенные телекоммуникационные системы являются информационными системами с тесно интегрированными компонентами. Они собирают от граждан, правительственных учреждений и коммерческих / некоммерческих организаций большие массивы уязвимой информации и распространяют ее. Однако, несмотря на то, что такие системы существенно улучшают жизнь гражданин, способствуют повышению эффективности решения ими множества различных задач и обеспечивают высокую устойчивость, они также представляют определенные уязвимости безопасности. Защита уязвимой информации от несанкционированного доступа в этом контексте является одним из главных препятствий в получении полного преимущества от развертывания таких инфраструктур. Последствия утечки данных, например, могут включать финансовые убытки, повреждение репутации или даже общественные беспорядки. При этом системы авторизации гарантируют, что доступ к уязвимой информации строго регламентирован через политику безопасности, которая кодирует правила о том, кто может или не может иметь доступ к некоторой информации при некоторых условиях.

Известно множество языков (моделей) для определения и формализации политики безопасности. Эти модели обеспечивают различные конструкции при моделировании требований к защите на основе базовой модели разграничения доступом. Выбор модели разграничения доступом, таким образом, является ключевым вопросом проектирования и построения системы разграничения доступа, так как он определяет выразительность в правилах кодирования и простоту в ее администрировании. Традиционной моделью разграничения доступа, нашедшей достаточно широкое распространение, принято считать ролевую модель (Role-Based Access Control – RBAC) [1]. Модель RBAC получила широкое распространение в связи с тем, что она тесно связана с процессами идентификации пользователей облачных хранилищ и сервисов.

Среди перспективных моделей разграничения доступа, которые возможно использовать в территориально-распределенных телекоммуникационных системах, следует выделить атрибутивную модель (Attribute-Based Access Control, ABAC) [2]. Эта модель выделяет атрибуты объектов, действий, субъектов и условий доступа. При применении этой модели значения атрибутов сравниваются с политикой безопасности, и принимается соответствующее решение о предоставлении доступа.

Модель ABAC учитывает, что территориально-распределенная телекоммуникационная система, как правило, состоит из нескольких локальных телекоммуникационных систем, изначально имеющих различные модели безопасности. Она способна реализовать достаточно гибкий механизм разграничения доступа, поддерживающий гетерогенные структуры и обеспечивающий безопасность своего функционирования. Считается, что недостатком этой модели является ее узкое практическое распространение. Однако, говоря о перспективной системе разграничения доступа к информации в территориально-распределенной телекоммуникационной системе, следует полагать, что эта система должны быть ориентирована в большей степени на использование модели ABAC.

В отличие от модели RBAC, модель ABAC ориентирована на выполнение тех или иных действий над ресурсами (объектами), основываясь на проверку корректности выполнения множества логических условий (правил), которые определяют используемую политику контроля доступа. Правила формируются в виде логических выражений, в которых используются значения атрибутов. Множество атрибутов состоит из атрибутов пользователей (субъектов), атрибутов ресурсов (объектов) и атрибутов компьютерного окружения. К последней группе относится также время. По этой причине модель ABAC является более гибкой, чем другие модели контроля доступа, и способной быстро реагировать на изменения [3].

Перспективная ABAC-ориентированная система разграничения доступа к информации в территориально-распределенной телекоммуникационной системе должна решать множество задач, включая оценку качества политик разграничения доступа, их структурную оптимизацию [4], верификацию и реструктуризацию. Решение каждой из перечисленных задач базируется на соответствующих математических моделях и обеспечивается функционированием соответствующих компонентов, входящих в состав этой системы. Вместе следует отметить, что центральным компонентом такой системы является компонент хранения политик разграничения доступа, или информационное хранилище.

К хранению данных в ABAC-ориентированной системе разграничения доступа к информации предъявляются следующие требования:

1) возможность представлять данные в реляционном формате, в XML-формате, а также в RDF-формате. XML-формат позволяет хранить шаблоны политик разграничения доступа, которые записываются на XML-ориентированном языке представления. RDF-формат необходим для реализации логического вывода (верификации политик);

2) достаточная производительность и отказоустойчивость. Учитывая, что хранилище данных является центральным узлом, достижение этих требований во многом будет определяться за счет использования для развертывания репозитория высокопроизводительной и отказоустойчивой аппаратной платформы;

3) достаточная гибкость интерфейсов взаимодействия с остальными компонентами перспективной системы разграничения доступа. Для реализации этого требования предлагается ориентироваться на концепцию «сервис-ориентированной архитектуры».

В соответствии с данными требованиями, в архитектуре перспективной ABAC-ориентированной системы разграничения доступа выделяются два уровня, ответственных за хранение данных: уровень хранения данных и уровень веб-сервисов. При этом на уровне хранения предполагается хранение всех видов информации, необходимой для решения задачи разграничения доступа в территориально-распределенной телекоммуникационной системе. Таковыми видами баз данных являются: реляционная база данных; базу XML-данных; базу RDF-данных. Последняя база данных иначе называется хранилищем триплетов. Тем самым обеспечивается гибридный подход к хранению данных о политиках разграничения доступа, сочетающий в себя достоинства всех базовых моделей представления данных и обеспечивающий, с одной стороны, формализацию политик разграничения доступа в виде сложных логических утверждений, а с другой – использование логического вывода для выработки решений.

Основными взаимодействующими компонентами предлагаемой системы разграничения являются следующие компоненты: компонент оценки качества политик разграничения доступа, компонент структурной оптимизации политик разграничения доступа, компонент верификации и обеспечения непротиворечивости политик разграничения доступа и компонент структурной реконфигурации политик разграничения доступа.

Реализация хранилища данных рассмотренной выше архитектуры была выполнена в среде комплексной семантической системы хранения Virtuoso. Оценка функциональных показателей сконструированного таким образом хранилища данных показала, во-первых, полноту реализации функций хранения и интеграцию политик разграничения доступа в различных форматах, и, во-вторых, достаточно высокую производительность при работе с RDF-данными.

Заключение. Предложенный подход к использованию модели ABAC для построения системы разграничения доступа к территориально-распределенной телекоммуникационной системе обеспечивает, в обличие от модели RBAC, выполнение требований, предъявляемых к этой системе. Дальнейшие исследования связываются с расширением области применения полученных решений и распространение их на более широкое множество информационных инфраструктур.

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01369) в СПИИРАН и бюджетной темы 0073-2019-0002.

СПИСОК ЛИТЕРАТУРЫ

1. Саенко И.Б., Бирюков М.А., Ясинский С.А., Грязев А.Н. Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах // Информация и космос. –2018. – №1. – С. 81-85.
2. Servos D., Osborn S.L. Current Research and Open Problems in Attribute-Based Access Control // ACM Comput. Surv. 2017. Vol. 49. No. 4. Article 65, 45 pages.
3. Karatas G., Akbulut A. Survey on Access Control Mechanisms in Cloud Computing // Journal of Cyber Security and Mobility. 2018. Vol. 7, No. 3. Pp. 1–36.
4. Kotenko Igor, Saenko Igor. Improved genetic algorithms for solving the optimization tasks in access scheme design for computer networks // Int. J. Bio-Inspired Computation. 2015. Vol. 7. No. 2. Pp. 98–110.

УДК 004.056.5

ПЕРСПЕКТИВНАЯ СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ ДЛЯ СИСТЕМЫ ГОРОДСКОГО ОБЩЕСТВЕННОГО ТРАНСПОРТА

Саенко Игорь Борисович, Комашинский Владимир Ильич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ibsaen@comsec.spb.ru, alexandr.y@mail.ru

Аннотация. Рассмотрены особенности применения перспективной модели разграничения доступа, основанной на атрибутах, для предметной области системы городского общественного транспорта. Выделены группы атрибутов, которые используются для формализации правил разграничения доступа. Определены основные функции, которые должна выполнять перспективная система разграничения доступа к информации в системе городского общественного транспорта. Обсуждаются результаты экспериментальной оценки программного прототипа системы, реализованного в среде Hadoop.

Ключевые слова: разграничение доступа, модель разграничения доступа, городской общественный транспорт, облачная инфраструктура, информационная система.

A PERSPECTIVE INFORMATION ACCESS CONTROL SYSTEM FOR THE URBAN PUBLIC TRANSPORT SYSTEM

Saenko Igor, Komashinski Vladimir
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ibsaen@comsec.spb.ru, alexandr.y@mail.ru

Abstract. The features of the application of a promising model of access control based on attributes for the subject area of the urban public transport system are considered. The groups of attributes that are used to formalize the rules of access control are highlighted. The main functions to be performed by a promising system of differentiating access to information in the system of urban public transport have been determined. The results of the experimental evaluation of the software prototype of the system implemented in the Hadoop environment are discussed.

Keywords: access control, access control model, urban public transport, cloud infrastructure, information system.

Введение. Система городского общественного транспорта (СГОТ) как информационная инфраструктура является достаточно специфической разновидностью автоматизированных систем управления. К числу особенностей такой системы можно отнести: очень большую распределенность узлов и центров обработки данных; большую разнородность и очень большие объемы обрабатываемой информации; жесткие требования по оперативности и безопасности процессов обработки данных [1].

В результате СГОТ может рассматриваться как разновидность киберфизической системы, повышение эффективности функционирования которой необходимо увязывать с облачной архитектурой построения этой системы [2] и с необходимостью решения вопросов разграничения доступа к обрабатываемой информации с использованием новых, более гибких моделей разграничения доступа [3, 4]. Одной из таких перспективных моделей разграничения доступа является модель разграничения доступа, основанная на атрибутах (Attribute-Based Access Control, ABAC) [5,6]. Поэтому основной целью настоящей работы является рассмотрение вопросов построения перспективной системы разграничения доступа к информации в СГОТ, базирующейся на модели ABAC, ориентированной на реализацию в облачной архитектуре и учитывающей особенности предметной области СГОТ.

Прежде всего, следует выделить особенности модели ABAC и определить, в чем заключается ее основное отличие от ставшей уже традиционной ролевой модели разграничения доступа (Role-Based Access Control, RBAC).

В модели RBAC производится формирование ролей и присваивание наборов ролей отдельным пользователям. Роли рассматриваются как математические абстракции, обладающие определенными наборами полномочий доступа к защищаемым объектам учета. Роли формируются в соответствии с задачами, которые решают пользователи. Роль обладает минимально необходимым набором полномочий, необходимых пользователям для выполнения своих функциональных обязанностей. Поэтому разрешенные полномочия пользователей определяются в соответствии с назначенными им роями. Полномочия в ролях, также как и роли, приписанные пользователям, могут добавляться или удаляться решениями администратора системы. Модель RBAC в настоящее время достаточно хорошо проработана и реализована во многих программно-инструментальных платформах. Она имеет множество разновидностей, таких как Task-RBAC (ориентированная на исполняемые задачи) [7], Trust-RBAC (учитывает доверительные отношения между будущими транзакциями) [8] и Temporal-RBAC (учитывает динамику изменения связей между пользователями, ролями и полномочиями) [9].

Модель ABAC выделяет атрибуты объектов, действий, субъектов и условий доступа. При применении этой модели значения атрибутов сравниваются с политикой безопасности, и принимается соответствующее решение о предоставлении доступа. Атрибутивная модель учитывает, что облачная инфраструктура, как правило, состоит из нескольких автономных корпоративных автоматизированных систем, изначально имеющих различные модели безопасности.

В предметной области СГОТ модель RBAC не является достаточно гибкой, даже учитывая ее разновидности. Это объясняется тем, что применяемые в СГОТ политики безопасности (точное, разграничения доступа) могут содержать правила, которые очень трудно или даже невозможно формализовать на основе модели RBAC. В то же время, модель ABAC свободна от каких-либо ограничений, касающихся формализации правил политик разграничения доступа.

Атрибуты предметной области СГОТ предлагается разделить на группы. К числу таких групп относятся:

- характеристики транспортных средств;
- характеристики маршрутов движения транспортных средств;
- характеристики пассажиропотоков;
- атрибуты водительского состава пассажирского транспорта;
- атрибуты диспетчерско-административного персонала;
- атрибуты средств и личного состава подразделений аварийно-восстановительной и ремонтной службы
- и некоторые другие.

Рассматриваемая перспективная система разграничения доступа к информации в СГОТ должна выполнять следующие функции:

- формировать правила, соответствующие требованиям применяемой в СГОТ политики безопасности:
- проводить оценку качества политик разграничения доступа, т.е. анализировать их в соответствии с принятыми критериями оценки качества;

– проводить структурную оптимизацию политик разграничения доступа, устраняя при этом избыточные правила и/или их компоненты;

– обеспечивать верификации и контроль непротиворечивости политик разграничения доступа, т.е. проверять истинность (правильность) сформированных правил и их взаимную непротиворечивость;

– проводить структурную реконфигурацию политик разграничения доступа в случае изменения задаваемых требований политик безопасности и/или состава субъектов и/или объектов доступа.

– хранение данных, необходимых для управления правилами разграничения доступа, в облачном хранилище;

– реализация визуального интерфейса пользователей с данной системой.

Прототип данный системы реализован в среде Hadoop и использованием базы данных Hbase. Этим обеспечивается высокая масштабируемость системы. При решении оптимизационных задач в ходе функционирования системы применялись генетические алгоритмы. Экспериментальные результаты продемонстрировали достаточно высокие значения показателей оперативности и безопасности функционирования этой системы.

Заключение. Предложенный подход к построению и функционированию перспективной системы разграничения доступа к информации в СГОТ обеспечивает достижение ею высоких значений показателей оперативности и безопасности функционирования. Дальнейшие направления исследований связываются с внедрением предложенных решений по разграничению доступа к обрабатываемой информации в систему управления «умным городом».

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01369) в СПИИРАН и бюджетной темы 0073-2019-0002.

СПИСОК ЛИТЕРАТУРЫ

1. Малыгин И.Г., Комашинский В.И., Королёв О.А. Внедрение когнитивных технологий обеспечения безопансоти дорожного движения в интеллектуальные транспортные системы // Транспорт России: проблемы и перспективы - 2018. Материалы международной научно-практической конференции. 2018. С. 7-13.
2. Малыгин И.Г., Шаталова Н.В., Комашинский В.И., Аванесов М.Ю., Михалев О.А. Транспортные технологии и глобализация в период 4-й индустриальной революции (проблемы и перспективы) // Информация и космос. 2018. № 1. С. 6-13.
3. Саенко И.Б., Бирюков М.А., Ясинский С.А. Методика формирования единой системы разграничения доступа к гетерогенным информационным ресурсам в облачных инфраструктурах // Информация и космос, 2019, №1. С. 77-83
4. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121-126.
5. Servos D., Osborn S.L. Current Research and Open Problems in Attribute-Based Access Control // ACM Comput. Surv. 2017. Vol. 49. No. 4. Article 65, 45 pages.
6. Калимолдаев М.Н., Бияшев Р.Г., Рог О.А. Анализ методов атрибутного разграничения доступа // ПДМ. 2019. №44. URL: https://cyberleninka.ru/article/n/analiz-metodov-atributnogo-razgranicheniya-dostupa (дата обращения: 20.07.2020).
7. Sejong O., Seog P. Task Role-Based Access Control Model // Information Systems. 2003. No. 6. Pp. 533–562.
8. Soon-Keow C., Jemal A., Masitah A., Isredza R. Enhancing trust management in cloud environment // Proceedings of the International Conference on Innovation, Management and Technology Research. 2014. Pp. 314–321.
9. Muthurajkumar S., Vijayalakshmi M., Kannan A. Intelligent temporal role based access control for data storage in cloud database // Proceedings of the IEEE Sixth International Conference on Advanced Computing (ICoAC). 2014. Pp. 184–188.

УДК 004.056.5

ФУНКЦИОНАЛЬНЫЕ ВЗАИМОСВЯЗИ И СОДЕРЖАНИЕ УРОВНЕЙ ОБОБЩЕННОЙ АРХИТЕКТУРЫ ПЕРСПЕКТИВНОЙ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Саенко Игорь Борисович[1], Паращук Игорь Борисович[1], Бушуев Сергей Николаевич[2]

[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

[2] Акционерное общество «Научно производственное предприятие ТЕЛДА»
Белоостровская ул., 25, Санкт-Петербург, 197342, Россия

e-mails: ibsaen@comsec.spb.ru, shchuk@rambler.ru, bsn5688@yandex.ru

Аннотация. Рассмотрены уровни обобщенной архитектуры перспективной интеллектуальной системы разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем, их функции и особенности. Эта архитектура представляет собой комплекс средств, алгоритмов, программных прототипов и отражает функциональные взаимосвязи и циркулирующие информационные потоки между отдельными компонентами, реализующими модели и методы анализа, структурной оптимизации и верификации систем разграничения доступа к информации.

Ключевые слова: архитектура, разграничение доступа, модель доступа, система, облачная инфраструктура, уровень, данные, угроза, моделирование, нарушитель, информационная система.

FUNCTIONAL RELATIONSHIPS AND CONTENT OF THE LEVELS OF THE GENERALIZED ARCHITECTURE OF A PROMISING SYSTEM FOR DELIMITING ACCESS TO INFORMATION IN CLOUD INFRASTRUCTURES OF CRITICAL INFORMATION SYSTEMS

Saenko Igor[1], Parashchuk Igor[1], Bushuev Sergey[2]
[1] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] JSC «Scientifically manufacturing enterprise TELDA»
25, Beloostrovskaya St, Saint-Petersburg, 197342, Russia
e-mails: ibsaen@comsec.spb.ru, shchuk@rambler.ru, bsn5688@yandex.ru

Abstract. The levels of the generalized architecture of a promising intelligent system for delimiting access to information in cloud infrastructures of critical information systems, their functions and features are considered. This architecture is a set of tools, algorithms, software prototypes and reflects the functional relationships and circulating information flows between individual components that implement models and methods of analysis, structural optimization, and verification of information access control systems.

Keywords: architecture, delimiting access, access model, system, cloud infrastructure, layer, data, threat, simulation, intruder, information system.

Введение. В мире все больше внимания уделяется постановке и решению задач совершенствования моделей контроля доступа. На их основе осуществляется разработка эффективных интеллектуальных методов и алгоритмов управления политиками разграничения доступа (РД) в облачных инфраструктурах (ОИ) критически важных информационных систем (КВИС). Множество современных работ посвящены обзору технологических решений в этой предметной области, решению задач обеспечения требуемого РД в ОИ, синтезу системы показателей и критериев оценки качества политик разграничения доступа для облачных инфраструктур, концептуальным вопросам моделирования процесса разграничения доступа к информации в ОИ, алгоритмам оценки качества, оптимизации, верификации и реконфигурации политик разграничения доступа для различных моделей управления доступом, применяемых в ОИ КВИС [1].

Решение всех этих задач нарабатывает на главную цель – выработку практических рекомендаций по эффективному применению систем РД к информации в различных сценариях построения и функционирования облачных инфраструктур критически важных информационных систем. При этом в ходе исследования и разработки моделей, методов и алгоритмов оценки качества политик РД в ОИ КВИС зачастую в качестве исходных данных используются требуемая и результирующая схемы разграничения доступа. Требуемая схема разграничения доступа задается лицом, принимающим решения, а результирующая схема образуется на основании правил, свойственных выбранной модели контроля доступа.

Результатом решения задачи является значение обобщенного показателя, отражающего степень различия между требуемой и результирующей схемами. Разработанные методы оценки качества чаще всего ориентированы на модель разграничения доступа, основанную на атрибутах (Attribute-Based Access Control, ABAC), поскольку эта модель считается наиболее перспективной для применения в ОИ КВИС. Важность этой задачи определяется тем, что оценка качества политик разграничения доступа является одной из составных частей проблемы нахождения наиболее эффективной политики (схемы) разграничения доступа в модели ABAC [2].

Особое место в перечне решаемых задач разработки и построения эффективной системы разграничения доступа (СРД) занимают вопросы формирования обобщенной архитектуры и создания программных прототипов компонентов перспективной СРД к информации в ОИ КВИС.

Обобщенная архитектура перспективной СРД к информации в ОИ КВИС должна отражать функциональные взаимосвязи и циркулирующие информационные потоки между отдельными компонентами, реализующими модели и методы анализа, структурной оптимизации и верификации систем РД к информации.

Понимая под «архитектурой» принципиальную организацию системы, воплощенную в её элементах, их взаимоотношениях друг с другом и со средой, а также принципы, направляющие её проектирование и эволюцию, остановимся на формулировке функциональных взаимосвязей и содержания уровней (граней) обобщенной архитектуры перспективной интеллектуальной СРД к информации в ОИ КВИС.

Первый уровень (грань) обобщенной архитектуры, отвечающий за компетенции (функции, опции) перспективной СРД к информации в ОИ КВИС, содержит, так называемые, опциональные компоненты:

– компонент оценки качества политик разграничения доступа – отвечает за анализ (на основе разработанных моделей, методов и алгоритмов) показателей качества политик разграничения доступа для различных моделей управления доступом, применяемых в ОИ КВИС;

– компонент структурной оптимизации политик разграничения доступа – отвечает за выбор оптимальных политик разграничения доступа (на основе разработанных интеллектуальных моделей и алгоритмов) для различных моделей управления доступом, применяемых в ОИ КВИС;

– компонент верификации и обеспечения непротиворечивости политик разграничения доступа – отвечает за проверку истинности (правильности) и гарантирует (на основе разработанных интеллектуальных моделей и алгоритмов), что политики РД не противоречат друг другу в ОИ КВИС;

– компонент структурной реконфигурации политик разграничения доступа – отвечает за выявление условий проведения и непосредственное выполнение процедур реконфигурации (на основе разработанных интеллектуальных моделей и алгоритмов) политик разграничения доступа в ОИ КВИС [3].

Помимо этого, к обязательным компонентам этого уровня могут относиться компонент управления и компонент хранения данных.

Второй уровень (грань) обобщенной архитектуры, отвечающий за интеграцию (функциональную взаимосвязь) в рамках перспективной СРД к информации в ОИ КВИС, является интеграционной платформой, включающей четыре ключевых подуровня:

– подуровень аппаратно-программных средств интеллектуального анализа и принятия решений по контролю и РД к информации в ОИ КВИС;

– подуровень хранилища информации о результатах интеллектуального анализа и принятия решений по контролю и РД к информации в ОИ КВИС;

– подуровень аналитических инструментов и средств РД к информации в ОИ КВИС, принятия решений по РД и генерации отчетов;

– подуровень средств управления и настраиваемые интерфейсы СРД с пользователями и администраторами безопасности ОИ КВИС.

Интеграционная платформа является ядром системы РД к информации в ОИ КВИС, она реализует функции по интеграции и взаимодействию всех компонент, составляющих эту систему. Основная цель интеграционной платформы состоит в обеспечении четкой и оперативной координации и взаимодействия средств (устройств) и лиц, отвечающих за РД к информации в ОИ КВИС. Программные приложения, реализующие интеллектуальное РД к информации в ОИ КВИС, отличаются ориентацией на платформу параллельной обработки данных. Программные прототипы ориентированы на возможность масштабирования в условиях обработки больших данных, а также использование открытого системного программного обеспечения.

Заключение. Предложенный подход к систематизации и формулировке опций и особенностей уровней обобщенной архитектуры перспективной интеллектуальной СРД к информации в ОИ КВИС отражает функциональные взаимосвязи и циркулирующие информационные потоки между отдельными компонентами, реализующими модели и методы анализа, структурной оптимизации и верификации систем разграничения доступа к информации. Это, по мнению авторов, позволит повысить достоверность и оперативность оценки качества политик разграничения доступа и позволит улучшить качество принимаемых решений по эффективному управлению разграничением доступа к информации в облачных инфраструктурах критически важных информационных систем.

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01369) в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Verma G., Verma V. Role and Applications of Genetic Algorithm in Data Mining // International Journal of Computer Applications. 2012. Vol. 48, No. 17. pp. 5-8.
2. Саенко И.Б., Бирюков М.А., Ефимов В.В., Ясинский С.А. Модель администрирования схем разграничения доступа в облачных инфраструктурах // Информация и космос. 2017. № 1. С. 121-126.
3. Саенко И.Б., Паращук И.Б., Бушуев С.Н. Модель и алгоритм выявления необходимости реконфигурации политик разграничения доступа в критически важных облачных инфраструктурах // Информационная безопасность регионов России (ИБРР-2019) XI-я Санкт-Петербургская Межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г., Материалы конференции, – СПб.: СПОИСУ, 2019. – 596 с. С.304-306.

УДК 004.422

МОДЕЛЬ СИСТЕМЫ АНАЛИТИКИ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

Тынымбаев Болат Айткожинович[1], Котенко Игорь Витальевич[2]
[1] Евразийский национальный университет имени Л.Н. Гумилева
Сатпаева ул., 2, Нур-Султан, 010000, Республика Казахстан
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ivkote@comsec.spb.ru, tynymbaevba@gmail.com

Аннотация. Работа посвящена разработке модели системы аналитики поведения пользователей для удаленных подключений к облачному сервис-провайдеру. Используется метод разбиения пользователей на отдельные группы в соответствии их навыками в области кибербезопасности.

Ключевые слова: модель данных, облачные сервис-провайдеры, аналитика поведения пользователей.

A MODEL OF USER BEHAVIOR ANALYTICS SYSTEM

Tynymbayev Bolat[1], Kotenko Igor[2]
Eurasian national university, L.N. Gumilev named
2 Satpaev St, Nur-Sultan, 010000, The Republic of Kazakhstan
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ivkote@comsec.spb.ru, tynymbaevba@gmail.com

Abstract. The work is devoted to the development of a data model for user behavior analytics by remote connections to cloud service provider. A method is used to divide users into separate groups according to their cybersecurity skills.

Keywords: data model, cloud services, user behavior analytics**.**

Ввиду роста угроз в сфере кибербезопасности, а также наличия большого количества данных, требуемых для анализа в системах кибербезопасности, одним из актуальных направлений развития в области кибербезопасности является обеспечение эффективной ситуационной осведомленности, в том числе определение с какими угрозами необходимо бороться, и какими рисками кибербезопасности необходимо управлять.

В связи с этим, аналитические инструменты начинают активно использоваться в решениях кибербезопасности.

Одними из таких решений является системы аналитики поведения пользователей UBA (user entity behavior analytics) и системы аналитики поведения пользователей и сущностей UEBA (user entity behavior analytics). Примеры решений класса UEBA, используемые сценарии и модели описаны в [1].

Архитектура потенциальной системы класса UEBA представлена в [2]. Основные данные для систем подобного класса: собранные логи информационных активов, для которых проводится нормализация логов; сценарии определения угроз и фактов аномального поведения; выявленные инциденты аномального поведения.

Разработанная архитектура представлена на рис 1.

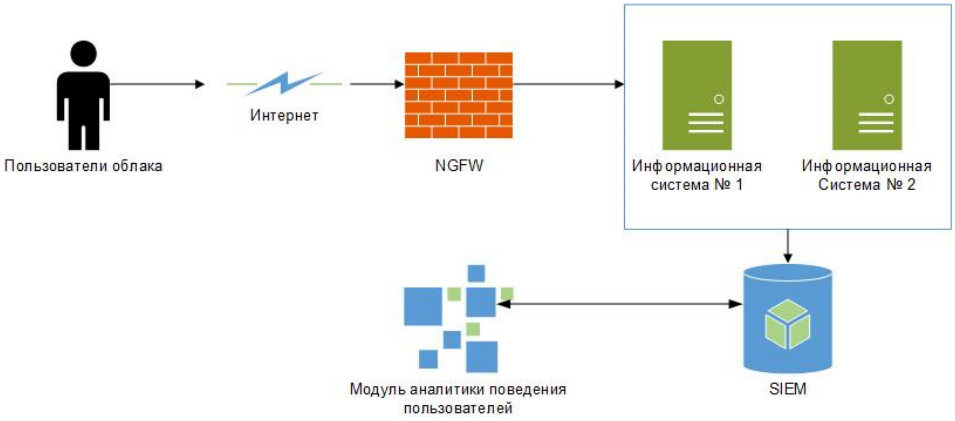

Рис.1 Архитектура системы аналитики поведения пользователей

В работе представлена модель аналитики поведения пользователей для удаленных подключений к облачному сервис-провайдеру. Модель построена на основе первичного анализа уровня осведомленности и знаний по информационной безопасности пользователей. Первичный анализ позволяет распределять пользователей на отдельные группы с соответствующим набором весов для определения аномального поведения.

Согласно данной архитектуре была апробирована система аналитики поведения пользователей с соответствующим разбиением пользователей на группы.

В докладе представлена модель и архитектура системы UEBA, предназначенной для защиты информационных ресурсов облачного сервис-провайдера. Предложена модель подсчета рейтинга поведения пользователей, при удаленном режиме работы.

Исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

СПИСОК ЛИТЕРАТУРЫ

1. Тынымбаев Б.А., Котенко И.В. Обзор решений класса UEBA // Актуальные проблемы инфо-телекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 586-590.
2. Котенко И.В., Тынымбаев Б.А Архитектура перспективной системы UEBA для провайдеров облачных услуг // Актуальные проблемы инфо-телекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 581-585.

УДК 004.056.5

ЭТАПЫ ИССЛЕДОВАНИЯ И ПОСТРОЕНИЯ БЕЗОПАСНОГО ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА ДЛЯ СОВРЕМЕННОЙ ИНТЕЛЛЕКТУАЛЬНОЙ ТРАНСПОРТНОЙ СРЕДЫ

Чечулин Андрей Алексеевич, Паращук Игорь Борисович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: chechulin@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Интеллектуальная транспортная среда и беспилотный транспорт приобретают все большую популярность, особенно в рамках концепции «умный город». Важнейшая проблема их внедрения – безопасность,

а наиболее уязвимым их элементом, влияющим на безопасность, являются человеко-машинные интерфейсы. Рассматривается подход к формулировке сущности и содержания этапов исследования и построения человеко-машинного интерфейса для современной интеллектуальной транспортной среды, сущность задач поиска уязвимостей таких интерфейсов. Перечень этапов включает как моделирование угроз, так и решение задач интеллектуальной обработки данных, что позволит повысить безопасность систем управления беспилотным транспортом «умного города».

Ключевые слова: интеллектуальная транспортная среда, беспилотный транспорт, умный город, интерфейс, уязвимость, угроза, данные, искусственный интеллект.

STAGES OF RESEARCH AND BUILDING OF A SAFE HUMAN-MACHINE INTERFACE FOR A MODERN INTELLECTUAL TRANSPORT ENVIRONMENT

Chechulin Andrey, Parashchuk Igor
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: chechulin@comsec.spb.ru, shchuk@rambler.ru

Abstract. Intelligent transport environment and driverless transport are becoming increasingly popular, especially within the framework of the "smart city" concept. The most important problem of their implementation is security, and the most vulnerable element affecting security is human-machine interfaces. The approach to the formulation of the nature and content of the stages of research and building human-machine interface for modern intelligent traffic environment, the entity search task of the vulnerabilities of these interfaces. The list of stages includes both threat modeling and solving problems of intelligent data processing, which will improve the security of the "smart city"driverless transport management systems.

Keywords: intelligent transport environment, driverless transport, smart city, interface, vulnerability, threat, data, artificial intelligence.

Введение. Современные исследователи считают концепцию «умного города» важным элементом развития больших киберфизических систем, а также новым поколением сетевых распределенных и функционально взаимосвязанных социальных, физических и кибернетических инфраструктур. При этом «умным городом» принято называть взаимоувязанную по месту и во времени, в биологической и технологической среде совокупность подсистем «умного жизнеобеспечения», «умного здравоохранения», «умного образования», «умного транспорта» и т.д. Лавинообразный рост количества транспортных средств за рубежом и в городах нашей страны создает объективные предпосылки для поиска путей и методов оптимизации транспортных потоков. Одним из подходов к решению подобных проблем на пути к созданию, например, «умного транспорта», является разработка и внедрение интеллектуальной транспортной среды (ИТС) «умного города», важным элементом которой являются беспилотный транспорт (БПТ) [1]. Вместе с тем, фундаментальной проблемой «умного города» продолжает оставаться его безопасность, поскольку к комплексности угроз добавляется их многоуровневость. Проблема наиболее активно проявляется в том, что уровень угроз различен на разных пространственных, социальных, физических и кибернетических участках, а также в разных временных координатах жизнедеятельности «умного города» и его ИТС [2, 3].

Современный БПТ в рамках ИТС «умного города» имеет различные реализации: беспилотные средства общественного транспорта (метро, автобусы); беспилотные средства частного транспорта (такси, дроны); беспилотные средства рабочей техники (техника для уборки дорог, вывоза мусора). Кроме того, «умный транспорт», помимо перечисленного, включает инфраструктуры для их навигации и функционирования (дороги, элементы дорожной разметки, знаки дорожного движения, светофоры, заправочные станции и станции подзарядки, станции техобслуживания), а также людей, представляющих собой как пользователей транспортной среды, так и персонал. Эффективно взаимодействовать этим компонентам призван помочь искусственный интеллект (ИИ), без помощи которого сегодня невозможно обрабатывать и анализировать поток больших данных, создаваемый множеством взаимодействующих элементов БПТ.

К ключевым этапам исследования и построения подсистем ИИ для БПТ в рамках ИТС «умного города» относят предоставление данных, необходимых человеку для взаимодействия с БПТ, в удобном для восприятия человеком виде, а также сбор необходимых данных о человеке для оценки его состояния, идентификации и аутентификации БПТ. Осуществляя обработку данных в режиме реального времени, ИИ может предоставить человеку информацию о загруженности ИТС «умного города» (трафик, наличие свободных средств передвижения и мест в них), о возможных маршрутах движения БПТ и их оптимизации, о расписании движения БПТ и его изменении, об авариях и инцидентах, о доступных парковочных местах, о размере очередей на заправках или станциях техобслуживания. Более того, ИИ может отвечать за сбор и обработку биометрических данных о человеке (например, отпечаток пальца), использующем или управляющем БПТ.

Безопасность работы человека с ИИ, а значит и с БПТ и с ИТС «умного города» в целом, опирается, по сути, на безопасность различных интерфейсов, призванных осуществлять взаимодействие этих компонент. Под интерфейсом понимается совокупность средств, методов и правил взаимодействия (управления, контроля и т.п.) между ИИ, БПТ и иными элементами ИТС «умного города». При этом различают понятия «системный интерфейс» – совокупность унифицированных технических, программных и конструктивных средств,

основанных на стандарте и реализующих взаимодействие функциональных элементов в ИТС «умного города», обеспечивающих информационную, электрическую и конструктивную совместимость этих элементов, а также «пользовательский интерфейс» – совокупность средств, при помощи которых пользователь взаимодействует с различными программами и устройствами. Многомодальные интерфейсы, в которых предусмотрена возможность взаимодействия человека с ИИ посредством ручного и автоматического ввода и вывода текстовой и графической информации, звуков и жестов, являются наиболее перспективными из современных интерфейсов. Важность, значимость роли интерфейсов, наряду с ростом числа угроз, предопределяют объективную необходимость формулировки этапов исследования и построения безопасного человеко-машинного интерфейса для современной ИТС, необходимость решения задач поиска уязвимостей таких интерфейсов в интересах безопасного управления БПТ «умного города».

Сущность и содержание этапов исследования и построения безопасного человеко-машинного интерфейса для современной ИТС «умного города» напрямую связаны с целевой функцией – обеспечением безопасности людей, транспортных средств и объектов инфраструктуры за счет обнаружения уязвимостей интерфейсов между человеком и ИИ в рамках управления БПТ и в ИТС «умного города» в целом. Для этого предполагается разработать методы поиска уязвимостей интерфейсов взаимодействия в рамках транспортной среды. При этом содержание конкретных задач нацелено на: анализ научных работ и результатов практических исследований, посвященных методам человеко-машинного взаимодействия, визуализации данных, когнитивного аппарата человека и методам машинного зрения [4]; классификацию интерфейсов взаимодействия с БПТ, а также разработку метода определения типа интерфейса «человек-ИИ»; классификацию возможных угроз для БПТ и для ИТС «умного города» в целом, реализация которых возможна посредством использования интерфейсов «человек-ИИ»; классификацию уязвимостей интерфейсов «человек-ИИ»; разработку концептуальных моделей интерфейсов взаимодействия пользователь-система, система-пользователь, оператор-система, система-оператор; разработку методов поиска уязвимостей этих интерфейсов взаимодействия на основе классификации уязвимостей и концептуальных моделей интерфейсов; разработку программного обеспечения для программно-аппаратного стенда с использованием компонентов, реализующих модели интерфейсов «человек-ИИ» и методы поиска уязвимостей в этих интерфейсах. Необходимы экспериментальные исследования с разработанными методами поиска уязвимостей и методом определения типа интерфейса, интерпретация полученных результатов. Итоговым этапом исследования и построения безопасного человеко-машинного интерфейса является разработка научно-технических предложений по внедрению полученных результатов решения перечисленных задач в интересах безопасного управления беспилотными транспортными средствами «умного города».

Заключение. Таким образом, ключевыми этапами исследования и построения безопасного человеко-машинного интерфейса для современной ИТС «умного города» являются этапы разработки научно-методического обеспечения, включающего комплекс взаимосвязанных методов, моделей и программных прототипов, предназначенных для поиска уязвимостей в интерфейсах «человек-ИИ», предназначенных для управления БПТ и ИТС «умного города» в целом. Данные этапы и решаемые на них задачи являются концептуально новыми, а их решение позволит, за счет учета аспектов безопасности, сделать качественно новый сдвиг в области систем управления беспилотным транспортом и пересмотреть эффективность текущих способов взаимодействия человека и искусственного интеллекта в обеспечении непрерывного и надежного управления интеллектуальной транспортной средой «умного города».

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099) в СПИИРАН.

СПИСОК ЛИТЕРАТУРЫ

1. Sladkowski A., Pamula W. (Eds.) Intelligent transportation systems – problems and perspectives (Vol. 32). Springer International Publishing, 2016. 303 p.
2. Котенко И.В., Паращук И.Б. Автоматизированный адаптивный мониторинг комплексной безопасности информационных систем «умного города»: целевые функции концептуальной модели // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника. Информатика», № 3, 2018. С. 7-15.
3. Котенко И.В., Паращук И.Б. Анализ задач и потенциальных направлений разработки современных методов и средств обеспечения комплексной безопасности киберфизических систем типа «умный транспорт» // Научное обозрение. № 25. 2017. С. 26-30.
4. Проноза А.А., Чечулин А.А., Котенко И.В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. Вып. 46. С. 90-107.

ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ

УДК 378.1

О МЕСТЕ И РОЛИ ИКТ-КОМПЕТЕНЦИИ В ОБНОВЛЕННЫХ ФГОС ВО

Воронов Сергей Алексеевич
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации,
Летчика Пилютова ул., 1, Санкт-Петербург, 198332, Россия
e-mail: voronov-sci@mail.ru

Аннотация. В статье автор обозначает роль ИКТ-компетенции в жизнедеятельности человека и приводит существующие классификации компетенций. Проводя сравнение содержания ключевых компетенций выделяется общий подход к обозначению компетенций в сфере информационных технологий. На основе проведенного анализа ФГОС ВО последнего поколения обсуждается место ИКТ-компетенции. Автор указывает на представленные изменения значимости ИКТ-компетенции в новых ФГОС ВО по сравнению с предыдущими требованиями.

Ключевые слова: Информационно-коммуникационные технологии, ИКТ-компетенция, универсальные компетенции, ФГОС ВО

ABOUT THE PLACE AND ROLE OF ICT COMPETENCE IN THE UPDATED FSES OF HE

Voronov Sergey
Saint Petersburg military order of Zhukov Institute of the national guard of the Russian Federation
Pilot Pilyutova str., 1, Saint Petersburg, 198332, Russia
e-mail: voronov-sci@mail.ru

Abstract. In the article, the author identifies the role of ICT competence in human life and provides existing classifications of competencies. When comparing the content of key competencies, a General approach to the designation of competencies in the field of information technology is highlighted. The place of ICT competence is discussed on the basis of the analysis of the latest generation of FES. The author points to the presented changes in the importance of ICT competence in the new FES of HE and expresses concern about the existing approach.

Keyword: Information and communication technologies, ICT competence, universal competencies, Federal educational standard of higher education

Информационно-коммуникационные технологии используются практически во всех сферах жизнедеятельности и являются неотъемлемой составляющей образования современного человека. Овладение этими технологиями в той или иной мере оказывает влияние на социализацию, а также успешность в профессиональной деятельности.

Условия информационного общества требуют от каждого участника способность критического суждения и всестороннего анализа потребляемой информации, которые сложно представить себе без использования средств информационных технологий на всех ее этапах. Отсутствие необходимых знаний и умений в области применения продуктов информационно-коммуникационных технологий, навыков работы с информационными потоками, способностей эффективно осваивать новые средства коммуникации и технологии не только ограничивают профессиональное развитие и рост специалиста, но и могут привести к негативным последствиям. Самыми яркими примерами могут быть следующие: возможность стать жертвой финансовых мошенников, использующих как персональные данные так и технические приемы и средства совершения преступных действий; заражение персонального компьютера или мобильных коммуникационных устройств вредоносным программным обеспечением с последующим вымогательством, угрозами распространения конфиденциальной информации или нарушения работоспособности и выходом из строя самого технического устройства; информационное воздействие на личность и сообщества через различные информационные ресурсы в рамках ведения информационной борьбы между государствами, политическими игроками или крупными корпорациями и т.д.

Задачи, определенные в Концепции национальной безопасности РФ [1], по обеспечению информационной безопасности лишь подчеркивают значимость необходимости формирования и развития ИКТ-компетенции у всех категорий граждан.

Возвращаясь к вопросу выделения компетенций по их значимости стоит упомянуть, что существует несколько их классификаций.

Так, Хутмахер, выступая в рамках своего доклада в Берне, выделил пять ключевых компетенций:

– «политические и социальные;
– компетенции, связанные с жизнью в поликультурном обществе;
– компетенции, относящиеся к владению устной и письменной коммуникацией;
– компетенции, связанные с информатизацией общества, владение этими технологиями, понимание их применения, слабых и сильных сторон и способов, критическое суждение в отношении информации, распространяемой масс-медийными средствами и рекламой;
– компетенции, связанные с самообразованием» [2].

Отечественный ученый А.В. Хуторской приводит следующий набор ключевых компетенций:
– «ценностно-смысловые компетенции;
– общекультурные компетенции;
– учебно-познавательные компетенции;
– информационные компетенции, являющиеся совокупностью навыков деятельности в окружающем мире, в образовательных областях и учебных предметах, по отношению к информации. Владение современными информационными технологиями и средствами информации, анализ, поиск, отбор, а также передача, сохранение и преобразование необходимой информации;
– социально-трудовые компетенции;
– коммуникативные компетенции;
– компетенции, характеризующие личностное самосовершенствование» [3].

В обоих случаях компетенции, напрямую указывающие на владение информационно-коммуникационными технологиями, выделены в отдельный блок. Ключевыми же компетенциями признаны те компетенции, которые обеспечивают нормальную жизнедеятельность человека в социуме и обладают признаками надпредметности и многофункциональности [4], и стоят выше профессиональных или базовых.

Учитывая анализ зарубежных и отечественных моделей образования и проводя аналогию с делением на группы компетенций в ФГОС ВО, можно представить следующие блоки компетенций:
– ключевые или общекультурные (в новых ФГОС ВО 3++ это универсальные), в которые входят все необходимые умения и качества, способности человека для его успешной социализации;
– базовые или общепрофессиональные компетенции, необходимые специалисту для деятельности в профессиональной сфере;
– профессионально-специализированные, профессиональные (в случае силовых структур это военно-профессиональные) компетенции, учитывающие специфику профессиональной деятельности, надпредметной сферы деятельности.

В связи с указанной актуальностью, были рассмотрены ФГОС ВО по специальности 40.05.01 Правовое обеспечение национальной безопасности и 37.05.02 Психология служебной деятельности, которые лежат в основе образовательной деятельности ряда образовательных организаций силовых структур. Сравнительный анализ утвержденных ФГОС ВО и ранее действующих по указанным специальностям показал, что такая значимая компетенция как способность работать с различными информационными ресурсами и технологиями, применять методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации не была учтена в явной форме при разработке универсальных компетенций. Можно сделать предположение, что скорее всего ИКТ-компетенция была отнесена к праву определения самой образовательной организацией в рамках описания профессиональных компетенций. Однако такой подход создает вариативность дисциплин и при действии различных условий, в том числе чисто бюрократических, дисциплины информационного профиля могут быть ущемлены в объеме зачетных единиц или полностью исключены. (как яркий пример, увеличение Передполагать, что ИКТ-компетенция будет сформирована в рамках получения среднего общего образования было бы неверно, так как на этом уровне образования возможно лишь получить начальный уровень сформированности компетенции, не позволяющий вести успешную жизнедеятельность в информационном обществе, свободно использовать информационные технологии.

Другой подход к определению места ИКТ-компетенции в новых ФГОС ВО заключается в интеграции указанной компетентности в одну или несколько групп категорий указанных универсальных компетенций. В таком случае, такими группами могут быть: системное и критическое мышление, разработка и реализация проектов, а для категорий общепрофессиональных компетенций (на основе анализируемых ФГОС ВО) ими могут выступать: правотворческая и правоприменительная деятельность, экспертно-диагностическая деятельность, организационно-управленческая деятельность.

В заключении стоит отметить, что ИКТ-компетенция имеет характеристики надпредметности и универсальности и такое существенное снижение значимости (исключение из категорий универсальных компетенций) вызывает обеспокоенность и возможно будет иметь определенные последствия для ее формирования и развития. Также стоит отметить, что в сопровождающих нормативно-правовых документах по прежнему четко не сформулированы требования к методам, алгоритмам и критериям определения уровней сформированности компетенций и их индикаторов.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Концепции национальной безопасности Российской Федерации [Электронный ресурс]: [указ Президента РФ от 17.12.1997 № 1300 (ред. от 10.01.2000)]. – Электрон. текстовые дан. – 2000. – Режим доступа: http://base.garant.ru/3974153/ (дата обращения: 21.08.2020 г.).

2. Hutmacher, W. Key competencies for Europe [Электронный ресурс]: Report of the Symposium Berne, Switzezland 27–30 March, 1996. Council for Cultural Co-operation (CDCC) / Hutmacher W. – Электрон. текстовые дан. – Bern, 1996. – Режим доступа: https://files.eric.ed.gov/fulltext/ED407717.pdf (дата обращения: 20.08.2020 г.).
3. Хуторской, А.В. Технология проектирования ключевых и предметных компетенции [Электронный ресурс] / А.В. Хуторской // Эйдос. – Электрон. журн. – 2005. – № 4. – Режим доступа: http://www.eidos.ru/journal/2005/1212.htm (дата обращения: 11.08.2020 г).
4. Совет Европы: Симпозиум по теме «Ключевые компетенции для Европы»: доклад DECS/SC/Sec (96) 43 / Совет по культурному сотрудничеству (CDCC). Среднее образование для Европы. – Берн, 1996. – 72 с.

УДК 004.056.5

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БОРЬБЫ

Ефимова Анна Борисовна, Воронов Сергей Алексеевич
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации,
Летчика Пилютова, ул., 1, г. Санкт-Петербург, 198206, Россия
e-mail: abefimova020770@mail.ru, Voronov-sci@mail.ru

Аннотация. Рассматривается вопрос защиты интересов России в информационной сфере. Проводится анализ особенности информационной войны, состоящей в воздействие на массовое сознание, и что то сегодня акцент необходимо делать на информационное превосходство.

Ключевые слова: информационная война, информационная цивилизация, процесс идентификации, пропаганда, глобальные информационные сети.

ON THE ISSUE OF INFORMATION SECURITY IN THE SPHERE OF INFORMATION STRUGGLE

Efimova Anna, Voronov Sergey
Saint Petersburg military order of Zhukov Institute of the national guard of the Russian Federation,
Pilot Pilyutov str., 1, Saint Petersburg, 198206, Russia
e-mail: abefimova020770@mail.ru, Voronov-sci@mail.ru

Abstract. The issue of protecting Russia's interests in the information sphere is being considered. The analysis of the features of the information war, which consists in the impact on the mass consciousness, and that today the emphasis should be placed on information superiority.

Keyword: Information warfare, information civilization, the process of identification, advocacy, global information network.

Неявная война против России идет уже очень давно и очень успешно. Конечно же, не на полях сражений, где русские всегда были сильнее, а там, где Запад всегда выигрывал и пока продолжает выигрывать – в информационных войнах. Западный мир уже давно научился лучше всех вести информационную войну. Удар наносится по тому месту, которое пока никому не приходит в голову защищать: умы и сознание людей.

«Информационная война» – новомодное словосочетание или вполне определенное понятие? Сам термин обязан своим происхождением военным и обозначает жесткую и опасную деятельность, но не связанную с реальными кровопролитными и разрушительными боевыми действиями. Военные эксперты, разрабатывающие доктрину информационной войны, отчетливо представляют себе отдельные ее грани: это штабная война, электронная война, психологические операции и так далее. Все эти действия постоянно видоизменяются с возрастающей ролью самой информации.

Любая война сопровождается массовой пропагандой и воздействием на человеческое сознание только ради того, чтобы скрыть тот факт, что одна из воющих сторон получает от войны огромную прибыль. Можно ли вообще рассматривать информацию в качестве оружия? Сегодня, многие из нас имеют доступ практически к любой информации, поэтому она становится вполне весомым средством борьбы. Информационная война, с одной стороны, это атака на информацию или атака на кого-то с помощью распространения информации. С другой стороны, информационную войну можно также рассматривать в качестве каких-либо действий по защите важной информации. Давно известно: «Кто владеет информацией – тот владеет миром». Важная особенность информационной войны в том, что это всегда воздействие на массовое сознание: нужно быстро воздействовать на всех и ради этого любые средства хороши. Информация уже давно стала главным, самым дорогим товаром и грозным оружием. Информационные баталии обязательно сопровождают реальные войны и успехи в них, зачастую, играют большую роль, чем победы на фронтах. Еще чаще они используются, как самостоятельные кампании в политике, бизнесе, и, даже, межличностных отношениях [1].

Информационные войны строятся на стратегии резонанса, когда одно сообщение в состоянии взбудоражить все общество. Если классические науки сориентированы на процессы сбора и анализа информации, то в случае информационных войн преобладают процессы распространения информации, различные варианты создания благоприятных контекстов для успешного ее проведения. Для изучения этих процессов необходимо знание теории коммуникации, социальной психологии, социологии. Современные государства хорошо понимают значимость информационной составляющей, особенно если это касается военных действий. Чем больше некая страна говорит об агрессивности соседей, тем существует большая вероятность, что она проецирует собственные агрессивные ощущения и намерения на других. Процесс идентификации заставляет сближаться с другим, а процесс компенсации заставляет гиперболизировать некоторые характеристики, чтобы закрыть собственные

ощущаемые недостатки. Например, небольшая страна может существенно переписывать свое место в мировой истории. Информационное воздействие представляет собой настолько тонкий механизм, что элемент творчества в поиске путей воздействия оказывается достаточно высоким и очень эффективным. На всякое действие находится свое противодействие и для информационных войн оно имеет такую же древнюю историю, как и сама информационная агрессия. И если раньше основной акцент в таком противодействии делался на репрессивных мерах (запрет, уничтожение, изъятие), то сегодня акцент делается на информационное превосходство.

Пока будет существовать биполярный мир, информационные войны останутся его неотъемлемым элементом в политике. К ним относятся, например, войны компроматов, которые стали приметной составляющей политических игр. Для одной из сторон такая война всегда идет под знаменами справедливости. Над производством и распространением информационных атак на Западе работают целые государственные управления, по своему масштабу и влиянию не сильно уступающие официальным спецслужбам. Они формулируют выгодные своей стране мифы, способствуют их распространению и оказывают поддержку тем, кто, в силу идеологических или финансовых аргументов, их ретранслирует. Они выстраивают свои тезисы в единые, внешне вполне логично выглядящие сюжеты, и пытаются, как можно более глубоко интегрировать их в общественную «повестку дня» атакуемого государства [2].

Сегодня для потенциальных объектов информационного нападения ситуация с каждым днем усложняется развитием Глобальных информационных сетей, и, в первую очередь, – Интернет. За несколько последних лет Интернет стал ведущим коммуникационным каналом, вытеснив с лидирующих позиций привычные средства массовой информации и стал основным инструментом распространения негатива и информационной агрессии. Практическая бесконтрольность, легкость размещения любой информации в Сети, реальная анонимность источника или инициатора атаки, глобальный охват получателей и высокая скорость распространения, позволяют вести широкомасштабные информационные войны при минимальных затратах, в сравнении с использованием традиционных средств коммуникации. Зачастую, к отражению информационных нападений объекты оказываются не подготовленными. Не следует быстрых ответных действий, и информация распространяется сама собой уже силами пользователей Интернет. В процессе распространения, таким образом, информация обрастает новыми «фактами» и «подробностями». Дело сделано, цель без особых усилий достигнута. Целями же информационных войн и в реальном и в виртуальном пространстве является, как правило, изменение имиджа объекта нападения таким образом, что бы нанести очень серьезный урон, часто с необратимыми последствиями. Объектом информационной атаки может стать кто и что угодно: государство, юридическое, физическое лицо. Иногда цель – это побуждение объекта к выгодному для нападающего действию, или наоборот бездействию, или же его полная (частичная) дестабилизация, парализация. В ближайшем будущем на государственном уровне придется разрабатывать политику оборонительных информационных действий, или останется мало шансов победить. Вся концепция боевых действий и ведения войн основана на идее национального суверенитета. Отличительной особенностью информационных действий является то, что они сметают эти барьеры [3].

К чему же нужно стремиться в данном виде противоборства? Возможно к созданию глобальной информационно - ударной системы страны и вооруженных сил, которая будет способна контролировать состояние и функционирование вооруженных сил и группировок противника и снижать их эффективность. В настоящее время информационная война может вестись как самостоятельно, так и является неотъемлемым элементом всех остальных форм борьбы. И если целью войны становиться не уничтожение, а управление при минимальном насилии и кровопролитии, что на первый взгляд кажется лучшим, но при более детальном рассмотрении это может оказаться весьма опасным. Ведь именно управление мировыми информационными потоками в своих целях – основная задача информационной войны [4].

У России, как одной из самых образованных стран в мире, есть все шансы для процветания. Необходимо только серьезно подойти к проблеме информационной безопасности. Всегда считалось, что путем тотальной секретности и различными ограничениями можно обеспечить информационную безопасность страны. Российское государство начинает серьезно и ответственно подходить к проблеме определения и отстаивания жизненно важных интересов, реальных и потенциальных угроз в информационной сфере. Успешная информационная компания, проведенная на оперативном уровне, будет поддерживать стратегические цели, лишая возможности врага принимать решения оперативно и эффективно.

СПИСОК ЛИТЕРАТУРЫ

1. Бобонец С.А., Потапова Л.С., Ципанович А.В. Основные способы стенографии для обеспечения информационной безопасности в деятельности ОВД/В сборнике: Региональная информатика и информационная безопасность. Сборник трудов. 2019. – С. 164-166.
2. Ярмоленко Н.В. Аспекты информационно-психологической защиты личности/В сборнике: Региональная информатика и информационная безопасность. Сборник трудов. 2019. – С. 209-211.
3. Костюк А.В., Бабошин В.А. Угрозы информационной безопасности личности в современном обществе/В сборнике: Развитие системы подготовки военных специалистов в войсках национальной гвардии Российской Федерации: традиции и современность. Сборник научных трудов. Под общей редакцией В.Ф. Купавского. Пермь, 2018. – С. 161-165.
4. Лободина А.С. Информационная безопасность / А.С. Лободина, В.В. Ермолаева. – Текст: непосредственный // Молодой ученый. – 2017.

УДК 004.9

ОСОБЕННОСТИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ СТУДЕНТОВ МОДЕЛИРОВАНИЮ РАСЧЁТОВ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ НА ЭВМ

Гуревич Татьяна Михайловна
Костромская государственная сельскохозяйственная академия
Учебный городок, 34 пос. Караваево, Кострома, 156530, Россия
e-mail: char1943@mail.ru

Аннотация. Рассматривается опыт дистанционного обучения студентов, обучающихся по программе магистратуры моделированию расчётов строительных конструкций на ЭВМ.

Ключевые слова: методика обучения; расчётная модель; приёмы моделирования; теоретическое армирование.

THE FEATURES OF REMOTE TRAINING OF STUDENTS-MAGISTRANTOV TO MODELING OF CALCULATIONS OF BUILDING CONSTRUCTIONS ON THE COMPUTER

Gurevich Tatiana
Kostroma state agricultural academy
Educational town, 34 settlements of Karavayevo, Kostroma, 156530, Russia
e-mail: char1943@mail.ru

Absract. The experience of remote training of students-magistrantov to modeling of calculations of building constructions on the COMPUTER is considered.

Keywords: training technique; calculating model; ways of modeling; theoretical reinforcing.

Практические занятия со студентами по моделированию расчётов строительных конструкций обычно проводятся в аудитории, оснащённой персональными компьютерами и большим экраном. При этом используются лицензионные программы – универсальные программные комплексы. Студенты, формируя свою модель, могут проконсультироваться с преподавателем. При выполнении контрольных заданий преподаватель имеет возможность следить за работой каждого студента.

Необходимость работать дистанционно выдвинула свои требования к методике обучения. Оснащённость программными средствами у всех студентов разная, то есть используются различные версии и релизы не лицензионных программ. Уже этот факт создаёт определённые трудности. Тем не менее, процесс дистанционного обучения состоялся, и большинство студентов успешно его прошли. Первое задание по дисциплине «Моделирование расчетов строительных конструкций на ЭВМ» состояло в формировании модели поперечной рамы с фермой из замкнутых гнутосварных профилей с целью проверочного расчёта всех элементов. Второе – формирование модели покрытия с пространственной плитой из круглых труб типа «КИСЛОВОДСК». Студенты должны были прислать на проверку свои модели и при необходимости скорректировать их согласно замечаниям преподавателя. Кроме того, были разработаны вопросы по этим моделям, контролирующие самостоятельность работы студента, освоение приёмов моделирования, знание критериев оценки несущей способности элементов согласно [1]. Первые два задания были выполнены большей частью студентов довольно успешно.

Третье задание состояло в формирование модели ребристо-кольцевого купола и подборе профилей несущих элементов. В задании поэтапно описан процесс создания модели, приведены иллюстрации, даны ссылки на нормативную литературу. Особое внимание уделено правильному закреплению купола и формированию загружений. Последующие задания включали в себя формирование моделей железобетонных конструкций с целью вычисления теоретической арматуры в балках, колоннах и плитах согласно [2]. Особую трудность представляла задача по моделированию многоэтажного железобетонного каркаса с основанием в виде фундаментной плиты. Обучить дистанционно формировать такие модели практически невозможно, поэтому студентам были предложены три готовых модели многоэтажного железобетонного каркаса и вопросы по анализу этих моделей. Студенты должны были произвести расчёт этих моделей, прислать на проверку иллюстрации результатов расчёта и ответить на вопросы. Задание вызвало затруднения у большинства студентов.

Создание расчётной модели сложной конструкции является творческой задачей, многовариантной. Вид модели зависит от цели расчёта [3]. Одна и та же конструкция может быть смоделирована по-разному в зависимости от поставленной задачи. Необходимо общение преподавателя и студента, их совместная работа, что при дистанционном обучении осуществить пока не удаётся.

Анализируя опыт дистанционной работы со студентами по приведённым выше дисциплинам, можно сделать вывод о существенных минусах такой подготовки. Процесс обучения приводит к увеличению затрат времени и преподавателем, и студентами в несколько раз при значительном снижении эффективности обучения.

СПИСОК ЛИТЕРАТУРЫ

1. СП 16.13330.2011. Стальные конструкции. – М.: Стандартинформ, 2019.
2. СП 63.13330.2018. Бетонные и железобетонные конструкции. – М.: Минстрой России, 2018.
3. А.С. Городецкий, И.Д. Евзеров «Компьютерные модели конструкций» – Москва, Издательство Ассоциации строительных вузов, 2009. – 360 с.

УДК 004.056.5

ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОТИВОДЕЙСТВИИ ИДЕОЛОГИИ ТЕРРОРИЗМА

Ефимова Анна Борисовна, Соболенко Илья Александрович
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации,
Летчика Пилютова, ул., 1, г. Санкт-Петербург, 198206, Россия
e-mail: abefimova020770@mail.ru, Sobolenko_ilya@mail.ru

Аннотация. Рассматривается вопрос защиты интересов России в информационной сфере противодействия терроризму. Проводится анализ особенности информационной войны, состоящей в воздействие на массовое сознание, и что то сегодня акцент необходимо делать на информационное превосходство.

Ключевые слова: информационные технологии, информационное противодействие, процесс идентификации, пропаганда, информационный терроризм.

LEGAL ASPECTS APPLICATION OF INFORMATION TECHNOLOGIES IN COUNTERING THE IDEOLOGY OF TERRORISM

Efimova Anna, Sobolenko Ilya
Saint Petersburg military order of Zhukov Institute of the national guard of the Russian Federation,
Pilot Pilyutov str., 1, Saint Petersburg, 198206, Russia
e-mail: abefimova020770@mail.ru, Sobolenko_ilya@mail.ru

Absract. The issue of protecting Russia's interests in the information sphere of countering terrorism is being considered. The analysis of the features of the information war, which consists in the impact on the mass consciousness, and that today the emphasis should be placed on information superiority.

Keyword: Information technologies, information counteraction, identification process, propaganda, information terrorism.

В настоящее время информационные технологии позволяют управлять огромными массивами информации, тем самым открывая неисчислимые возможности. Возможности, которые могут быть использованы как в созидательных, так и в разрушительных целях.

В свете своей востребованности и практически безграничных перспектив развития, информационные технологии (ИТ) приобретают сегодня не только колоссальную ценность, но и тревожную неоднозначность.

На нынешнем этапе развития ИТ представляют собой целый «комплекс взаимосвязанных наук и методов организации и взаимодействия с людьми и производственным оборудованием, его практическое применение, а также связанные со всем этим социальные, экономические и культурные проблемы».

ИТ включают в себя всевозможные технологии сбора и анализа данных (различные варианты сенсоров), объединяют информацию из огромного количества различных источников, проводят аналитическую работу, прогнозируют, моделируют и выполняют множество других функций [1].

При этом, как уже было сказано выше, многие из ресурсов современных ИТ можно направить не только на повышение качества нашей жизни. Одновременно они являют собой благоприятную почву для расцвета противоправной деятельности, в том числе и террористической.

По мнению специалистов, именно в информационной сфере происходит наибольшее количество «террористических мутаций». Что, в свою очередь, требует постоянного информационного противодействия, опирающегося на новейшие разработки в сфере информационных технологий.

Однако, само понятие «информационное противодействие» вплоть до настоящего времени не получило чёткого официального определения. Информационный аспект борьбы с терроризмом предполагает преимущественно реализацию мер защитного характера.

Терроризм – постоянный спутник человечества, который относится к числу самых опасных и трудно прогнозируемых явлений современности, приобретающих все более разнообразные формы и угрожающие масштабы. Террористические акты приносят массовые человеческие жертвы, оказывают сильное психологическое давление на большие массы людей, влекут разрушение материальных и духовных ценностей, не поддающихся порой восстановлению, сеют вражду между государствами, провоцируют войны, недоверие и ненависть между социальными и национальными группами, которые иногда невозможно преодолеть в течение жизни целого поколения.

Некоторые источники определяют информационное противодействие терроризму как «комплекс мероприятий по поражению информационного ресурса террористических организаций, блокированию осуществляемых ими информационных процессов и внедрению дезинформации на всех этапах их реализации».

В содержательном плане информационное противодействие терроризму предполагает воплощение крупномасштабного и продолжительного комплекса мер, в том числе и непрерывную деятельность по противодействию идеологии терроризма и экстремизма.

Противодействие идеологии терроризма представляет собой один из множества подходов предупреждения терроризма, в рамках которого применяются ИТ.

Противодействие идеологии терроризма включает в себя:

– работу по разъяснению населению всей деструктивности и античеловечености терроризма, созданию и внедрению в общественное сознание образа террориста как антигероя;

– демонстрацию разрушительных последствий террористической деятельности;

– формирование установки на неотвратимость разоблачения и наказания за участие в террористической деятельности;

– воспитание у населения законопослушности и уважительного отношения к представителям органов власти;

– работу по внедрению в общественное сознание положительного отношения ко всему многообразию культур, формированию навыков кросскультурного взаимодействия;

– работу по поддержанию деятелей творческих профессий, создающих произведения, положительно влияющие на формирование антитеррористического сознания в обществе.

Информационная работа с населением в сфере противодействия терроризму должна вестись в направлении повышения бдительности населения, формирования доверия к действиям государственных структур, воспитанию гражданской сознательности.

В связи с тем, что в настоящее время наиболее используемой и востребованной системой сообщения является Интернет, на первый план выходит задача организации непрекращающейся оценки и анализа всего веб-контента.

В настоящее время выделяют восемь различных способов использования сети Интернет в террористических целях, а именно, использование глобальной сети для сбора информации, пропаганды, отправки закодированных сообщений и т.д.

Интернет представляет собой благодатное поле для деятельности террористических организаций. И большое содействие этому оказывают такие особенности сети Интернет как свобода доступа, низкий уровень цензуры, многомиллионные аудитории, возможность анонимности, скорость передачи информации и дешевизна.

В настоящее время в качестве одного из перспективных направлений противодействия распространению идей терроризма предлагается «силовое вытеснение» из легального киберпространства веб-ресурсов, носящих радикальный, экстремистский характер. В этот процесс должны быть вовлечены «не только государственные силы Российской Федерации, но и антивирусные компании, спам-регуляторы, иностранные киберполицейские организации путем технического использования особенностей экономической модели западных Интернет-провайдеров» [2].

Однако, мировая практика показывает, что силовой подход к решению проблем в сфере противодействия терроризму не устраняет проблемы, поскольку такой подход не способен, да и не призван устранять причины, порождающие их.

Приходится признать, что в настоящее время информационные технологии используются преимущественно в целях выявления и пресечения террористической деятельности. И в гораздо меньшей степени ориентированы на профилактику идеологии терроризма, несмотря на то, что необходимость особой концентрации внимания на применении ИТ в направлении ослабления и искоренения причин, порождающих идеологию терроризма, очевидна. Одной из таких причин является экстремистское мировоззрение, что подтверждается всё большим количеством научных исследований, проводимых как на территории Российской Федерации, так и других государств.

В настоящее время имеется достаточно много нормативных документов, стандартов, рекомендаций, ведомственных норм и правил, в которых в той или иной мере рассматриваются вопросы комплексного подхода к безопасности. Существует множество организаций, которые предлагают свои собственные методы в построении комплексных систем безопасности. Все эти подходы имеют много общего, однако есть в них большое количество различий и особенностей, а зачастую и противоречий, что затрудняет их применение на практике

На наш взгляд, удачное и лаконичное определение экстремизму представлено в одном из изданий института военной истории Министерства обороны Российской Федерации: «экстремизм как таковой является формой радикального отрицания существующих общественных норм и правил в государстве со стороны отдельных лиц, групп и слоёв населения».

Экстремистское мировоззрение не просто толкает человека к крайностям в суждениях и жесткому разделению мира на «чёрное» и «белое», но и формирует в нём сознание собственной непогрешимости и правоты. Более того, позволяет человеку принимать решения без размышлений о возможных последствиях, призывает его к решению любых проблем путями, не требующими никакой внутренней работы над собой для достижения значимого результата, формирует психологическую готовность для перехода от размышления к действию, требует революции, и по большому счёту отказывает обществу, ближнему своему, себе в способности к развитию. Такое мировоззрение является прочным фундаментом, на котором в последующем выстраивается вся идеология терроризма [3].

Терроризм является плодом экстремистского мировоззрения. Одни и те же обстоятельства, ситуации, действуя на людей, обладающих различным мировоззрением, приводят их к различным выводам и действиям.

Разные авторы, исследователи дают свои определения терроризма.

Некоторые зарубежные исследователи (У. Лакер, П.Уилкинс, Дж. Хардман, Б. Хоффман) определяют терроризм как «незаконное применение или угрозу использования насилия против лиц, чтобы принудить правительство выполнить политические или идеологические цели».

Несколько другие определения дают отечественные исследователи.

Так, Кожушко Е.П. определяет трактует терроризм как тактику политической борьбы, которая характеризуется применением идеологически обоснованного насилия.

Федеральный закон Российской Федерации от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» определяет терроризм как «идеологию насилия и практику воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий».

Идеология терроризма представляет собой всю совокупность идей и концепций, которые обосновывают, оправдывают и призывают к использованию насильственных путей для достижения политических, социальных и экономических целей, а также, формируют психологическую готовность и провоцируют к действиям в этом направлении.

Одной из важнейших задач террористической деятельности - через запугивание и причинение вреда, принудить действовать в интересах террористов. При этом, причинение вреда вовсе не выступает самоцелью. Целью, в данном случае, является достижение, распространение и наращивание влияния террористических организаций в мировом сообществе.

Не секрет, что в ряду наиболее уязвимых в плане подверженности экстремистским воззрениям является подростковая и молодёжная среда. В современных условиях частичной деилогизации общества, в силу своего максимализма, склонности к протестным реакциям, постоянной неудовлетворённости и, в то же время, беспечного отношения к жизни, наше подрастающее поколение становится не просто открытым для внедрения радикальных идей экстремизма, но, зачастую, активно их впитывает [4].

Современный Интернет – это не только уникальная информационная среда, но и источник многих угроз. Наибольшую опасность из них представляет различное вредоносное программное обеспечение: вирусы, «троянские кони», рекламные и шпионские утилиты, именно глобальная сеть стала основным каналом их распространения, а любой компьютер, подключенный к ней, подвергается постоянной опасности.

При построении информационной защиты в образовательном учреждении необходимо:

– разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных;

– сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т.д.

Следует уделить особое внимание процедуре передачи персональных данных третьим лицам.

27 июля 2006 года был принят Федеральный закон «О персональных данных» ФЗ-152 в соответствии с Конвенцией Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (ETS №108, 1981г), которую Россия ратифицировала в 2005 году.

Молодые люди нынешнего поколения значительную часть своего времени проводят в виртуальном мире, активно пользуясь достижениями в области информационных технологий, в первую очередь, Интернетом. Что, в свою очередь, открывает возможности с максимальной эффективностью использовать информационные технологии для формирования антиэкстремистского мировоззрения в молодёжной среде. Вследствие этого, применение современных информационных технологий в целях профилактики и противодействия идеологии терроризма должно иметь приоритетное значение.

СПИСОК ЛИТЕРАТУРЫ

1. Ефимова А.Б., Кайзер В.А., Титов А.Б. Информационные технологии в системе военного образования/ В сборнике: Неделя науки СПбПУ. Материалы научной конференции с международным участием. 2019. – С. 80-83.
2. Костюк А.В., Бобонец С.А., Примакин А.И. Подходы к обеспечению информационной безопасности электронного обучения/ Вестник Санкт-Петербургского университета МВД России. 2019. № 3 (83). – С. 181-187.
3. Ярмоленко Н.В. Аспекты информационно-психологической защиты личности/ В сборнике: Региональная информатика и информационная безопасность. Сборник трудов. 2019. – С. 209-211.
4. Бережнова Л.Н., Белоус О.И., Воронов С.А., Гнездилов В.А., Гупалов М.М., Коновалова Л.И., Поминова О.Л., Сивак А.Н., Сидоров И.А., Тимочкин А.С. Првокационное воздействие на человека в информационном пространстве/ Монография, СПВИ ВНГ РФ, Под общ. ред. Л.Н. Бережновой. Санкт-Петербург, 2019.

УДК 004.4

РАЗРАБОТКА МЕТОДИКИ ПОИСКА ИНФОРМАЦИИ ПО ЧЕЛОВЕКУ В СОЦИАЛЬНЫХ СЕТЯХ

Иванов Даниил Дмитриевич, Чудаков Олег Евгеньевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: danl98@yandex.ru, oechuda@yandex.ru

Аннотация. В статье рассматривается методика, в том числе способы поиска информации по человеку, её анализ, подготовка к восприятию и использование. Статья содержит сведения о данных, которые объект изучения оставляет при времяпрепровождении в социальных сетях. Также затронут вопрос о рамках этичного поиска открытой информации OSINT.

Ключевые слова: социальные сети; сбор сведений; поиск информации; анализ данных; поиск по открытым источникам; методы поиска; сбор сведений; методика.

DEVELOPMENT OF A METHOD FOR SEARCHING INFORMATION ON A PERSON IN SOCIAL NETWORKS

Ivanov Daniil, Chudakov Oleg
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: danl98@yandex.ru, oechuda@yandex.ru

Abstract. The article discusses the technique, including methods of searching for information on a person, its analysis, preparation for perception and use. The article contains information about the data that the object of study leaves when spending time on social networks. It also touches on the OSINT framework for ethical search for public information.

Keywords: social networks; information gathering; information search; data analysis; open source search; search methods; data collection; methodology.

В современном мире процесс цифровизации с каждым годом затрагивает всё больше сфер и внедряется в жизнь каждого. Так в мире интернетом пользуется 60% процентов населения, а в России 81% [5]. В связи с этим мы можем говорить об огромной популярности социальных сетей, почти каждый пользователь глобальной сети проводит достаточно большое время получая информацию, общаясь с людьми, выкладывая фотографии или оценивая их у друзей. Россияне проводят более семи часов в интернете, что говорит о симбиозе информационных технологий и повседневной жизни людей.

Беря во внимание тот факт, что любой человек проводя значительную часть времени в интернете, в том числе в социальных сетях, оставляет информацию о себе, помимо цифрового следа, то есть совокупности данных, которые пользователь генерирует во время пребывания в цифровом пространстве, ещё и сам умышлено рассказывает о себе – геометками, фотографиями, личной информацией.

В связи с этим, в новом столетии появился такой способ получения информации о людях, как OSINT (Open Source INTelligence) – поиск, сбор и анализ информации, полученной из общедоступных источников. При этом руководящим документом является Конституция РФ [1], а именно статья 29, ч. 4 «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом». Часто это может называться, как конкурентная разведка, за счёт того, что сведения(информация) добываются из открытых источников. Исторически своё начало Open-source intelligence берёт от создания Службы внешнего Broadcast Monitoring (FBMS), то есть агентства, отвечающего за мониторинг зарубежных передач.

Помимо ряда общедоступных источников, среди которых – сайты средств массовой информации, общедоступные данные правительства, научные публикации, сервисы оказывающие услуги, коммерческие данные, важным являются социальные сети (vk.com, Facebook, Instagram, Мой.Мир, LinkedIn, Одноклассники, Twitter, etc.) [7]. Ведь это огромные базы данных, содержащие множество персональной информации о людях, их личные данные, фотографии, интересы, увлечения. Данную информацию можно получать, благодаря непосредственной работой с этими данными, так и с помощью специальных сервисов и программного обеспечения, в том числе бот-программ [4].

Данная информация очень полезна, как сотрудникам оперативных подразделений, так и следственных. Благодаря ей можно ускорить поиск человека, совершившего преступление или получить новые знания о деле.

Сам цикл с поиском и анализом информации о человеке из социальных сетей или методику можно представить следующим образом.

На первом этапе планирования, необходимо понять, что требуется получить, выдвигаются гипотезы и делаются предположения. Кроме того, требуется понять какие источники будут задействованы и какие средства необходимы, каким образом эта информация будет использоваться в дальнейшем и какие средства требуются для её осуществления.

Следующим этапом является сбор информации, который в свою очередь наиболее трудоёмкий. При наличии небольшой информации, стоит её использовать максимально полно. То есть, имея фотографию человека, являющегося объектом исследования, информацию надо искать во всех социальных сетях с помощью различных сервисов, таких как поиск по изображению от Яндекс (yandex.ru/images/), Google (https://www.google.ru/imghp) и более узконаправленные Findclone (findclone.ru/) для vk.com и другие. Среди полезных сервисов можно выделить – 220vk (https://220vk.com/), благодаря которому мы можем найти корреляцию информации между людьми, а именно получить различные метрики, такие как связи между пользователями и структурные дыры. Существует и программа для сбора геолокационной информации из многих социальных сетей (http://www.geocreepy.com/), которая представляется в виде отметок на Google картах, ведь часто пользователи, загружая свои изображения на медиаресурс прикрепляет, то место где оно было сделано. Почти у каждого пользователя интернет есть свой уникальный логин (никнейм), который используется на различных ресурсах, чтобы можно было использовать и эту информацию, стоит воспользоваться сервисом namechk (https://namechk.com/). Применяются и поисковые запросы для поиска информации, где после имеющегося словосочетания (ФИО, логин, дата рождения etc) дописывается site:*.*, где вместо символа * – указывается информационный ресурс, который необходим и домен.

Вне зависимости какую информацию мы имеем, несложно получить другие, интересующие нас сведения с помощью косвенных данных. Под косвенными сведениями стоит понимать информацию, содержащую общую,

нецелевую информацию, такую как примерную область проживания, дату и месяц рождения, возможные интересы и другое.

Анализ полученной информации – это третий этап, на котором полученные данные систематизируются, извлекаются метаданные (информация о другой информации, либо данные, относящиеся к вспомогательной информации об объекте), ненужные сведения отбрасываются, а с необходимыми идёт дальнейшая работа по представлению данных [3].

Зачастую данные представляются в графическом виде для более удобного и понятного восприятия и нахождения связей [2]. Происходит создание карты человека на основе проанализированной информации и подготовка её для использования. Этому могут поспособствовать различные сервисы, такие как Xmind (https://www.xmind.net/), Coggle.it (https://coggle.it/), также для этого подойдёт Excel для простейшей визуализации данных.

Заканчивается цикл сбора информации на использовании этих сведений, тут субъектом, осуществляющим поиск, принимается решение – была ли выполнена поставленная задача или были полученные новые сведения для дальнейшего продолжения поиска. Формируются выводы, а также пересматривается дорожная карта, для понимания правильности поиска информации.

Получить можно практически любую информацию о человеке, оставленной им за многие годы [6].

Построение собственной методики по поиску информации о человеке складывается разнообразно. Нельзя сказать, что существуют неправильные пути, так как именно в этой работе нужно проверять максимально все возможные варианты и использовать все варианты. Исходя из увлечений объекта можно получить те группы в социальных сетях, в которых он состоит тем самым его найдя. По контактной информации, имея номер телефона реально получить профиль на Avito (https://www.avito.ru/), где легко найти геопозицию, если продавец оставил информацию об этом у своего товара. Имея фамилию, имя и отчество с датой рождения – находим человека и/или фотографии человека. Таких путей множество, но главным фактором является упорство и внимательность субъекта, осуществляющего поиск. Наиболее правильным решением будет автоматизация процесса сбора и обработки информации о человеке с помощью API (application programming interface) социальных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской федерации от 12.12.1993г (принята всенародным голосованием 12.12.1993) (с учетом поправок от 14.03.2020 № 1-ФКЗ).
2. Батура Т.В., Модели и методы анализа социальных сетей Электронный ресурс]. URL: https://cyberleninka.ru/article/n/modeli-i-metody-analiza-kompyuternyh-sotsialnyh-setey/viewer (дата обращения: 18.07.2020).
3. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети интернет // Мониторинг правоприменения №1 (18) – 2016.
4. Смирнова О.С., Петров А.И., Бабийчук Г.А. Основные методы анализа, используемые при исследовании социальных сетей // Современные информационные технологии и ИТ-образование 2016 [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/osnovnye-metody-analiza-ispolzuemye-pri-issledovanii-sotsialnyh-setey/viewer (дата обращения: 18.07.2020).
5. Вся статистика интернета на 2020 год — цифры и тренды в мире и в России [Электронный ресурс] // web-canape — URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения: 17.07.20).
6. Как собрать досье на человека через интернет [Электронный ресурс] // cryptoworld — URL: https://cryptoworld.su/kak-sobrat-dose-na-cheloveka-cherez-internet/ (дата обращения: 17.07.20).
7. С открытым исходным кодом разведки – Open-source intelligence [Электронный ресурс] // cryptoworld – URL: https://ru.qwe.wiki/wiki/Open-source_intelligence (дата обращения: 17.07.20).

УДК 004.056.5

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Игнатов Данил Юрьевич, Локнов Алексей Игоревич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: da.ignatoff@gmail.com, nfo_for_aleksey@mail.ru

Аннотация. Рассматриваются основные методы и средства защиты информации в системах электронного документооборота.

Ключевые слова: средства защиты информации, системы электронного документооборота.

METHODS AND MEANS OF INFORMATION SECURITY IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Ignatov Danil, Loknov Alexey
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
Letchika Pilyutova, st., 1, St. Petersburg, 198206, Russia
e-mail: da.ignatoff@gmail.com, nfo_for_aleksey@mail.ru

Abstract. The main methods and means of information security in electronic document management systems are considered.

Key words: information security tools, electronic document management systems

В связи с развитием информационных технологий стремительно внедряются системы электронного документооборота (СЭД). Переход к системам электронного документооборота приводит к необходимости уделять пристальное внимание вопросу информационной безопасности [1].

Перед созданием системы защиты необходимо провести детальный анализ процессов обработки, хранения и передачи информации в СЭД. Существует 3 типовых объектов защиты информации в СЭД [2]. Первый – сведения, содержащие коммерческую тайну; персональные данные; служебная тайна; общедоступная информация, целостность и доступность которой обеспечивает выполнение технологических процессов СЭД. Второй – носители информации: ключевые носители, съемные и встроенные в программно-аппаратные платформы накопители, системы хранения данных; программно-аппаратные платформы обработки, хранения, передачи и защиты информации; персонал СЭД: пользователь, технический персонал, ответственный за функционирование СЭД. Третий – информационные процессы, к которым можно отнести основные процессы электронного документооборота и вспомогательные процессы: процессы физической защиты оборудования, пожарной безопасности, организации пропускного и объектного режимов и т.п.

Угрозы безопасности информации в системе электронного документооборота можно классифицировать по мотивам: непреднамеренные (случайные) и преднамеренные (умышленные) [2]. К непреднамеренным относятся: стихийные бедствия, отказы и сбои оборудования и т.п. К преднамеренным – перехват данных, передаваемых по каналу связи (нарушение конфиденциальности); подмена авторства информации; хищение носителей информации паролей; использование недостатков ОС.

Источники угроз подразделяются на внешние и внутренние. Уменьшить отрицательное воздействие угроз информации можно с помощью специальных методов: организационных (организация физической защиты и охраны оборудования СЭД, подбор и работа с персоналом и т.п.); технических (скрытие сетевой структуры СЭД, шифрование информации, блокирование сетевых атак и т.п.); правовых (установление порядка использования и защиты информации, заключение соглашений о конфиденциальности с партнерами и контрагентами, заключение договоров на обработку персональных данных).

Эффективное использование средств защиты информации возможно только при условии их совместного применения в комплексе с вышеперечисленными методами защиты информации. Система защиты информации должна включать в себя процессы управления доступом – регистрация субъектов доступа, идентификация, аутентификация и авторизация. В случае выявления попыток получения информации несанкционированным путем должны срабатывать механизмы блокирования нарушителя.

Должны быть реализованы процессы межсетевого экранирования, фильтрация по IP-адресам, портам, сетевым протоколам. Кроме того, в современной системе защиты информации применяются системы реализации процессов обнаружения инцидентов информационной безопасности, обнаружения сетевых атак и иных форм вторжения в процессы функционирования СЭД.

При создании эффективной системы защиты информации необходимо учитывать то, что любая информационная система находится в состоянии развития.

СПИСОК ЛИТЕРАТУРЫ:

1. Бачило И.Л. Информационное право: учебник для академического бакалавриата. 5-е изд. перераб. и доп. – М.: Издательство Юрайт, 2017. – 416 с
2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – 586 с.

УДК 004.9

ПЕРСПЕКТИВА ПРИМЕНИЯ МЕТОДОВ OPENSOURCEINTELLIGENCEПРИ ОСУЩЕСТВЛЕНИИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Игнатов Данил Юрьевич, Филёва Дарья Алексеевна, Якушев Денис Игоревич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: da.ignatoff@gmail.com,filyova.daria@yandex.ru, d.i.ya@yandex.ru.

Аннотация. Рассматривается вопрос перспективы применения современных методов сбора информации и анализа разведданных на основе открытых источников в деятельности органов внутренних дел.

Ключевые слова:поиск информации;анализ данных;открытые источники;технология OSINT.

THE PROSPECT OF USING OPEN SOURCE INTELLIGENCE METHODS IN LAW ENFORCEMENT ACTIVITIES

Ignatov Danil, Fileva Darya, Yakushev Denis
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
LetchikaPilyutova, st., 1, St. Petersburg, 198206, Russia
e-mail: da.ignatoff@gmail.com, filyova.daria@yandex.ru, d.i.ya@yandex.ru.

Abstract. The article considers the prospects of applying modern methods of collecting information and analyzing intelligence based on open sources in the activities of internal affairs bodies.

Key words: information search; data analysis; open sources; OSINT technology.

Сейчас мы живем в эпоху, когда одним из важнейших ресурсов является информация. Каждый из нас ежедневно использует свой смартфон или иные гаджеты: для поиска информации в сети Интернет, для навигации в городе, для ведения социальных сетей, для оплаты покупок и т.д. Объединяет все эти действия то, что таким образом человек оставляет так называемый «цифровой след». Законопослушному гражданину стоит переживать только лишь за то, что эти данные могут попасть злоумышленникам, которые, в свою очередь, могут воспользоваться информацией на свое усмотрение. Но также стоит понимать, что потенциальный преступник редко отличается особой сообразительностью и зачастую, сам того не понимая, размещает о себе информацию в открытый доступ, например, в социальную сеть. Это может быть как личная информация, геолокация, социальные связи, так и иная информация, которая может оказать содействие в осуществлении правоохранительных функций.

Если верить словам аналитика ЦРУ Кена Шермана, сказанным им в 1947 году, то государство получает около 80% необходимой информации именно из открытых источников [1]. Немного позднее коллега Шермана, а именно руководитель Разведывательного управления министерства обороны США Самуэль Уилсон, утверждал, что всего 10% разведданных получают благодаря работе агентов, остальные 90% специалисты собирают из открытых источников [2]. Вполне возможно, что статистика для отчета была подкорректирована, но все же – разница значительная. На сегодняшний день нет подобных заявлений, но есть вероятность, что в эпоху стремительно развивающейся сети Интернет у сотрудников спецслужб и у обычных пользователей появилось куда больше возможностей по поиску информации – в частности, поиск по открытым источникам с помощью технологии OSINT.

OpenSourceIntelligence, илипростоOSINT – этотехнология поиска и анализа данных, собранных из открытых источников. К ним относятся газеты, сеть Интернет, книги, научные журналы, радиовещание, телевидение, правительственные отчеты, техническая документация, руководства и т.п.

Сегодня с помощью данной технологии частные детективы выполняют больше половины поставленных перед ними задач. Это одно из подтверждений того, что сотрудники ОВД также могут взять на вооружение подобную технологию при осуществлении своей деятельности. Также, в федеральном законодательстве закреплено положение о том, что полиция должна и обязана использовать в своей служебной деятельностисовременную информационно-телекоммуникационную структуру, информационные системы, передовые достижения науки и техники, а также системы связи [3].

Относительная общедоступность технологии OSINT дает возможность злоумышленникам представить полноценный портрет своей жертвы, выявить ее слабые места. Высокоорганизованное преступление начинается с начальной разведки, а первым этапом цифровой разведки является OSINT – пассивное извлечение информации в то время, когда жертва об этом даже не подозревает. Таким образом, злоумышленник с легкостью может разработать план своих действий и реализовать свой преступный замысел. Поэтому правоохранительные органы, обладая данной информацией, обязаны направить усилия на осуществление превентивных мер с целью предотвращения готовящихся или потенциально возможных преступлений.

Наверное, возникает вопрос – чем же отличается обычный поиск информации в сети Интернет от технологии OSINT? На этот счет в узких кругах существует высказывание – «большинство людей завершит поиск там, где для профессионалов он только начинается».

Самыми ценными источниками информации в сети Интернет следует считать различные сайты объявлений, торговые площадки, форумы, взломанные базы данных банковских клиентов, государственные реестры, а также социальные сети. Также можно воспользоваться IP-логгером, чтобы установить IP-адрес, просканировать порты, чтобы иметь представление, какие технологические устройства окружают объект исследования. Перед специалистом стоит задача – вычленить из общего «информационного шума» именно ту информацию, которая будет полезна.

Технология OSINT позволяет собирать данные, представленные в различных формах: текстовые файлы и документы, аудио- и видеофайлы, фотографии и картинки, анимация и т.д.

Поиск и аккумулирование информации является не самым сложным этапом в технологии OSINT. Далее перед специалистом стоит сложная задача – комплексныйи качественный анализа большого массива данных. Получение точных результатов для непрофессионала в целом становится сложной задачей. Могут помочь инструменты с открытым исходным кодом, которые могут работать одновременно. Они будут собирать для специалиста данные из доступных источников, оставляя ему только сравнительную и аналитическую работу.

В инструментарии технологии OSINT находится большое количество методов и механизмов для достижения желаемого результата поиска. Однако специалист должен понимать, что одни из них будут работать, другие – нет, все зависит от конкретной задачи и цели поиска. Первым шагом в OSINT является ответ на ряд вопросов: Что мне необходимо найти? В чем состоит цель поиска? Что из себя представляет моя цель? Как я буду проводить комплексный анализ полученных данных? После чего специалист определяется с источниками, в которых он будет искать нужную информацию, и непосредственно начинает поиск.

Многие популярные и полезные методы технологии OSINT доступны частным пользователям сети Интернет:

- сбор информации с помощью поисковых систем (Google, Яндекс, Yahoo, Bing, DuckDuckGoи др.);
- сбор информации и анализ данных социальных сетей (ВКонтакте, Instagram, Facebookи др.);
- поиск по картинкам и фотографиям через вышеупомянутые поисковые системы;

– использование спутниковых изображений и геолокаций для получения информации о географическом положении цели;

– поиск информации в мессенджерах, социальных сетях и на различных других сайтах при наличии контактного номера.

Сбор и анализ неструктурированной информации из различных источников – это обширная и трудоемкая работа, требующая усидчивости и аналитического мышления. Однако в арсенале продвинутых пользователей есть более «мощный» инструментарий, позволяющий автоматизировать и тем самым упростить поиск и структурирование полученных данных. Широкий спектр подобных специализированных OSINT-инструментов доступны всем пользователям, но стоит отметить, что многие из них требуют более продвинутый уровень подготовки и знание информационных процессов:

– Shodan – это продвинутаяпоисковаясистема, принципиальное отличие которой состоит в том, что она индексирует информацию, собранную из ответных баннеров, в то время как классические поисковые системы – индексируют контент веб-сайтов. С помощью данного инструмента можно найти устройство, которое подключено к сети Интернет;

– GoogleDorks – это техника поиска при помощи создания запросов в различных поисковых системах для выявления «дыр» в безопасности, которые позволяют обнаружить скрытую информацию на незащищенных серверах;

– TheHarvester. Ограниченный, но не менее полезный инструмент для поиска поддоменов, электронных писем, IP-адресов и других полезных вещей из широкого спектра общедоступной информации;

– –SpiderFoot. Полезный инструмент, имеющий открытый исходный код как для Windows, так и для Linux, позволяющий использовать запросы больше чем из ста ресурсов, выстраивая все в удобные графические интерфейсы;

– Creepy. Специальный инструмент для проведения геолокационных исследований, сбора данных в основном из социальных сетей, сайтов размещения изображений и фотографий. По результатам работы сервис публикует отчеты на карте с помощью специального поискового фильтра. Отчеты можно загружать в формате CSV или KML для экспорта в специальные аналитические программы.

Технология OSINT представлена серией платформ, которые позволяют в несколько кликов выполнять набор действий: исследование и сбор данных, анализ, изучение динамики изменений, сравнение результатов за период времени и т.п.

Все вышеперечисленное – лишь небольшая часть программ, используемых для анализа открытых данных. Последним шагом в стратегии OSINT будет перевод всех полученных цифровых данных в удобный формат, чтобы они были понятными и доступными для людей, далеких от ИТ-технологий.

Еще одно преимущество – уникальность самой технологии OSINT. Модельных алгоритмов проведения расследования не существует, так как все случаи уникальны и поэтому требуют индивидуального подхода.

Подводя итоги, стоит отметить, что использование технологий OSINT в деятельности органов внутренних дел, на наш взгляд, является экономически выгодным и эффективным решением, так как для реализации вышеупомянутых функций сотруднику необходимо всего лишь иметь персональный компьютер с предустановленным специальным программным обеспечением, а также свободный доступ в сеть Интернет.

СПИСОКЛИТЕРАТУРЫ:

1. КондратьевА. Наосновеоткрытыхисточников. // ВПК. – № 36 (302). – 16 сентября 2009. – «Ninety percent of intelligence comes from open sources. Theothertenpercent, theclandestinework».
2. Киви Бёрд. Модель OSINT // Компьютерра – 06.07.2007.
3. О полиции: Федеральный закон от 07февраля 2011 г. № 3-ФЗ ст. 11//Собрание законодательства РФ. -2011г. – №7.

УДК 004.4

ПОСТАНОВКА ЗАДАЧИ МОДЕЛИРОВАНИЯ ФУНКЦИОНИРОВАНИЯ ПОДРАЗДЕЛЕНИЙ ОВД

Козлов Михаил Андреевич, Чудаков Олег Евгеньевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: polka1794@yandex.ru, oechuda@yandex.ru

Аннотация. Развитие структуры органов внутренних дел в условиях внедрения современных информационных технологий, повышение эффективности их функционирования является актуальной задачей, что связано не только с изменениями структуры ОВД и расширением их функций, но и с необходимостью в этих условиях повышения эффективности их работы с учетом необходимости взаимодействия органов управления различного уровня. Необходимость количественного обоснования развития структуры органов внутренних дел в этих условиях становится важным и необходимым условием обоснованного принятия решений.

Ключевые слова: структура; подразделения; функции; моделирование; эффективность.

SETTING THE TASK OF MODELLING OF FUNCTIONING OF DIVISIONS OF DEPARTMENT OF INTERNAL AFFAIRS

Kozlov Mihail, Chudakov Oleg
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: polka1794@yandex.ru, oechuda@yandex.ru

Abstract. The development of the structure of the internal affairs departments in the context of introducing modern information technologies, increasing the efficiency of their functioning is an urgent task, which is associated not only with changes in the structure of the internal affairs departments and the expansion of their functions, but also with the need in these conditions to increase the efficiency of their work, taking into account the need for interaction between management departments at various levels. The need for quantitative substantiation of the development of the structure of the internal affairs departments under these conditions becomes an important and necessary condition for informed decision-making.

Keywords: structure; units; functions; modeling; efficiency.

Министерство внутренних дел представляет собой сложную организационно-техническую систему [1], включающую в себя достаточно большое количество функциональных подсистем. Как и любая организационно-техническая система как в целом, так и любая ее подсистема имеет в своем распоряжении развитые средства автоматизации для решения как повседневных, так и специфических задач, связанных с особенностями области деятельности органов управления. современных условиях является автоматизированной, что предполагает наличие в органах управления различного уровня средств автоматизации различного назначения и масштаба – от одиночных автоматизированных рабочих мест до сложных информационных систем различного назначения. Наличие сложной организационно-технической структуры в министерстве внутренних дел предполагает также необходимость активного использования сетевых технологий для обмена информацией между информационными подсистемами и другими средствами автоматизации на различных уровнях управления в системе министерства внутренних дел РФ.

Появление новых задач, основанных на практической деятельности ОВД МВД России приводит к необходимости определять те структурные подразделения, которые будут решать эти задачи. В этих случаях речь, как правило, идет как о создании некоторых новых структур в составе МВД России, так и о перераспределении функций между уже существующими подразделениями.

В любом случае стоит вопрос о том, будет ли вновь создаваемое подразделение успешно решать поставленные задачи или будут ли успешно решаться задачи существующим подразделением без ухудшения выполнения уже решаемых ими задач. Следовательно, для лиц, принимающих решение на проведение каких-либо реорганизаций желательно иметь некоторые оценки результатов преобразований по некоторым вариантам. Современные технологии позволяют решать поставленную задачу двумя способами:

– проведение экспертной оценки последствий (рисков) принимаемых решений для выбора оптимального (целесообразного) варианта;

– проведение математического (имитационного) моделирования функционирования вновь создаваемых или реорганизуемых подразделений МВД во взаимосвязи с деятельностью других подразделений.

Анализ показывает, что в настоящее время наиболее распространенным является первый способ, опирающийся на опыт экспертов, имеющих необходимые знания в области организационного управления, особенностей функционирования различных подразделений. Однако такой способ имеет существенный недостаток, связанный с субъективностью оценок каждого эксперта, что часто приводит к их противоречивости и необходимости применения специальных процедур согласования их мнений.

Современные технологии позволяют активно использовать второй способ, основным элементом которого является имитационного моделирования. В настоящее время существует достаточно много средств имитационного моделирования [2-4], позволяющих получать численные оценки показателей эффективности функционирования подразделений ОВД МВД, которые могут служить существенным подспорьем для принятия обоснованного решения и снижения рисков неэффективных преобразований.

Для реализации такого подхода необходимо решить ряд частных задач, к основным из которых можно отнести следующие:

Разработка вариантов преобразования структуры подразделений МВД для реализации новых функции или корректуры существующих функций. Появление новых функций может быть вызвано как появлением новых угроз, требующих реакции системы МВД, так и разделением уже существующих функций на более мелкие функции с целью повышения качества управления.

Проведение анализа вариантов структуры ОВД МВД с учетом реализации новых функций и построение функциональных моделей деятельности структур (подразделений) ОВД МВД. Данный этап представляется исключительно важным, поскольку именно он далее может быть положен в основу имитационных моделей для оценки вариантов построения ОВД МВД.

Обоснование показателей и критериев эффективности для оценки функционирования подразделений в различных вариантах структуры МВД. Набор показателей эффективности должен соответствовать требованиям, предъявляемым к ним, прежде всего они должны быть измеримы и достаточно просто интерпретированы в данной области. Критерии

эффективности должны опираться на выбранные показатели и соответствовать реальной практической деятельности ОВД МВД.

Разработка имитационной модели, позволяющей получить (рассчитать, получить статистические оценки) функционирования элементов функциональной модели с учетом исходных данных о характеристиках выполнения каждой функции. Для разработки имитационной модели могут быть использованы различные современные пакеты визуального моделирования, которые позволяют представлять различные функции, выполняемые подразделениями ОВД МВД в виде математических моделей или вероятностно-временных характеристик их выполнения, связанных в единую имитационную модель функционирования, исследуемого ОВД МВД.

Оценка адекватности модели. Оценка адекватности модели имеет принципиальное значение, поскольку на основании результатов моделирования могут приниматься решения, которые могут иметь существенные последствия на развитие системы ОВД МВД и эффективность их функционирования, а это имеет и существенные социально-политические последствия.

Проведение экспериментов с использованием имитационной модели для получения оценок функционирования моделей подразделений в различных вариантах структур. При решении данной задачи важно прежде всего определить план проведения экспериментов, исходные данные и результаты, которые должны быть получены в ходе проведения каждого эксперимента.

Оценка достоверности и значимости полученных результатов моделирования. Обоснование достоверности и значимости полученных результатов должны опираться на использование современных методов системного анализа.

Представление результатов моделирования. Результаты моделирования целесообразно представлять в понятном и удобном для проведения анализа и принятия решения виде.

Необходимо отметить, что каждая из задач представляет собой существенный элемент для получения обоснованных оценок и требует отдельной проработки. Необходимо также отметить, что все эти задачи взаимосвязаны и опираются на методы системного анализа. Фактически последовательное решение приведенных выше задач представляет собой методику проведения исследований для принятия обоснованного решения по реорганизации ОВД МВД.

Применение данного подхода позволит подготовить обоснованные решения по вариантам реорганизации подразделений ОВД МВД, обеспечит принятие решения, которое позволит повысить эффективность функционирования подразделений ОВД МВД России, и снизить материальные затраты при проведении реорганизаций.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ МВД от 30 апреля 2011 г. № 333 «О некоторых организационных вопросах и структурном построении территориальных органов МВД России».
2. Довженко В.Н., Наумов В.Н., Чудаков О.Е. Технология моделирования сложных систем с использованием пакета имитационного моделирования AnyLogic. Санкт-Петербург, ВУНЦ ВМФ ВМА им. Н.Г. Кузнецова. Вестник УМО №2(15), 2014.
3. Захаров И.С., Куватов В.И., Чудаков О.Е. Технология исследования сложных систем на основе современных case-средств. Вестник СПб университета МВД № 3 (71), 2016. С. 156 – 162.
4. Гвоздик М.И., Гладких М.Б., Чудаков О.Е., Хохлов Г.Г. Модели оценки эффективности деятельности РСЧС и методы их применения. X Международная научно-практическая конференция. Санкт-Петербург, 7-9 октября 2014 года.

УДК 004.056.5

СОВЕРШЕНСТВОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Парфенов Николай Петрович, Алексеев Сергей Алексеевич, Стахно Роман Евгеньевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: parfenov-nikolai@mail.ru, ksgati@yandex.ru, piter rus@mail.ru

Аннотация. Рассматривается вопрос совершенствования мероприятий по защите информации в деятельности органов внутренних дел, методы защиты информации.

Ключевые слова: служба безопасности; мероприятия; защита информации; угрозы; объект защиты.

IMPROVEMENT OF INFORMATION PROTECTION MEASURES IN THE ACTIVITIES OF THE INTERNAL AFFAIRS

Parfenov Nikolay, Alekseev Sergey, Stakhno Roman
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: parfenov-nikolai@mail.ru, ksgati@yandex.ru, piter rus@mail.ru

Abstract. The issue of improving measures to protect information in the activities of internal affairs bodies, methods of protecting information.

Keywords: security service; measures; information protection; threats; object of protection.

В настоящее время информация приобретает все большую значимость, поэтому она нуждается в постоянной защите. Информация, обрабатываемая в служебной деятельности органов внутренних дел, является одной из наиболее значимых, поэтому она, в первую очередь, подлежит защите от несанкционированного доступа (НСД).

Кроме этого, бурное развитие человечества в последние годы привело к ожидаемому переходу от индустриального к информационному обществу.

В современном информационном обществе необходимо, чтобы каждый член общества владел информацией, умел производить, распространять, хранить и использовать ее.

Сотрудники органов внутренних дел - наилучшие представители человеческого общества, являясь в то же время, членами информационного общества, обязаны в большей степени удовлетворять вышеперечисленным требованиям.

Также, согласно нормативному законодательству [1], полиция должна и обязана использовать в своей служебной деятельности, современную информационно-телекоммуникационную структуру, информационные системы, передовые достижения науки и техники, а также системы связи.

Помимо этого, органы внутренних дел обязаны обеспечить техническую защиту от утечек информации и техническое противодействие разведкам противников.

Для организации технической защиты информации в органах внутренних дел используется Положение о государственной системе защиты информации в Российской Федерации [2].

Для совершенствования мероприятий по эффективной защите информации необходимо анализировать, классифицировать и перекрывать всевозможные пути утечки служебной информации. Для решения этих задач в органах внутренних дел создается система безопасности, далее в тексте служба безопасности. Чаще всего служба безопасности создается на базе структурных подразделений секретариата и технической защиты информации. Сотрудники данных подразделений в служебной деятельности обеспечивают режим секретности и техническую защиту конфиденциальной информации.

Дополнительно служба безопасности, кроме технической защиты информации, обеспечивает физическую, правовую, оперативную, технологическую и организационную защиту информации, используемую в служебной деятельности.

Архиважное значение имеют мероприятия по защите служебной информации от внутренних и внешних угроз. Далее в тезисах приведем определения некоторых общепринятых понятий и терминов в области защиты информации. Объект защиты информации (далее в тексте объект) – это здания, помещения и территория, на которой расположены все имущество, технические средства органа внутренних дел, требующие защиты.

Техническая защита объекта информации – это комплекс мер, обеспечивающих защиту информации на объекте от НСД, от неправомерного использования конфиденциальной информации, а также защиту компьютеров, компьютерных систем, технологий и сетей.

Для полного понимания рассматриваемых вопросов коротко перечислим те мероприятия, которые в комплексе, обеспечивают информационную безопасность: предупреждение внутренних и внешних угроз; выявление внутренних и внешних угроз; обнаружение внутренних и внешних угроз; локализация преступных посягательств и преступных действий; ликвидация последствий угроз и преступных посягательств, а также восстановление прежнего состояния[3].

Рассмотрим более подробно комплекс мероприятий по совершенствованию защиты информации.

Предупреждение внутренних и внешних угроз – это упреждающие, до их возникновения, действия по защите информации. Эти действия носят разноплановый характер, например, создание осознанного микроклимата, внутри коллектива сотрудников органа внутренних дел по защите информации; защита информации криптографическими, аппаратными, физическими и аппаратно-программными средствами; постоянная работа с информаторами по предупреждению утечек конфиденциальной информации; упреждающая информационно-аналитическая работа службы безопасности органа внутренних дел по текущему и прогнозируемому состоянию криминогенной обстановки. Один из простых примеров предупреждения угроз – это заборы с датчиками сигнализации по периметру объекта защиты.

Планомерное выявление внутренних и внешних угроз – это систематическая работа по выявлению и предупреждению потенциальных и/или реальных внутренних и внешних угроз безопасности информации. Классический пример выявления угроз – это внедрение тайных информаторов в среду криминальной структуры и получение упреждающих сведений о подготовке преступных посягательств и преступных действий.

Обнаружение внутренних и внешних угроз – это систематическая деятельность по определению явных внутренних и внешних угроз и реальных преступных действий.

Значимый результат этой деятельности – обнаружение фактов хищения и разглашения конфиденциальной информации; фактов НСД к служебной информации. Использование охранного телевидения, видеокамер, а также датчиков сигнализации предназначено для обнаружения угроз.

Локализация преступных посягательств и преступных деяний – это систематическая деятельность по устранению реальной угрозы и явных преступных посягательств, и преступных деяний. В качестве простого примера можем привести пресечение подслушивания служебной информации во время совещания по звуковым каналам их утечки.

Ликвидация последствий угроз и преступных посягательств, а также восстановление прежнего состояния – это систематическая работа по восстановлению состояния, предшествовавшего наступлению угроз и преступных деяний. Самые простые системы ликвидации угроз – это типовые системы пожаротушения.

Организационно-технические мероприятия по совершенствованию защиты информации – это комплекс мер, блокирующих разглашения и утечки служебной информации с помощью технических средств и режима. В свою очередь вышеназванные мероприятия подразделяются на пространственные, режимные и энергетические

меры. Учитывая направленность рассматриваемых в данной работе вопросов, хотелось бы более подробно рассказать о технических и организационных мероприятиях по совершенствованию защиты конфиденциальной информации.

Технические мероприятия по совершенствованию защиты служебной информации подразделяются на следующие:

– скрытие – это применение радиомолчания и конструирование пассивных помех техническим средствам криминальных структур;

– подавление – это конструирование активных помех техническим средствам криминальных структур;

– дезинформация – это чаще всего предоставление ложной информации криминальным структурам, злоумышленникам, т.е. использование в работе информационных технологий и средств ложной информации.

Организационные мероприятия – это в основном ограничительные мероприятия к регламенту доступа конфиденциальной информации и технологий обработки и переработки служебной информации. Наиболее распространенные мероприятия по совершенствованию защиты информации, следующие:

– установление надежного пропускного режима;

– установление надежного контроля над сотрудниками органа внутренних дел, работающими со служебной информацией;

– установление отдельных зон в соответствии с уровнями конфиденциальной информации и режимными системами допуска;

– установление регламента допуска и работы с конфиденциальной информацией, включая операции их учета, перемещения, исполнения, хранения и уничтожения.

В органах внутренних дел служат множество сотрудников, которые имеют различные формы допуска к конфиденциальной информации, поэтому для эффективной защиты информации необходимо провести классификацию объектов защиты по уровням секретности информации; т.е. установить категорию объекта защиты информации. В зависимости от важности и конфиденциальности информации устанавливается минимальный комплекс мер по ее защите.

Подведя итоги рассмотренных вопросов необходимо подчеркнуть, что основными мероприятиями совершенствования защиты информации в деятельности органов внутренних дел являются лицензирование деятельности органов внутренних дел в области информации, аттестование объектов защиты по степени секретности, сертификация средств защиты информации и категорирование объектов защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. О полиции: Федеральный закон от 07 февраля 2011 г. № 3-ФЗ ст. 11//Собрание законодательства РФ. -2011г. - №7.
2. Постановление Правительства Российской Федерации от 15 сентября 1993 г. №912-51.
3. Парфенов Н.П., Стахно Р.Е. Вопросы правового регулирования обработки и защиты персональных данных. / Проблемы современной науки и образования № 19 (101). Москва. изд. «Проблемы науки». 2017. С. 29-32.

УДК 37.036.5

ИСПОЛЬЗОВАНИЕ СВОБОДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПОДГОТОВКИ КУРСАНТОВ ВОЕННЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ ВЫСШЕГО ОБРАЗОВАНИЯ

Потапова Людмила Сергеевна
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
Пилютова, ул. 1, Санкт-Петербург, 198206, Россия
e-mail: ly-da.83@mail.ru

Аннотация: Организационная и образовательная деятельность на кафедрах высших учебных заведениях неразрывно связана с применением информационных технологий. Но использование современных информационных технологий в учебном процессе ограничено техническими характеристиками рабочих станций в компьютерных классах кафедр и высокой стоимостью программного обеспечения. Тем не менее, можно найти альтернативу в виде открытого программного обеспечения, распространяемого на условиях свободной лицензии, и удовлетворяющего системным и аппаратным требованиям компьютеров, используемых на занятиях.

Ключевые слова: военные образовательные организации высшего образования, свободное программное обеспечение, учебный процесс в военных образовательных организациях высшего образования, электронные учебные пособия.

USE OF THE FREE SOFTWARE FOR TRAINING OF CADETS OF THE MILITARY EDUCATIONAL ORGANIZATIONS OF THE HIGHER EDUCATION

Luydmila Potapova
St. Petersburg Military Order of Zhukov Institute of the National Guard Troops of the Russian Federation
(SPVI National Guard Troops)
1 Pilyutova, st. 1, St. Petersburg, 198206, Russia
e-mail: ly-da.83@mail.ru

Abstract: Organizational and educational activities in the departments of higher educational institutions are inextricably linked with the use of information technology. But the use of modern information technologies in the

educational process is limited by the technical characteristics of workstations in the computer classes of departments and the high cost of software. Nevertheless, one can find an alternative in the form of open source software distributed under a free license and satisfying the system and hardware requirements of computers used in the classroom.

Key words: military educational organizations of higher education, free software, the educational process in military educational organizations of higher education, electronic textbooks.

В настоящее время большую актуальность приобретают вопросы, связанные с программным обеспечением учебного процесса в военных образовательных организациях высшего образования (ВОО ВО). Это обусловлено, в первую очередь, тем, что цены на коммерческое лицензионное программное обеспечение настолько высоки, что зачастую, в условиях существующих санкций в отношении Российской Федерации, не позволяют в полной мере обеспечить требования федеральных государственных образовательных стандартов к материально-техническому обеспечению учебного процесса [1]. Для военных образовательных организациях высшего образования остро стоят и вопросы обеспечения надежности и безопасности информационных ресурсов, использующихся в процессах обработки, хранения, использования и передачи информации в информационных системах этих организаций. Например, выпускник, освоивший программу ВОО ВО, должен обладать способностью работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации. Это требует от него знаний и практических навыков работы с различными операционными системами, с пакетами прикладных программ различного назначения [2].

В июле 2016 года вышло распоряжение правительства Российской Федерации № 1588-р «Об утверждении плана перехода в 2016-2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения». В частности операционная система Linux, что влечет за собой и поиск прикладных программ для решения задач. Эта операционная система основана на GNU/Linux, то есть на свободном программном обеспечении.

В рамках указанных обстоятельств, по нашему мнению, одним из выходов из сложившейся ситуации может быть использование свободного программного обеспечения. Свободным программным обеспечением (англ. free software) считаются такие программы, которые можно свободно устанавливать, изучать, распространять и даже при необходимости изменять. Можно использовать и бесплатное (англ. freeware) программное обеспечение, которое, в отличие от свободного, распространяется без исходных кодов, и изменять его нельзя. Кроме того, военные образовательные организации высшего образования, могут в частности использовать полусвободное программное обеспечение, для которого Фонд свободного программного обеспечения (FSF) использует термин «проприетарное». Проприетарное программное обеспечение – (англ. proprietary software) – программное обеспечение, являющееся частной собственностью авторов или правообладателей и не удовлетворяющее критериям свободы ПО (речь именно о свободе, а не просто открытости ПО) и, с позиции Фонда свободного ПО, при этом не являющееся полусвободным ПО. Правообладатель сохраняет за собой монополию на его использование, копирование и модификацию, полностью или в существенных моментах. Часто проприетарным называют любое несвободное ПО, включая полусвободное. Такое программное обеспечение нередко бесплатно для образовательных и медицинских организаций и учреждений и частных лиц в случае неполучения прибыли от его использования.

Таким образом, в большинстве случаев имеется альтернатива коммерческому программному обеспечению в виде открытого программного обеспечения, распространяемого на условиях свободной лицензии, и удовлетворяющего системным и аппаратным требованиям комплексов технических средств, используемых в учебном процессе [3].

В Санкт-Петербургском военном ордена Жукова институте войск национальной гвардии на кафедре информатики и математики с 2019 года, в ходе проведения занятий изучается операционная система Astra Linux Special Edition, эта операционная система является проектом GNU/Linux (ассоциация разработчиков свободной операционной системы семейства GNU/Linux на базе ядра Linux Kernel). В связи с этим в общем случае архитектура операционной системы Astra Linux Special Edition соответствует архитектурным решениям GNU/Linux. Главным и основным плюсом GNU/Linux является то, что эта операционная система является свободной. Так, например:

1. Один из свободно распространяемых графических редакторов, для пользователей GNU/Linux Image Manipulation Program (GIMP), эта программа, предназначенная для обработки изображения, имеет открытый исходный код для создания изображений, ретуширования фотографий, а также дает возможность создавать авторские изображения. В свободном пользовании у Linux есть большое число ПО для работы с растровой и векторной графикой, такие как: Photoshop Wine, Pinta, Digikam, Showfoto и другие.

2. Для работы с видео изображениями в Linux свободно доступны такие программы как: Kdenlive, OpenShot, Lightworks, Blenderb и другие, предназначенные как для профессиональной обработки видео, так и для любительской, с камерами имеющие низкое разрешение.

3. Практически все версии Linux поставляются с базовым, но очень эффективным программным набором, для хранения данных. Так, например, база данных dbm, позволяет хранить структуры данных переменного размера с помощью индекса и затем извлекать структуру либо используя индекс, либо просто последовательно просматривая базу данных.

Говоря о создании баз данных, практикуемых на занятиях, нельзя не упомянуть программное обеспечение LibreOffice – мощный офисный пакет, который входит в операционную систему Astra Linux и используется во всех высших учебных заведениях войск национальной гвардии. Важная его особенность в том, что он также является абсолютно бесплатным и может устанавливаться и использоваться в бюджетных и коммерческих организациях, а также на домашних компьютерах и в учебных заведениях. Данный офисный пакет установлен и в компьютерных классах кафедры информатики и математики и состоит из: текстового редактора Writer, табличного редактора Calc, средства создания и демонстрации презентаций Impress, векторного редактора Draw, редактора формул Math и, вышеупомянутой системой управления базами данных Base.

В этой связи, необходимо упомянуть публикации [4, 5], в которых рассмотрены вопросы оптимизации организации образовательной деятельности в ОО ВО, а также предлагаются эффективные алгоритмы, на основе которых должны разрабатываться с использованием свободного программного обеспечения, компьютерные программы, реализующие оптимизацию этих процессов.

В заключение отметим, что, конечно же, свободное программное обеспечение не лишено некоторых недостатков. Но вряд ли существует единое конкретное решение всех возникающих проблем при выборе программного обеспечения учебного процесса в образовательных организациях. В любом случае, при выборе программного обеспечения руководствоваться нужно «Единым реестром российских программ для электронных вычислительных машин и баз данных», а также критериями, которые стоят перед образовательной организацией для максимально эффективного решения служебно-боевых задач.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев В.П., Черных А.К., Горлова О.С. Вопросы применения информационных технологий на кафедрах образовательных организаций высшего образования //В сборнике: Экономические стратегии ЕАЭС: проблемы и инновации Сборник материалов Всероссийской научно-практической конференции. – М: РУДН, 2018. С. 7-18.
2. Андреев В.П. Применение информационных технологий в образовательном процессе на кафедрах вуза». Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. – Краснодар: Краснодарский университет МВД России, 2017. С. 8-11.
3. Стахно Р.Е., Андреев В.П., Яковлева Н.А., Алексеев С.А. Анализ и моделирование информационной системы кафедры образовательного учреждения высшего образования с разработкой банка данных. Информационные ресурсы России. 2019. №4(10). С. 38-42.
4. Вилков В.Б., Флегонтов А.В., Черных А.К. О выборе оптимального плана осуществления программы дополнительного образования или переподготовки //Письма в Эмиссия. Оффлайн: электронный научный журнал. 2017. № 8. С. 2553.
5. Дергачев А.И., Байдина Н.В., Перепеченов А.М., Андреев В.П., Костянко Н.Ф. Сборник учебно-методических материалов и контрольных решений для проведения занятий со студентами университета всех специальностей по дисциплине «Информатика».
6. Свидетельство о государственной регистрации базы данных №2015620678/ Санкт-Петербург, 2015.

УДК 004.056.5

МЕТОДИКА СОЗДАНИЯ ЗАШИФРОВАННЫХ ВИРТУАЛЬНЫХ ДИСКОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ МВД РОССИИ

Примакин Алексей Иванович, Иванов Николай Сергеевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: primakin@mail.ru, ivanov160598@gmail.com

Аннотация. Рассматривается вопрос защиты информации, обрабатываемой в территориальных органах МВД России, виды и способы шифрования информации.

Ключевые слова: шифрование; криптография; алгоритм; информационные технологии; компьютерные технологии.

METHODOLOGY FOR CREATING ENCRYPTED VIRTUAL DISKS OF THE INFORMATION SYSTEM OF THE TERRITORIAL BODIES OF INTERNAL AFFAIRS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Primakin Alexey, Ivanov Nickolay
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: primakin@mail.ru, ivanov160598@gmail.com

Abstract. The question of the information security processed in territorial authorities of the Ministry of Internal Affairs of the Russian Federation, types and ways of enciphering of information is considered.

Keywords: encryption; cryptography; algorithm; information technology; computer technology.

Информация в последние годы обретает все большую важность, поэтому она нуждается в защите. Информация, обрабатываемая в органах внутренних дел, является одной из наиболее важных, поэтому подлежит защите от несанкционированного доступа.

Шифрование диска – технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать. Для шифрования диска используется специальное программное или аппаратное обеспечение, которое шифрует каждый бит хранилища. На рынке есть множество реализаций полного шифрования диска, они могут очень сильно различаться по возможностям и

защищённости, их можно разделить на программные и аппаратные. Аппаратные в свою очередь можно разделить на те, что реализованы в самом устройстве хранения, и другие, например, адаптер шины.

На данный момент существует несколько подходов к шифрованию жестких дисков:

1. Прозрачное шифрование (Transparent encryption), также называемое шифрованием в реальном времени (real-time encryption) или шифрованием на лету (on-the-fly encryption) – это метод, использующий какое-нибудь программное обеспечение для шифрования диска. Слово «прозрачный» означает, что данные автоматически зашифровываются или расшифровываются при чтении или записи, для чего обычно требуется работа с драйверами, для установки которых нужны специальные права доступа. Однако некоторые FDE после установки и настройки администратором позволяют обычным пользователям шифровать диски [2].
2. Шифрование на уровне файловой системы (filesystem-level encryption – FLE) – процесс шифрования каждого файла в хранилище. Доступ к зашифрованным данным можно получить только после успешной аутентификации. Некоторые операционные системы имеют собственные приложения для FLE, при этом доступно и множество реализаций от сторонних разработчиков. FLE прозрачно, это значит, что каждый, кто имеет доступ к файловой системе, может просматривать названия и метаданные зашифрованных файлов, которыми может воспользоваться злоумышленник.
3. Шифрование диска и Trusted Platform Module. Trusted Platform Module (TPM) – это безопасный криптопроцессор, встроенный в материнскую плату, который может быть использован для аутентификации аппаратных устройств. Так же он может хранить большие двоичные данные, например, секретные ключи и связывать их с конфигурацией целевой системы, в результате чего они будут зашифрованы, и расшифровать их можно будет только на выбранном устройстве. Есть как FDE, использующие TPM, например, BitLocker, так и те, которые не поддерживают работу с ним, например, TrueCrypt [5].
4. Полное шифрование и главная загрузочная запись. При установке программно-реализованного FDE на загрузочный диск операционной системы, которая использует главную загрузочную запись (англ. master boot record, MBR), FDE должен перенаправлять MBR на специальную предзагрузочную среду (англ. pre-boot environment, PBE), для осуществления предзагрузочной аутентификации (англ. Pre-Boot Authentication, PBA). Только после прохождения PBA будет расшифрован загрузочный сектор операционной системы. Некоторые реализации предоставляют возможность PBA по сети. Однако изменение процесса загрузки может привести к проблемам. Например, это может помешать осуществлению мультизагрузки или привести к конфликту с программами, которые обычно сохраняют свои данные в дисковое пространство, где, после установки FDE, будет расположена PBE. Так же это может помешать пробуждению по сигналу из локальной сети, так как перед загрузкой требуется PBA. Некоторые реализации FDE можно настроить так, чтобы они пропускали PBA, но это создаёт дополнительные уязвимости, которыми может воспользоваться злоумышленник. Данных проблем не возникает при использовании самошифрующихся дисков. В свою очередь, это не означает преимущество самошифрующихся дисков над остальными накопителями. Для сохранения мультизагрузки операционных систем разных семейств, необязательно настраивать программный процесс шифрования до инсталляции операционной системы: полное шифрование диска с сохранением мультизагрузки возможно применить при уже установленных системах [5].

Актуальность написания статьи обусловлена тем, что сейчас в органах внутренних дел для защиты информации используется электронная подпись, но она хорошо защищает только передаваемую информацию, а информация, хранящаяся на жестком диске даже категорированного компьютера, остается под угрозой. Потому что большинство Компьютеров работают на базе ОС Windows 7, которая недостаточна защищена от взлома. Для взлома Windows 7 достаточно через режим устранения неполадок зайти в реестр и сделать так, чтобы при запуске попасть в командную строку и оттуда можно сбросить пароль учетной записи. Если диск не зашифрован, что бывает в большинстве случаев, то его можно подключить к компьютеру как второй диск и найти на нем всю необходимую информацию. Для защиты компьютеров НСД целесообразно использовать программы шифрования жестких дисков, но большинство программ шифрования написаны сторонними компаниями и направлены на получение прибыли, поэтому доверять таким программам какую-либо защищаемую государством информацию небезопасно [1].

Самый актуальный стандарт шифрования на данный момент в России – это ГОСТ Р 34.12-2015 описывающий симметричный алгоритм блочного шифрования «Кузнечик». Данный алгоритм является разработкой ФСБ и по заявлениям разработчиков является очень стойким, то шифровать лучше всего им, но существует множество других алгоритмов шифрования, которые могут быть использованы для защиты информации жестких дисков. Это такие алгоритмы как: AES (Advanced Encryption Standard), DES (Data Encryption Standart) и так далее.

Тем не менее существуют проблемы безопасности у программно-реализованных средств защиты Большинство программно-реализованных систем полного шифрования уязвимы для атаки методом холодной перезагрузки, посредством которого ключи могут быть украдены. Атака основана на том, что данные в оперативной памяти могут сохраняться до нескольких минут после выключения компьютера. Время сохранения можно увеличить охлаждением память. Системы, использующие TPM, тоже неустойчивы к такой атаке, так как ключ, необходимый операционной системе для доступа к данным, хранится в оперативной памяти. Программные реализации также сложно защитить от аппаратных кейлогеров. Есть реализации, способные их обнаружить, но они аппаратно-зависимы. Для систем шифрования дисков необходимы безопасные и надёжные механизмы

восстановления данных. Реализация должна предоставлять простой и безопасный способ восстановления паролей (наиболее важную информацию) в случае, если пользователь его забудет.

Большинство реализаций предлагают решения на основе пароля пользователя. К примеру, если есть защищённый компьютер, то он может отправить пользователю, забывшему пароль, специальный код, который он потом использует для доступа к сайту восстановления данных. Сайт задаст пользователю секретный вопрос, на который пользователь ранее давал ответ, после чего ему будет выслан пароль или одноразовый код восстановления данных. Это также может быть реализовано обращением к службе поддержки. Другие подходы к восстановлению данных, как правило, сложнее. Некоторые FDE предоставляют возможность самому без обращения к службе поддержки восстановить данные. Например, используя смарт-карты или криптографические токены. Также есть реализации, поддерживающие локальный механизм восстановления данных «вопрос-ответ». Но такие подходы уменьшают защищённость данных, поэтому многие компании не разрешают использовать их. Утрата аутентификатора может привести к потере доступа к данным или к доступу злоумышленника к ним [5].

Второй важной проблемой является восстановление пароля. Большинство программно-реализованных систем полного шифрования уязвимы для атаки методом холодной перезагрузки, посредством которого ключи могут быть украдены [6]. Атака основана на том, что данные в оперативной памяти могут сохраняться до нескольких минут после выключения компьютера. Время сохранения можно увеличить охлаждением памяти. Системы, использующие TPM, тоже неустойчивы к такой атаке, так как ключ, необходимый операционной системе для доступа к данным, хранится в оперативной памяти. Программные реализации также сложно защитить от аппаратных кейлогеров. Есть реализации, способные их обнаружить, но они аппаратно-зависимы. Таким образом существует множество различных способов зашифровать жесткие диски, что позволит защитить обрабатываемую в территориальных органах информацию.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 34.12-2015 Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры.
2. А.М. Коротин. О способах реализации прозрачного шифрования файлов на базе сертифицированного скзи для операционной системы Linux // Безопасность информационных технологий. – 2012. – № 2012 – 2. – С. 62-66.
3. Информационная безопасность: основы правовой и технической защиты информации: учебное пособие / В.А. Мазуров, А.В. Головин, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2005. – 196 с.
4. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
5. K. Scarfone, M. Souppaya, M. Sexton. Guide to Storage Encryption Technologies for End User Devices. – Special Publication 800-111. – National Institute of Standards and Technology, 2007. – 40 с.
6. Tilo Müller, Hans Spath, Richard Mackl, Felix C. Freiling. Stark Tamperproof Authentication to Resist Keylogging. – 2013.

УДК 004.94

ПРИМЕНЕНИЕ РАСЧЕТНОГО ПРОГРАММНОГО КОМПЛЕКСА «ЛИРА-САПР» В ПОДГОТОВКЕ СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ «ОСНОВАНИЯ И ФУНДАМЕНТЫ»

Примакина Елена Ивановна
Костромская государственная сельскохозяйственная академия
Учебный городок, 34 пос. Караваево, Кострома, 156530, Россия
e-mail: ei-primakina@yandex.ru

Аннотация. Приводится опыт применения расчетного программного комплекса ЛИРА-САПР при подготовке студентов, обучающихся по направлению «Строительство»

Ключевые слова: расчетный программный комплекс ЛИРА-САПР; модель грунтового основания; автоматизированный расчет.

APPLICATION OF THE SETTLEMENT PROGRAM LIRA-SAPR COMPLEX IN TRAINING OF STUDENTS ON THE SUBJECT MATTER «FOUNDATION ENGINEERING»

Primakina Elena
Kostroma state agricultural academy
Educational town, 34 settlements of Karavayevo, Kostroma, 156530, Russia
e-mail: ei-primakina@yandex.ru

Abstract. Experience of application of the LIRA-SAPR settlement program complex when training the students studying in the Construction direction is given.

Keywords: the LIRA-SAPR settlement program complex; model of the soil basis; the automated calculation.

В настоящее время при проектировании строительных конструкций в проектных организациях значительная часть расчетов выполняется на персональных компьютерах с использованием универсальных программно-вычислительных комплексов, среди которых наибольшей популярностью пользуется ПК ЛИРА. В связи с этим кафедра строительных конструкций КГСХА использует этот программный комплекс на протяжении более двадцати лет при подготовке студентов по профилю «Промышленное и гражданское строительство».

Изучение многофункционального программного комплекса для расчета, исследований и проектирования конструкций различного назначения проводится в компьютерном классе кафедры,

оснащенном десятью операторскими местами с сетевым лицензионным программным обеспечением. Автоматизированным расчетам фундаментных конструкций предшествует изучение ПК ЛИРА-САПР студентами, обучающихся по программе бакалавриата в дисциплине «Информационные технологии в проектировании строительных конструкций» Таким образом, к этапу проектирования оснований и фундаментов студенты имеют определенные навыки: в формировании расчетных моделей, включающих в себя геометрию конструкции, связи и сопряжения ее элементов, все необходимые загружения и их сочетания для надземных плоских, пространственных конструкций [1], моделируемых стержневыми или пластинчатыми конечными элементами; в работе с конструирующими системами СТК-САПР, АРМ-САПР; в формировании отчета по результатам расчета.

При изучении дисциплины «Основания и фундаменты» ПК ЛИРА-САПР используется для проектирования фундаментных плит, ленточных фундаментов под ряды колонн, перекрестных ленточных фундаментов, как конструкций на упругом основании.

Так как по условиям работы в большинстве своем здания на таких фундаментах относятся к пространственным статически неопределимым системам с элементами чувствительными к неравномерным осадкам. В связи с этим проектирование таких сооружений предполагает высокий уровень прочностных расчетов элементов конструкций с учетом действия всей системы здания с грунтовым основанием [2]. Значительную сложность представляет выбор модели основания. На практических занятиях студенты знакомятся с возможностью создания различных моделей грунтового основания (Винклера, Пастернака), а также способами определения и назначения их характеристик.

На практических занятиях студентам демонстрируются проектные решения, выполненные с использованием ПК ЛИРА-САПР преподавателями при проектировании фундаментов под реальные объекты города и области, осуществленные на базе проектно-конструкторского бюро кафедры.

Процесс подготовки студентов продолжается и на этапе дипломного проектирования, где при выполнении раздела по основаниям и фундаментам при разработке подобных конструкций студентам предлагается выполнить анализ напряженно-деформированного состояния системы «основание-фундамент-надземная часть» по результатам статического расчета с целью выбора достоверной модели грунта, оценить возможность перераспределения усилий в элементах конструкций надземной части здания из-за влияния податливости основания.

СПИСОК ЛИТЕРАТУРЫ

1. СП 20.13330.2016. Свод правил. Нагрузки и воздействия. Актуализированная редакция СНиП 2.01.07-85*. М.: Стандартинформ, 2019.
2. СП 22.13330.2016. Свод правил. Основания зданий и сооружений. Актуализированная редакция СНиП 2.02.01-83*. М.: Стандартинформ, 2016.

УДК 004.056.5

ФОРМЫ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Родин Владимир Николаевич, Богданов Евгений Игоревич
Санкт-Петербургский университет МВД России
ул. Летчика Пилютова, 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, ovruk333@yandex.ru

Аннотация: в связи с широким распространением информационно-коммуникационных технологий меняется характер преступности. В настоящее время все больше преступлений совершаются с помощью компьютерной техники и сети Интернет. Целью данной статьи является анализ составов преступлений, которые совершаются с использованием сети Интернет, а также выработка системы мер противодействия таким преступлениям. Нормативную основу исследования образуют Конституция Российской Федерации, уголовное и уголовно-процессуальное законодательство. Использованы современные общенаучные методы познания социальных явлений и процессов. Представлен анализ действующего российского уголовного законодательства в сфере противодействия преступлениям, связанным с компьютерной информацией, рассмотрены иные составы преступлений, способом (орудием) совершения которых могут выступать информационно-телекоммуникационные сети. в результате исследования предложены основные направления повышения эффективности уголовно-процессуального противодействия преступлениям, совершаемым с использованием информационно- телекоммуникационных сетей, в том числе связанные с развитием международного сотрудничества в сфере уголовного процесса. Полученные данные могут быть использованы для предотвращения и эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей.

Ключевые слова: правоохранительная деятельность, уголовный процесс, информационно-телекоммуникационные сети, сеть Интернет, преступления, совершаемые с использованием информационно-телекоммуникационных сетей, незаконный оборот наркотиков, группы смерти, киберпреступность.

FORMS AND METODS OF COMBATING CRIMES COMMITTED IN THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Rodin Vladimir, Bogdanov Evgeniy
St. Petersburg University of the Ministry of Internal Affairs of Russia
st. pilot Pilyutova, 1, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, ovruk333@yandex.ru

Abstract: Due to the wide spread of information and communication technologies, the nature of crime is changing. Currently, more and more crimes are committed using computer equipment and the Internet. The purpose of this article is to analyze the composition of crimes that are committed using the Internet, as well as to develop a system of measures to counter such crimes. The regulatory framework of the study is formed by the Constitution of the Russian Federation, criminal and criminal procedure legislation. Used modern general scientific methods of cognition of social phenomena and processes. The analysis of the current Russian criminal legislation in the field of countering crimes related to computer information is presented, other corpus delicti are considered, the informational telecommunication networks can act as an instrument (instrument) of which. As a result of the study, the main directions of improving the efficiency of criminal procedure to counter crimes committed using information and telecommunication networks, including those related to the development of international cooperation in the criminal process, have been proposed. The obtained data can be used to prevent and effectively counter crimes committed using information and telecommunication networks.

Keywords: Law enforcement activities; criminal process; information and telecommunication networks; Internet; crimes committed with the use of information and telecommunication networks; drug trafficking; death groups; cybercrime.

В связи с широким распространением информационно-коммуникационных технологий меняется характер преступности. В настоящее время все больше преступлений совершаются с помощью компьютерной техники и информационно-телекоммуникационных сетей (далее ИТС). Интернет-преступность растет быстрыми темпами. Информационная инфраструктура позволяет преступникам действовать скрытно, не оставляя своих координат, совершать преступные действия с территории любого государства (где имеются технические возможности), а также действовать с соисполнителями на международном уровне.

По подсчетам, произведенным компанией Symantec, совокупные доходы киберпреступников составляют более 110 млрд. долларов в год. При этом побочные убытки, возникающие в результате совершения данных преступлений (затраты времени на восстановление работоспособности, простой оборудования и пр.), можно дополнительно оценить еще в 274 млрд. долларов. Соответственно, общий ущерб от киберпреступности в мировом масштабе составляет около 388 млрд. долларов в год. При этом глобальный мировой оборот марихуаны, кокаина и героина, составляет порядка $288 млрд., что на 26 % ниже [7].

В настоящее время с использованием информационно-коммуникационных технологий совершаются не только преступления, связанные с компьютерной информацией. Практически по всем преступлениям современные виды компьютерных программ или программно-технические средства могут использоваться в качестве средства или орудия совершения.

Как считает И.М. Рассолов, компьютерная преступность представляет собой криминальную отрасль, в которой действуют мошенники, хакеры, вымогатели, педофилы, сутенеры, процветает торговля людьми и наркотиками, а также многие другие правонарушения [4].

Так, ряд преступлений в сфере экономики совершается с использованием информационно-коммуникационных технологий. К таковым можно отнести мошеннические действия, связанные со взломом профилей пользователей в социальных сетях и последующей рассылкой сообщений «друзьям» жертвы взлома с просьбой о переводе денежных средств под различными предлогами. В эту же группу можно отнести заведомо фиктивную продажу товаров (услуг).

Основным средством совершения таких преступлений, как неправомерный оборот средств платежей, незаконная банковская деятельность, также являются информационно-коммуникационные технологии. Так, совершение данных преступлений предполагает проведение банковских операций по переводу денежных средств. При этом платежные поручения направляются в основном посредством сети Интернет, что значительно ускоряет и упрощает преступную деятельность, а также создает определенные препятствия по уголовно-процессуальному документированию данной деятельности.

На протяжении последних нескольких лет в сети Интернет стали активно развиваться «группы смерти», созданные с целью склонения детей и подростков к суицидам. Для того, чтобы вступить в группу, необходимо выполнять определенные задания, связанные с фотографированием себя в опасных местах, например, на краю крыш высотных зданий, на железнодорожных рельсах и т.д. Кроме того, членам группы внушается, что они никому не нужны, что есть другой, более счастливый мир, куда надо стремиться. Психологическое воздействие на членов групп заключается в основном в эксплуатации потребности принадлежать к значимой тайной группе, ощущать свою избранность и уникальность [2].

По различным данным в настоящее время в мире действуют около 5 тыс. Интернет-сайтов, содержащих экстремистский (террористический) контент. Что касается русскоязычных сайтов экстремистской направленности, то более 90 % из них находятся за пределами российского правового поля. Для достижения своих целей представители экстремистских и террористических организаций используют возможности

социальных сетей (ВКонтакте, Фейсбук, Твиттер, Одноклассники), в которых ведется активная пропагандистская работа. В настоящее время преобладает и имеет устойчивую тенденцию к росту количество преступлений, которые совершаются с использованием сети Интернет. В структуре экстремистской преступности удельный вес таких деяний составляет практически две трети [6].

Коммуникационные возможности ИТС также активно используются для совершения преступлений, связанных с незаконным оборотом наркотиков. В настоящее время наиболее распространен бесконтактный сбыт наркотиков. Так, установление контакта потребителя со сбытчиком происходит посредством переписки или звонков через социальные сети и мессенджеры (например, Skype, Viber, WhatsApp и т.п.). Затем производится оплата посредством различных платежных систем. После оплаты сбытчики сообщают места так называемых закладок с наркотическим веществом. Вещество в место закладки помещается обычно таким образом, чтобы максимально снизить возможность его обнаружения посторонними лицами [5, с. 85].

На территории Российской Федерации законодательно запрещено осуществление деятельности, связанной с организацией и проведением азартных игр с использованием ИТС. Игорные заведения могут функционировать лишь в специально отведенных игорных зонах [1]. Но многие предприниматели в обход российского законодательства регистрируются и осуществляют организацию азартных игр с территории иностранных государств. Для доказывания факта организации незаконной игорной деятельности необходимо иметь доступ к соответствующим серверам, которые, как отмечено выше, в основном располагаются на территории иностранных государств. В связи с этим доказать факт преступной деятельности представляется достаточно проблематичным.

Таким образом, в настоящее время четко прослеживается тенденция увеличения количества преступлений, совершаемых с использованием ИТС и в ближайшей перспективе изменения данной тенденции, не предвидится.

Специфика преступлений определяется использованием при их совершении высоких технологий, необходимостью обладания определенным уровнем специальных познаний и наличием специального инструментария для их совершения. Данные обстоятельства обусловливают высокую латентность этих преступлений, что существенно затрудняет их выявление и документирование, а также организацию уголовно-процессуального противодействия им.

Основными особенностями преступлений, совершаемых с использованием ИТС, являются иные механизмы следообразования, и, соответственно перед правоохранительными органами ставится проблема их выявления и фиксации.

Также особенностью является отсутствие привязки совершения активных преступных действий к месту наступления последствий, т.е. дистанционный характер совершения преступлений.

Исходя из этого, представляется целесообразным разрабатывать новые способы противодействия такой категории преступлений.

Способы противодействия можно условно разделить на внутригосударственные и межгосударственные. К внутригосударственным способам противодействия можно отнести совершенствование криминалистических тактик и методик расследования, а также выработку новых требований к сбору, проверке и оценке доказательств при расследовании преступлений, совершенных с использованием ИТС.

Применительно к Российской Федерации представляется целесообразным значительное внимание уделять разработке тактики проведения таких следственных действий, как осмотр места происшествия, обыск (выемка) контроль телефонных и иных переговоров, допрос.

Специфика проведения осмотра места происшествия, а также обыска или выемки предполагает тщательную предварительную подготовку к нему, привлечение специалистов соответствующего профиля, использование, кроме стандартных технико-криминалистических средств, также специальных технических устройств и программного обеспечения, принятия мер, направленных на обеспечение сохранности компьютерной информации [3].

Также необходима выработка рекомендаций по изъятию, упаковке и транспортировке компьютерной техники и иных носителей информации, обнаруженных в ходе данных следственных действий.

Проведение такого следственного действия, как контроль телефонных и иных переговоров по уголовным делам может способствовать выявлению мест нахождения используемой компьютерной техники, иных незаконных предметов, документов (в частности электронных).

При проведении допроса значительное внимание необходимо уделять вопросам использования в преступных целях ИТС.

Учитывая, что к ИТС практически неприменим принцип территориальности, то расследование такого рода преступлений лишь на национальном уровне малоэффективно. В связи с тем, что во многих случаях поставщики информационно-телекоммуникационных услуг зарегистрированы, как отмечено выше, на территории иностранных государств, одним из важнейших вопросов в сфере противодействия преступлениям, совершаемым с использованием ИТС, является необходимость совершенствования международного сотрудничества, в том числе в сфере уголовного процесса.

В настоящее время основной формой международного сотрудничества в уголовно-процессуальной сфере является направление запросов о правовой помощи. Порядок взаимодействия российских судов, прокуроров, следователей и органов дознания с соответствующими компетентными органами и должностными лицами иностранных государств регламентирован главами 53, 54 и 55 УПК РФ.

Международная правовая помощь по уголовным делам может оказываться в случаях, когда возникает необходимость производства на территории иностранного государства таких следственных действий, как осмотр, обыск (выемка), допрос, экспертиза либо иных процессуальных действий. В частности, когда обвиняемый (подозреваемый) скрывается на территории другого государства, либо в случаях, когда свидетели, потерпевшие или иные участники уголовного судопроизводства, а также документы, необходимые для расследования, находятся на территории другого государства.

Представляется необходимым развивать международное сотрудничество в уголовно-процессуальной сфере, в особенности по преступлениям, совершаемым с использованием ИТС. Так, целесообразно предусмотреть упрощенный порядок трансграничного взаимодействия с поставщиками информационно-телекоммуникационных услуг с целью получения от них данных об абонентах, траффике и контенте коммуникаций. Основной целью выработки упрощенных порядков должна выступать оперативность исполнения запроса о правовой помощи, т. е. получение запрашиваемой информации должно осуществляться в максимально короткие сроки, что напрямую влияет на эффективность расследования вышеуказанных преступных проявлений.

Проведенное исследование позволило сформулировать вывод о том, что с целью эффективной реализации правоохранительной функции государства в сфере борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей (в том числе сети Интернет), необходимо совершенствование криминалистических тактик и методик их расследования, выработка новых требований к сбору, проверке и оценке доказательств по уголовным делам указанной категории, а также дальнейшее развитие международного сотрудничества, в том числе в области уголовного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации: федеральный закон от 29.12.2006 № 244-ФЗ (ред. от 28.03.2017) // Рос. газ. - 2006. - № 297. - 31 дек.
2. О направлении методических материалов: письмо Минобрнауки России от 31.03.2017 № ВК-1065/07 // СПС «КонсультантПлюс».
3. Давыдов В.О. Информационное обеспечение раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием компьютерных сетей: автореф. дис. ... канд. юрид. наук. - Ростов н/Д., 2013. - 26 с.
4. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. - 2008. - № 2. - С. 44-46.
5. Торговченков В.И., Иванов С.А. Особенности предупреждения бесконтактных способов сбыта наркотических веществ в Российской Федерации // Законы России: опыт, анализ, практика. - 2016. - № 12. - С. 84-88
6. Хохлов Ю.П. Этот опасный Интернет. Генеральная прокуратура Российской Федерации реализует комплекс мер, направленных на обеспечение профилактики экстремизма и терроризма // Прокурор. - 2015. - № 3. - С. 15-19.
7. Чекунов И.Г. Киберпреступность: Понятие и классификация // Рос. следователь. - 2012. - № 2. - С. 37-44.

УДК 004.056.5

РАЗРАБОТКА МЕТОДОВ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕРРИТОРИАЛЬНОМ ОРГАНЕ МВД РОССИИ

Родин Владимир Николаевич, Каупенас Денис Вячеславович
Санкт-Петербургский университет МВД России
ул. Летчика Пилютова, 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, zenitovich@gmail.com

Аннотация: в статье рассматриваются основные методы, посредством применения которых представляется возможным улучшение качества защищенности систем информационной безопасности в территориальных органах МВД России, а также варианты реализации представленных методов. Материал содержит анализ научной литературы, связанной с рассматриваемой тематикой статьи, предложены различные варианты совершенствования систем информационной безопасности в территориальных органах МВД России. Рассматривая методы повышения уровня защищенности систем информационной безопасности, автор акцентируют внимание на существующих проблемах, с которыми сталкиваются практические работники в рассматриваемой области.

Ключевые слова: разработка; метод; уровень защищенности; система; информационная безопасность.

DEVELOPMENT OF METHODS TO INCREASE THE LEVEL OF SECURITY OF THE INFORMATION SECURITY SYSTEM IN THE TERRITORIAL ORGANIZATION OF THE MIA OF RUSSIA

Rodin Vladimir, Kaupenas Denis
[1]St. Petersburg University of the Ministry of Internal Affairs of Russia
st. pilot Pilyutova, 1, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, zenitovich@gmail.com

Absrtact: The article discusses the main methods through the use of which it seems possible to improve the quality of security of information security systems in the territorial bodies of the Ministry of Internal Affairs, as well as options for implementing the methods presented. The material contains an analysis of scientific literature related to the subject of the article under consideration, various options for improving information security systems in the territorial bodies of the Ministry of Internal Affairs are proposed. Considering methods of increasing the level of security of information security systems, the author focuses on the existing problems faced by practitioners in the area under consideration.

Key words: development; method; security level; system; information security.

Однажды небезызвестный немецкий банкир Н. М. Ротшильд произнес крылатую фразу, до сих пор будоражащую умы поколений: «Кто владеет информацией – владеет миром». И сейчас эта фраза становится актуальной как никогда раньше. В условиях современного быстроразвивающегося информационного общества, где информация является важнейшим аспектом жизнедеятельности людей, встает острый вопрос о том, как обеспечить целостность и конфиденциальность главной «единицы» нашего времени – информации [1]. Именно такова главная задача систем информационной безопасности. Когда люди слышат слово «безопасность», первая ассоциация с этим словом, что приходит им в голову – это полиция. Ведь именно полиция является главным защитником простых людей от преступных посягательств и обеспечивает их безопасность круглосуточно. Однако порой сами полицейские нуждаются в защите. Точнее не полицейские, а информация, которой они оперируют. Как уже было описано выше, информация сегодня одна из главных ценностей, этакая современная «валюта». Утечка или утрата ее равносильна денежным убыткам, а следовательно таких утрат необходимо избегать, тем более когда речь идет об информации, хранящейся в базах данных территориальных органов МВД России, ведь такая информация зачастую важна и конфиденциальна, а ее утрата или утечка может повлечь за собой необратимые последствия, куда более опасные не только для обладателя информации (в данном случае – МВД России), но и для общества в целом, нежели проблемы с доступностью, целостностью и конфиденциальностью какой-либо другой информации, ведь хорошо осведомленный преступник – втройне опасен и представляет повышенную угрозу для законопослушных граждан, общества и государства [2].

Возвращаясь к понятию системы информационной безопасности, дадим ему определение. Итак, систему информационной безопасности можно определить как совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение. Такой системой должно обладать любое предприятие или организация и, разумеется, таковая система присутствует и в ОВД. Каждый территориальный орган полиции имеет свою собственную систему информационной безопасности, которая спроектирована и структурирована в соответствии общепринятому стандарту, но все же отличается в зависимости от информации, которая обрабатывается и защищается системой [3].

Каждый год объем информации растет и обеспечивать ее защиту становится все труднее. Появляются новые угрозы и вызовы со стороны нарушителей, и системы информационной безопасности должны им не уступать, дабы обеспечить соответствующий уровень безопасности. Для этого необходимо не только знать существующий перечень угроз, но и, по возможности прогнозировать будущие угрозы и заранее быть к ним готовыми.

Современные системы информационной безопасности строятся на основе следующих положений: определение степени и группы защищаемой информации и перечня лиц, ответственных за ее защиту и имеющих право доступа к ней. В дальнейшем определение этих двух групп позволит соотнести уже на программном уровне, выстраивая степени дифференциации доступа, модель системы информационной безопасности в соответствии с установленными нормативно-правовыми актами.

На сегодняшний день, система информационной безопасности в территориальных органах в большинстве случаев обеспечивает приемлемый уровень безопасности информации, однако, с связи с недостатком финансирования и нехватки специалистов на местах, системы информационной безопасности далеко не совершенны и требуют доработок.

В связи с этим предлагается разработать перечень методов, которые смогут повысить уровень защищенности таких систем информационной безопасности, и, как следствие, усовершенствовать защиту информации, обращающейся в территориальных органах, а также улучшить качество работы с ней соответствующих специалистов [4, 5].

В качестве таких методов можно указать:

1. Совершенствование инфраструктуры. Довольно объемный метод, включающий в себя множество направлений. В роли примера можно рассмотреть развертывание межсетевых экранов во всех офисах и подразделениях, что позволит обеспечить базовую защиту информации, с которой работают сотрудники. Также укажем установление антивирусного программного обеспечения не только на физических, но и вообще всех серверах, а именно почтовом сервере, шлюзе доступа, файловом сервере и сервере резервного копирования. На них, как правило, не всегда установлено антивирусное программное обеспечение. Рекомендуется рассмотреть возможность развертывания многофакторной проверки подлинности для VPN-соединений, в настоящий же момент используется доменная авторизация. Это лишь немногие и наиболее простые из основных направлений в рамках данного метода, которые помогут обеспечить защищенность информации на приемлемом уровне.

2. Качественное улучшение знаний и навыков сотрудников, увеличение количества специалистов, подготовка кадров. Очевидный, но очень важный метод, ведь, как правило, подавляющее большинство утечек информации и проблем с безопасностью происходят по вине слабо подготовленного персонала. Так, в качестве примеров реализации данного направления можно указать: разработка плана обучения сотрудников подразделения по вопросам безопасности и работы с информацией; создание политики по уведомлению сотрудников о вопросах безопасности для своевременного информирования об угрозах в ИТ среде. Такая политика должна разрабатываться в зависимости от объема и вида информации, который обрабатывается в конкретном территориальном органе.

3. В качестве третьего направления необходимо указать правовой аспект. Объемы информации и способы ее несанкционированного получения увеличиваются практически ежедневно. МВД России – государственный аппарат, следовательно, его подразделения обязаны осуществлять свою деятельность в соответствии с принятыми законодательными актами как общими, так и ведомственными. Но информационное направление слишком быстро развивается, можно разрабатывать закон, а затем принять его, на что уйдет драгоценное время, в течении которого возникшая актуальная проблема может не решаться с помощью уже принятых НПА, а информационная безопасность будет уязвима и нестабильна. Следовательно, для решения данной проблемы необходимо дать возможность территориальным органам на местах издавать собственные локальные нормативно-правовые акты, чтобы более оперативно и своевременно решать возникшие проблемы. Естественно, такие акты не должны противоречить уже существующим. Также рекомендуется усовершенствовать уже существующие законы в соответствии с современными реалиями.

Таким образом, резюмируя все вышеописанное, можно сделать вывод о том, что, если анализировать текущее состояние информационной безопасности в подразделениях полиции, то можно сказать, что эти подразделения в большинстве случаев обеспечивают приемлемый уровень безопасности информации, однако уровень защищенности их систем информационной безопасности необходимо повышать и зачастую в этом направлении лучше работать «на перспективу». Также следует увеличить материальное обеспечение и совершенствовать подготовку будущих специалистов. В тезисе приведены лишь основные, наиболее доступные и простые в реализации методы совершенствования защищенности систем информационной безопасности в территориальных органах МВД России, их перечень куда более широк и сложен, чтобы описать его в рамках одной статьи, однако, реализовав хотя бы те методы, которые были указаны, информационная безопасность в МВД России в целом выйдет на качественно новый, улучшенный уровень.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.
2. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
3. ГОСТ Р 53114-2008, «Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 № 532-ст).
4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. -- М.: РИОР: ИНФРА-М, 2015. – 315с.
5. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности -- Альпина Паблишерз, 2011. – 338 с.

УДК 004.04

РОЛЬ ИНФОРМАТИЗАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Родин Владимир Николаевич, Крылова Арина Евгеньевна
Санкт-Петербургский университет МВД России
ул. Летчика Пилютова, 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, rinka-99@mail.ru

Аннотация: огромный поток информации поступает в органы внутренних дел, данная информация содержит сведения о состоянии преступности и общественного порядка, поэтому для быстрой обработки информации крайне необходимо обеспечение информатизации в органах внутренних дел.

Ключевые слова: информатизация, информационные технологии, Министерство внутренних дел Российской Федерации, органы внутренних дел, правоохранительные органы.

ROLE OF INFORMATIZATION IN THE INTERNAL AFFAIRS

Rodin Vladimir, Krylova Arina
St. Petersburg University of the Ministry of Internal Affairs of Russia
st. pilot Pilyutova, 1, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, rinka-99@mail.ru

Absrtact: a huge flow of information enters the internal affairs bodies, this information contains information about the state of crime and public order, and therefore, for the rapid processing of information, it is extremely necessary to ensure informatization in the internal affairs bodies.

Key words: informatization, information technology, the Ministry of Internal Affairs of the Russian Federation, internal affairs bodies, law enforcement agencies.

Правоохранительные органы являются одним из основных элементов государства, поэтому информационные технологии активно внедряются в профессиональную деятельность органов внутренних дел В правоохранительных органах создают специальные информационные базы, куда заносят различные статистические показатели, каковые позволяют обмениваться данными на удаленных расстояниях, что играет важную роль в ускорении расследования правонарушений.Главной целью информатизации считается повышение эффективности оперативно-служебной и служебно-боевой работы органов внутренних дел на основе

применения нынешних информационных технологий, научного и научно-технического обеспеченья системы МВД Российской Федерации.

Основными задачами информатизации ОВД считаются:

– формирование общей информационно-телекоммуникационной инфраструктуры МВД Российской Федерации, обеспечивающей создание единого информационного пространства, необходимый уровень информационной безопасности;

– разработка, внедрение и развитие общей информационно-телекоммуникационной инфраструктуры МВД Российской Федерации;

– разработка новых и модернизация существующих информационных ресурсов (ИР);

– формирование возможностей для информационного взаимодействия;

– обеспечение комплексной автоматизации управления ОВД на основе создания ситуационных центров управления [1].

Повышение уровня информатизации Министерства внутренних дел Российской Федерации на основе общей информационной инфраструктуры ОВД призвано обеспечить скорость формирования, достоверность и полноту информации, содержащейся в автоматизированных банках данных АТС. В процессе информатизации постоянно совершенствуются межведомственный и ведомственный обмен информацией, гармонизация данных, сокращение избыточности и устранение дублирования первичной входной информации, а также сокращение документооборота.

Кроме того, информационная поддержка ОВД предназначена для:

– обеспеченья соответствия требованиям комплексной защиты информации;

– обеспеченья необходимого уровня стабильности, непрерывности, эффективности и скрытности управления;

– повышения качества управленческих решений и сокращения продолжительности цикла управления на основе эффективного использования информационных технологий и аналитических возможностей ситуационных центров.

Меры по компьютеризации органов внутренних дел позволяют повысить уровень информационного обеспеченья процесса раскрытия и расследования правонарушений и предотвращения правонарушений путем своевременного получения сотрудниками органов внутренних дел в реальном времени точной и достоверной оперативной информации, следственной и криминалистической информации, интегрированной в системы МВД России.

В настоящее время ни одно уголовное дело не расследуется без информационной поддержки со стороны служб, каковые проводят судебно-медицинские экспертизы. Информационная поддержка для правоохранительных органов позволяет принимать обоснованные тактические и процедурные решения, успешно внедрять данные. Информация не может быть передана, получена либо сохранена в чистом виде. Его носитель считается закодированным сообщением эквивалентом события, записанного источником информации и выраженного через последовательность условных физических символов (алфавитов), образующих упорядоченный набор. Связь осуществляется по каналам связи, по которым сообщения могут передаваться лишь в приемлемой для них форме.

Используемая в органах внутренних дел информация содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. В дежурных частях, у оперативных сотрудников, участковых уполномоченных полиции, следователей, сотрудников экспертно-криминалистических подразделений, других подразделений на документах первичного учета, в учетных журналах и на других носителях накапливаются массивы данных оперативно-розыскного и оперативно-справочного назначения.

Информационные центры МВД считаются важнейшим звеном в системе информационного обеспеченья органов внутренних дел Российской Федерации. Они несут основное бремя оказания информационной поддержки органам внутренних дел по раскрытию и расследованию правонарушений, розыску преступников. Информационные центры считаются основными подразделениями в системе Министерства внутренних дел в области информатизации: предоставление статистической, оперативной справочной, оперативно-розыскной, криминалистической, архивной и другой информации, а также компьютеризация и формирование региональной информационно-компьютерной информации, сети и интегрированные банки данных.

Централизованные оперативно-справочные, криминалистические и поисковые записи содержат следующую информацию о гражданах Российской Федерации, иностранцах и лицах без гражданства:

– судимость, место и время отбывания наказания, дата и основания для освобождения;

– движение заключенных;

– смерть в местах лишения свободы, смена приговора, амнистия, количество уголовных дел;

– место жительства и место работы до осуждения;

– кровь и отпечатки пальцев заключенных.

Отпечатки пальцев позволяют идентифицировать преступников, арестованных, задержанных, а также неизвестных пациентов и неопознанные трупы [2].

Эффективность борьбы с преступностью определяется уровнем организации оперативно-розыскной и профилактической работы, проводимой органами внутренних дел. В свою очередь, результаты этой работы

зависят от качества информационной поддержки, поскольку основные усилия практиков по расследованию, раскрытию и предупреждению правонарушений так либо иначе связаны с получением необходимой информации, эти функции призваны обеспечить информационную систему для органы внутренних дел, каковые в настоящее время поддерживают значительный объем информации. В целом органы внутренних дел Российской Федерации в автоматизированном режиме с применением компьютеров решают задачи оперативно-розыскного и справочного назначения, а также задачи бухгалтерского, статистического, управленческого и производственно-экономического назначения. Без использования самых нынешних технических средств эффективность следственных действий в сфере высоких технологий резко снизится. В работы подразделений органов внутренних дел может применяться как универсальное, так и специальное программное обеспечение.

Универсальные программы (информационно-поисковые системы, редакторы, электронные таблицы и так далее) общего назначения не только повышают производительность и эффективность в выявлении, раскрытии и расследовании правонарушений, но и поднимают его на совершенно новый уровень.

Специализированные программы могут быть ориентированы на их непосредственное применение при осуществлении оперативно-розыскных мероприятий в направлении противодействия информационной (в том числе компьютерной) преступности.

Следует отметить, что решение задач поиска, отбора и систематизации такой информации предполагает применение интегрированной информационной системы, способной значительно расширить информационную базу, необходимую для информационно-аналитического обеспеченья, сократить возможности поиска и выбора источников информации, выявить аспекты, с помощью каковых анализировать информацию, а главное, в процессе аналитической обработки данных, обеспечить выявление сущности и динамики пространственно-временных и причинно-следственных связей между фактами, явлениями, процессами.

Таким образом, информационно-аналитическое обеспечение работы правоохранительных органов по борьбе с организованными формами преступной работы представляет собой систему, включающую два взаимосвязанных компонента информационная поддержка, которая заключается в изучении информационного спроса потребителей, поддержании стабильного состояния информационных отношений и аналитическое сопровождение, которое состоит в изучении криминальных угроз, выявлении причин и условий, влияющих на формирование ситуации, прогнозировании ее развития, изучении проблемных ситуаций в сфере борьбы с организованной преступностью.

СПИСОК ЛИТЕРАТУРЫ

1. Основы информационной безопасности в органах внутренних дел: учебное пособие / К.Л. Костюченко, А. В. Монахов. – Екатеринбург: Уральский юридический институт МВД России, 2009. – 93 с.
2. Организация безопасности информации в органах внутренних дел Российской Федерации [Текст]: лекция / В. А. Макаров ; ВИПК МВД Рос., Центр изучения проблем доп. И проф. Образ. – Домодедово: ВИПК МВД России, 2013. – 31с.

УДК 004.056.53

НАПРАВЛЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Родин Владимир Николаевич, Маричева Евгения Владимировна
Санкт-Петербургский университет МВД России
ул. Летчика Пилютова, 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, marichevazhenya@gmail.com

Аннотация: в статье рассматривается одна из основных проблем в обеспечении защиты информации, а именно защита от несанкционированного доступа, возможность решения проблемы посредством применения встроенных и дополнительных средств защиты информации. Статья содержит анализ нормативно-правовых актов и научной литературы, связанной с тематикой статьи.

Ключевые слова: информационная безопасность; несанкционированный доступ; операционная система; система защиты информации.

DIRECTION OF PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS

Rodin Vladimir, Maricheva Eugenia
St. Petersburg University of the Ministry of Internal Affairs of Russia
st. pilot Pilyutova, 1, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, marichevazhenya@gmail.com

Abstract: The article deals with one of the main problems in ensuring information security, namely protection from unauthorized access, the possibility of solving the problem by using built-in and additional information security tools. The article contains an analysis of legal acts and scientific literature related to the subject of the article.

Key words: information security; unauthorized access; operating system; information security system.

Для каждого очевидно, что человечество в своем развитии никогда не двигается назад. Стараясь использовать все знания, накопленные ранее, общество не стоит на месте, развивается и прикладывает все усилия для автоматизации многих процессов жизнедеятельности. Прогресс в области автоматизации всех процессов нашей жизни невозможно оспаривать. Развитие в области техники, а именно с точки зрения методики ее

обслуживания и организации труда, приносит в нашу жизнь проблемы, напрямую связанные с информационной безопасностью.

В Доктрине информационной безопасности Российской Федерации указано на то, что одним из определяющих направлений обеспечения информационной безопасности является обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Угроза информационной безопасности Российской Федерации - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере [1]. Возникает серьезная проблема несанкционированного доступа, требующая разрешения.

ГОСТ Р 53114-2008, «Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» устанавливает основные термины, применяемые при проведении работ по стандартизации в области обеспечения информационной безопасности в организации. В нем под несанкционированным доступом понимается доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них. [2].

Для предотвращения несанкционированного доступа создаются системы защиты информации, как от случайного, так и от преднамеренного искажения, хищения или уничтожения информации. Системы защиты информации совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации [3]. Они представляют собой одну из подсистем интегрированной системы безопасности объекта защиты, и в свою очередь состоят из ряда подсистем, в основе которых находятся комплексы законодательных, организационных, технических методов и средств. В зависимости от особенностей объекта защиты система защиты информации включает в свой состав то или иное подмножество методов и средств.

Большинство операционных систем уже оснащены подсистемы защиты от несанкционированного доступа, другой вопрос в эффективности их работы. Такой подсистемой можно назвать, например, механизм аутентификации пользователя при входе в учетную запись операционной системы Windows или Linux. Вместе с тем перечень механизмов защиты операционной системы может быть очень обширным, к ним можно отнести:

- механизмы защиты от исправления ядра;
- ограничения режимов работы служб;
- предотвращение выполнения нежелательных данных;
- случайное распределение адресного пространства и уровней целостности [4].

Также к ним можно отнести немаловажные части комплексной защиты, такие как: упрощенный контроль учетных записей; обеспечение безопасности универсального доступа; защита пользователей и инфраструктуры от вторжений и вредоносного программного обеспечения. При условии, что эти подсистемы являются встроенными для того, чтобы грамотно и эффективно ими пользоваться, от пользователя требуется высокий уровень компетенции в работе с ними. При этом наличие встроенных средств защиты не дает никакой гарантии безопасности данных.

Для упрощения работы пользователя и с целью снижения рисков неправильной настройки средств защиты информации, компанией «АЛТЭКС-СОФТ» было разработано стандартизированное семейство программ контроля и настройки сертифицированных версий Microsoft, получившее название «CHECK» [5]. Основным видом деятельности «АЛТЭКС-СОФТ» являются разработка, производство и внедрение сложных систем защиты для различного рода информационных систем на основе сертифицированных по требованиям безопасности решений, разработанных специалистами компании, а также ее партнеров. «CHECK» имеет своим назначением установление оценки соответствия условиям действия сертификатов и контроля защищенности информационных систем, организованных в Microsoft. Кроме того программы могут быть применены в любых системах, где необходим высокий уровень обеспечения безопасности информационных ресурсов. Реализованный перечень возможностей данных программ повышает эффективность использования встроенных механизмов защиты, правильно выполняя настройку параметров безопасности и безопасную эксплуатацию продуктов Microsoft. Сейчас различают два основных направления семейства «CHECK»: Net_Check и RedCheck.

Net_Check представлена в виде программного средства для централизованного контроля, настройки и обновления механизмов безопасности сертифицированных программных продуктов Microsoft в сети одного предприятия.

Программа RedCheck лицензируется по количеству проверяемых IP-адресов. Если необходимо рассмотреть корпоративный вариант исполнения данной программы, то он включает в себя четыре подвида:

RedCheck Base – начальная версия программы, где есть все необходимые инструменты для полноценной работой с вариантами уязвимости и обновлениями в Windows и Linux системах. Круг ее полномочий очень широк, это контроль целостности, сетевые проверки, процедуры, выполнение которых обеспечивает повседневный контроль защищенности информационных систем.

RedCheck Professional – полностью функционирующая версия, позволяющая использовать широкий спектр возможностей для выполнения мониторинга и управления защищенностью сетей корпоративного уровня.

RedCheck Professional для сертифицированных версий Microsoft – аналогична предыдущей версии, но также дополнена возможностью управлять конфигурациями и установкой обновлений для сертифицированных по требованиям безопасности версий Microsoft.

RedCheck Enterprise – этот вариант использует все имеющиеся возможности программы и ориентирована на распределенные информационные системы с возможностью неограниченного масштабирования.

С развитием информационного общества появилось большое количество операционных систем, сейчас компания Microsoft далеко не единственный их производитель. Поиск средств контроля и настройки средств защиты информации, аналогичных системе контроля «CHECK», для операционных систем других производителей результатов не дает. Получается, что современные операционные системы российского или зарубежного производства требуют доработки со стороны безопасности их использования, а в первую очередь, именно с точки зрения возможности несанкционированного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом президента Российской Федерации от 5 декабря 2016 г. № 646.
2. ГОСТ Р 53114-2008, «Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 № 532-ст).
3. ГОСТ Р 50922-2006, « Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст).
4. Щербинина И.А., Леонтьева Н.А. Сравнительный анализ возможностей средств защиты информации от несанкционированного доступа в соответствии с приказом ФСТЭК России № 21 от 18 февраля 2013 г // Россия молодая: передовые технологии - в промышленность! 2015. № 2. С. 299-306.
5. Программы контроля «Check». // [Электронный ресурс]. Режим доступа: https://www.altx-soft.ru/groups/page-267.htm. Дата обращения: 16.09.2020.

УДК 004.056.5

СОВЕРШЕНСТВОВАНИЕ СОСТАВА И ФОРМ КАДРОВЫХ ДОКУМЕНТОВ В ОРГАНИЗАЦИИ, ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Родин Владимир Николаевич, Шапчук Мария Константиновна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Лётчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: vl.rodin@mail.ru, shapchuk.m@yandex.ru

Аннотация. Рассматривается вопрос автоматизации кадрового делопроизводства, совершенствования состава и форм кадровых документов в организации, а также определены специфические черты подхода к применению информационных технологий.

Ключевые слова: управление; документ; делопроизводство; кадровый документ; кадровое делопроизводство; информационные технологии.

IMPROVEMENT OF COMPOSITION AND FORMS OF PERSONNEL DOCUMENTS IN THE ORGANIZATION, IMPLEMENTATION OF INFORMATION AND COMPUTER TECHNOLOGIES

Rodin Vladimir, Shapchuk Maria
Saint Petersburg University of the Ministry of internal Affairs of the Russian Federation
Pilyutov's pilot 1 St., Saint Petersburg, 198206, Russia
e-mail: vl.rodin@mail.ru, shapchuk.m@yandex.ru

Abstract. The issue of automation of personnel records management, improving the composition and forms of personnel documents in the organization is considered, and specific features of the approach to the use of information technologies are also identified.

Keywords: management; document; paperwork; personnel document; personnel paperwork; information technology.

В современном мире применение в управлении информационных технологий, обладающих высокой гибкостью, мобильностью и способностью приспосабливаться к различным условиям работы, является непременным условием повышения эффективности управленческого труда. Отсюда следует, что квалифицированный и профессиональный работник должен уметь не только правильно составлять и оформлять сами документы, но и должен знать, через какие именно процедуры и стадии проходят эти документы. Должен

обладать таким навыком, как правильное составление и оформление документов в соответствии с требованиями законодательства – главная обязанность работников делопроизводственных служб [1]. В число функций, выполняемых службой отдела кадров, входит совершенствование форм и методов работы с документами, и в рамках этой функции служба отдела кадров занимается совершенствованием форм документов, применяемых в деятельности учреждений как по составу, так и по форме.

Эффективность системы управления персоналом на примере любой организации во многом зависит от правильно выстроенной работоспособности самой организации и действий кадрового делопроизводства. Каждый работодатель, вне зависимости от того, юридическое или физическое это лицо, в процессе осуществления хозяйственной деятельности всегда сталкивается с вопросами организации труда, управления трудовыми отношениями между работниками и работодателем и регламентированием этих процессов.

В процессе исследования темы были изучены различные виды кадровых документов, состав и их формы, а также порядок и особенности их оформления. Необходимо разобраться, что же такое кадровая документация как единое целое и из чего она состоит [2].

Делопроизводство – это отрасль деятельности, которая обеспечивает документирование и организацию работы с официальными документами. Отсюда следует, что кадровое делопроизводство — это более узкое понятие, подразумевающее организацию работы с документами, которые затрагивают кадровые вопросы.

Кадровая документация – это совокупность форм, отражающих наличие и движение трудовых ресурсов. Отметим, что кадровое делопроизводство – отрасль деятельности, документирующая трудовые отношения. В свою очередь, кадровая документация фиксирует информацию о наличии и движении персонала, в ходе которой все кадровые процедуры приобретают документальное оформление (прием, перевод, поощрение, применение дисциплинарного взыскания, командировка, отпуск, увольнение и многое другое). Информация, облеченная в форму документа, составляет основу управления. А именно информация фиксируется в документах, которые придают ей организационную форму и перемещают во времени и пространстве. Стоит отметить, что документы и документированная информация являются материальным воплощением управленческих решений, придают им юридическую силу.

Как ранее было отмечено, что любая кадровая документация свидетельствует о том, что любой кадровый документ фиксирует юридически значимые факты, которые являются основанием совокупности корреспондирующих друг другу прав и обязанностей работника и работодателя, что в свою очередь является ключевым элементом работоспособности любой организации. Например, должностная инструкция является документом, подтверждающим правомочия должностного лица на совершение юридически значимых действий, входящих в его должностные обязанности. Кроме того, с помощью некоторых кадровых документов, используемых в качестве важных письменных доказательств, работодатель может с легкостью доказать свою правоту в суде [3].

Комплекс кадровых документов можно представить в виде системы, которая включает в себя следующие, связанные единством происхождения и различающиеся по функциональному назначению группы документов: организационно-правовая документация, персональная документация, договорная документация, распорядительная документация, учетная кадровая документация, информационно-справочная документация. Состав документов кадровой службы значительно шире, он также может включать в себя переписку с другими сторонними организациями, контролирующими организациями, отчетную, плановую документацию, а также значительный объем нормативной и нормативно-справочной документации.

Перейдем к рассмотрению конкретного примера.

В компании ООО «XXX» работают 700 специалистов кадрового администрирования, а именно:

– 400 сотрудников в отделе аутсорсинга кадрового администрирования;

– 100 сотрудников в отделе зарплатных процессов;

– 200 сотрудников в отделе оперативного хранения документов.

Рабочие места специалистов автоматизированы следующими программными средствами [4]:

1. Neocase Power – французская разработка электронного документооборота. Программа предназначена для оформления заявок на прием, перевод, увольнение и прочие кадровые процессы. Преимуществом данной программы является возможность работы в удаленном доступе, высокая скорость обработок входных документов на прием, увольнение и т.д.

2. SAP ERP Human Capital Management («Управление человеческим капиталом») – программа позволяет синхронизировать и оптимизировать все бизнес-процессы управления персоналом в соответствии с локальными требованиями законодательства и бизнеса.

С помощью данного решения один специалист кадрового администрирования может за восьмичасовой рабочий день провести 20 мероприятий приема на работу, более 45 увольнений и 50 переводов.

В целом 450 специалистов в день проводят более 49 000 кадровых операции в программе. Формируется около 1500 кейсов на прием, 4000 кейсов на увольнение и более 5000 кейсов на переводы сотрудников [5].

Такие большие цифры возможны только благодаря использованию унифицированных форм документов: приказы о приеме, увольнении, переводах; трудовой договор; договор материальной ответственности; согласие на обработку персональных данных; личная карточка Т2; расчетный лист; различные дополнительные соглашения. Использование унифицированных форм уменьшает трудозатраты специалистов и количество ошибок в кадровой документации.

3. Корпоративный сайт «Битрикс24» – облачная система, предназначенная для более эффективного выполнения совместной работы, в основе которой лежит идея социального Интернета. Внедрение «Битрикс24» позволило сотрудникам ставить себе задачи через сайт, получать задания от руководителя, передавать их часть своим коллегам, создавать отчеты, выполнять другие бизнес-процессы на сайте (например, через данный сайт сотрудников знакомят с новыми локальными актами организации).

4. Outlook.com – почтовый ящик от корпорации Microsoft, который позволяет безопасно обмениваться электронными письмами и любого рода информацией.

5. Сайт https://www.x5.ru. На данном сайте есть разделы, которые являются обязательными для просмотра сотрудниками компании, а именно нормативные акты и новостная лента.

За неиспользование программ «Битрикс24» и сайта x5 сотрудников лишают премии, так как на данных ресурсах выкладываются новые внутренние документы, регламентирующие работу компании. Рекомендуется включение двух указанных ресурсов в должностную инструкцию специалистов для более эффективной работы с ними.

Работа в данных программных средствах не только облегчает ведение кадрового делопроизводства, но и снижает трудозатраты на создание кадровой документации, а также риск возникновения ошибок.

Таким образом, на сегодняшний день существует множество различных программных продуктов, позволяющих вести управление документами, что упрощает работу и повышает эффективность документооборота.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. Приказом Росстандарта от 08.12.2016 № 2004-ст) (ред. от 14.05.2018) (в редакции от 14.05.2018)
2. Барихин А.Б. Делопроизводство и документооборот: [практическое пособие: подготовка и оформление документов, особенности составления отдельных документов, документы, содержащие коммерческую тайну, организация работы, систематизация и хранение] / А.Б. Барихин - 2-е изд., перераб. и доп. - М.: Кн. мир, 2018. – 415 с.
3. Белов А.Н. Делопроизводство и документооборот: учебное пособие / А.Н. Белов, А.А. Белов - 6-е изд., перераб. и доп. - М: Эксмо, 2017. – 553 с.
4. Рогожин М.Ю. Документы кадровой службы предприятия практическое пособие/ М.Ю. Рогожин. - М.: ГроссМедиа, 2010. – 281 с.
5. Филина Ф.Н. Практический универсальный справочник работника кадровой службы. - М.: ГроссМедиа, 2011. – 242 с.

УДК 004.491

ПРЕСТУПЛЕНИЯ В СФЕРЕ IT-ТЕХНОЛОГИЙ НА СОВРЕМЕННОМ ЭТАПЕ

Родин Владимир Николаевич, Ципанович Анастасия Владимировна
Санкт-Петербургский университет МВД России
ул. Летчика Пилютова, 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, nastea0797@mail.ru

Аннотация: В статье рассматриваются основные причины возникновения IT-преступлений, способы борьбы с использованием информационных технологий в сфере незаконного оборота наркотиков. Материал содержит анализ научной литературы, связанной с рассматриваемой тематикой статьи, предложены различные варианты совершенствования раскрытия IT-преступлений.

Ключевые слова: IT-преступления, Dark Web, АИС «Незаконный оборот наркотиков», компьютерные преступления, взлом, фишинг.

CRIMES IN THE FIELD OF IT-TECHNOLOGIES AT THE PRESENT STAGE

Rodin Vladimir, Tsipanovich Anastasia
St. Petersburg University of the Ministry of Internal Affairs of Russia
st. pilot Pilyutova, 1, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, nastea0797@mail.ru

Abstract: The article discusses the main causes of IT crimes, ways to combat the use of information technologies in the field of drug trafficking. The material contains an analysis of the scientific literature related to the subject of the article, various options for improving the disclosure of IT crimes are proposed.

Key words: IT crimes, Dark Web, AIS «drug trafficking», computer crimes, hacking, phishing.

Современный человек не представляет свою жизнь без компьютера. Информационные технологии стремительно внедрились практически во все сферы деятельности людей. Однако многие вопросы защиты информации до сих пор не решены.

На ежегодном расширенном заседании коллегии Министерства Внутренних дел Российской Федерации, состоявшемся 26 февраля 2020 года, глава МВД Колокольцев В.А., отметил, что, несмотря на объективные сложности, связанные с расследованием IT-преступлений, раскрытых деяний данного вида за 2019 год увеличилось в полтора раза [5]. Однако показатель совершения преступлений данного типа все еще очень высок (68,5%).

К причинам возникновения компьютерной преступности можно отнести: информационно-технологическое переоборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением зарубежного производства, базами данных; а также реальную возможность получения значительной экономической выгоды от противоправных деяний с использованием ЭВМ.

С инновацией технических средств развивается вирусная база и сети взломщиков. На сегодняшний день взлом паролей, кража реквизитов кредитных карточек, различного рода фишинги, неправомерное противозаконное распространение информации через глобальную сеть стали очень популярными и зачастую остаются безнаказанными.

Еще один способ незаконного использования информационных технологий - бесконтактный сбыт наркотиков. Преступник размещает объявление на форуме или специальном сайте в доменной зоне. biz с помощью любых средств вычислительной техники: мобильного телефона, планшета, смартфона, персонального компьютера. Данный домен используется для различных услуг в сфере бизнеса.

Выйти на подобные объявления можно просто, через запрос в поисковиках или крупные форумы наркоторговцев. Большинство из них официально заблокированы в России, но всё еще доступны и активно работают через прокси сервер. Больше возможностей открывается, если попасть в Dark Web. Это некая группа вебсайтов, которые существуют в зашифрованном сетевом пространстве. На запрос «как попасть в Dark Web?» браузер нашел различные пошаговые руководства и инструкции, а также видео уроки.

Покупатель, заинтересовавшись объявлением, договаривается с продавцом и, обговорив детали, оплачивает товар через электронные платежные системы: «WebMoney», «Яндекс. Деньги», «Qiwi-кошелек»; либо перечисляет деньги через систему переводов, таких как: «Western Union», «UNIstream», а также используя крипто валюту – (Биткоин, Ethertum). Использование последней – создает большую сложность для идентификации преступников. После получения денег наркоторговец отправляет смс-сообщение покупателю о сделанной «закладке» с помощью мессенджеров, с использованием шифрования, например, Skype или WhatsApp.

В данных системах прослеживается ступенчатая иерархия, все функции участников преступной группировки четко распределены, продумана система безопасности, на которую инвестируется полученная от наркобизнеса прибыль. В такие преступные структуры обычно входят «закладчики» различных уровней, «вербовщики», «кладовщики», «курьеры», «операторы», «финансовый директор», программисты, координаторы и др. Хорошо зарекомендовавший и проявивший себя в работе сотрудник переводится на вышестоящие должности с увеличением заработной платы. В отношении «персонала», допустившего нарушения, применяются штрафы. Каждый сотрудник получает развернутые инструкции, в которых подробно описано, как правильно фасовать, хранить и перевозить наркотические средства, делать «закладки», общаться с потребителями наркотиков, как безопасно пользоваться электронными счетами и обналичивать денежные средства, как пользоваться анонимными средствами передачи информации через Интернет и анонимными иностранными прокси-серверами при посещении интернет-страниц и в общении между собой, как вести себя в случае задержания сотрудниками правоохранительных органов и т.д. Ряды нижестоящих звеньев постоянно пополняются посредством ведения грамотной и высокооплачиваемой работы в Интернете при минимальных временных затратах.

Подобные схемы сетевого наркобизнеса существенно затрудняют установление личностей наркодельцов и формирование доказательственной базы их причастности к преступной деятельности.

При расследовании преступлений связанных с незаконным оборотом наркотических средств и психотропных веществ, распространяемых посредством интернета объектом поиска будет выступать информация отражающая направленность умысла на приобретение или сбыт наркотических средств, психотропных или сильнодействующих веществ как непосредственно переписка приобретателя со сбытчиком, номера телефонов, паспортные и иные данные для совершения денежных переводов, иная информация, распространяемая через Интернет характеризующая направленность умысла на распространение или приобретение наркотиков [4].

Существует множество особенностей, которые должны учитываться при производстве следственных действий, при изъятии средств компьютерной техники, посредством которой распространялись наркотики. Так по прибытии на место производства следственного действия рекомендуется сразу же принять меры к обеспечению сохранности средств компьютерной техники и имеющихся на них данных и ценной информации. Для этого необходимо:

– не разрешать кому бы то ни было из лиц, работающих на объекте обыска прикасаться к средствам компьютерной техники с любой целью;

– не производить никаких манипуляций со средствами компьютерной техники, если результат этих манипуляций заранее не известен [3].

Возможно, причиной роста преступлений в сфере незаконного оборота наркотиков, совершенных с помощью информационных технологий, является отсутствие соответствующих законодательных норм, связанных с преступлениями в сфере компьютерной информации. На сегодняшний день, не предусмотрено уголовной ответственности за создание, администрирование программной среды, интернет-сайтов, форумов, на которых размещается информация о сбыте наркотиков и психотропных веществ. Однако, хочется отметить, что кражи и мошенничества с использованием IT-технологий переведены в категорию тяжких составов, что, естественно, сказалось на восприятии гражданами общей картины состояния тяжкой преступности в стране.

Безусловно, оперативными сотрудниками осуществляется ежедневный мониторинг поисковых сервисов и подозрительных сайтов и форумов, которые могли бы быть связаны со сбытом наркотических веществ. Так, в некоторых регионах России создана и внедрена автоматизированная информационная система «Незаконный оборот наркотиков» [2]. Информационная система представляет собой базу данных, в которую вносятся данные о сбытчике и обстоятельствах приобретения задержанным лицом наркотического средства.

Ее формирование происходит на основе учетных карточек, отображающих сведения о фигуранте уголовного дела и неустановленном лице, сбывшем ему наркотическое средство, с указанием используемых при сбыте логинов (никнеймов), IP-адресов, MAC-номеров, банковских счетов, электронных платежных системах, «Интернет-кошельках», а также мест закладок наркотических средств, изображенных на картах. База данных позволяет выявлять дополнительные эпизоды преступной деятельности изобличенного продавца наркотиков путем установления совпадений данных о сбытчиках по нескольким параметрам (по логинам, номерам телефонов, номерам счетов, через которые происходила оплата приобретаемого товара, и другое [1].

Однако до сих пор основной проблемой является сложность определения и поиска наркоторговцев, так как преступные группы в основном используют средства анонимизации, а также шифрование передаваемого трафика, для выявления которых необходимо внедрение качественно новых методов и технических средств обработки информации.

СПИСОК ЛИТЕРАТУРЫ

1. Морозов А.А. Особенности борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий. Публикация. Объединенной редакции МВД (Профессионал № 3, 2018 г.): http://www.ormvd.ru/pubs/102/drug-control/. Дата обращения: 16.09.2020.
2. Попов А.Н. Преступления в сфере компьютерной информации: учебное пособие / Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. – 68 с.
3. Вехов, В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пособие / В.Б. Вехов. – Волгоград: Перемена, 1998. – С. 31.
4. Е.С. Бикеева, Первоначальные следственные действия при расследовании незаконного оборота наркотиков через глобальные сети интернет: статья, 2018 г.
5. Интернет ресурс: https://mvdmedia.ru/news/official/sostoyalos-rasshirennoe-zasedanie-kollegii-mvd-rossii/ Дата обращения: 17.09.2020.

УДК 343.85

ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННЫМ СДЕЛКАМ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Саратов Дмитрий Николаевич, Мясников Илья Олегович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: saratovdn@mail.ru, unkownsmail@gmail.com

Аннотация. Рассматриваются способы противодействия совершению нелегальных сделок с использованием информационно-телекоммуникационных сетей и криптовалюты.

Ключевые слова: криптовалюта; незаконный оборот; способы противодействия; незаконные сделки.

ISSUES OF COUNTERING ILLEGAL TRANSACTIONS WITH THE USE OF CRYPTOCURRENCY

Saratov Dmitriy, Myasnikov Ilya
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
LetchikaPilyutova, st., 1, St. Petersburg, 198206, Russia
e-mail: saratovdn@mail.ru, unkownsmail@gmail.com

Abstract. Methods of counteracting illegal transactions using information and telecommunication networks and cryptocurrency are considered.

Keywords: cryptocurrency; illegal traffic; methods of counteraction; illegal transactions.

В своем выступлении на расширенном заседании коллегии МВД России 26 февраля 2020 года, В.А. Колокольцев отметил актуальную тенденцию увеличения числа количества преступлений, совершаемых с использованием информационно-телекоммуникационных сетей [1]. Непростая криминогенная обстановка осложняется использованием злоумышленниками последних достижений информатизации, в том числе, криптовалюты.

Однако, для того чтобы совершить сделку с использованием криптовалюты, злоумышленники также используют: мессенджеры с оконечным шифрованием, программы, обеспечивающие VPN-соединение, электронные платежные системы, программы, поддерживающие OTR-шифрование, а также имеющие специализированные хранилища информации с защитой от несанкционированного доступа [2]. В совокупности, все вышеперечисленные средства помогают участникам сделки сохранять анонимность и избегать поимки правоохранительными органами.

Преодоление противодействия раскрытию, оказываемого злоумышленниками при совершении сделок с использованием криптовалюты, предполагает комплекс различных мер, к которым можно отнести следующие.

1. Разработку и внедрение специальных программных продуктов, направленных на деанономизацию сделок с криптовалютой.

Начиная с 2016 г., в мире наблюдается постепенный отказ от использования криптовалюты Bitcoin и рост спроса на более анонимные валюты (Dah, Monero, ZCach). Снижение популярности Bitcoin объясняется тем, что в посреднических транзакциях по типу «человек в середине» Bitcoin позволяет отследить участников сделки и деанонимизировать их через использование общедоступных источников данных.

2. Блокировка сайтов, размещающих информацию о продаже предметов и веществ, запрещенных или ограниченных к обороту.

Например, на сегодняшний день одним из способов борьбы с незаконным оборотом наркотических средств в целом, и сбытом с использованием криптовалюты, в частности, является блокировка сайтов Роскомнадзором, который использует схему блокирования либо по IP адресу, либо по URL адресу.

По итогам 2018 г. МВД России рассмотрено свыше 7700 электронных обращений с жалобами на популярные социальные сети и онлайн-мессенджеры, где размещалась информация о подконтрольных веществах. За 6 месяцев 2019 г. – 21575 электронных обращений, по которым принято 12148 экспертных решений об ограничении доступа к интернет-ресурсам [3].

3. Разработка и принятие нормативных актов, направленных на противодействие незаконных сделок, совершенных с использованием криптовалют.

Подводя итоги вышеизложенного, можно сделать вывод:

а) использование криптовалюты при совершении преступных деяний обусловлено ее свойствами: децентрализацией, анонимностью, трансграничностью и высокой скоростью транзакций; возможностью обмена на другие криптовалюты или фиатные деньги;

б) отдельными мерами противодействия незаконным сделкам с использованием криптовалюты являются: внедрение специальных программных продуктов, направленных на деанономизацию сделок с криптовалютой; блокировка веб-сайтов, размещающих информацию о продаже предметов и веществ, запрещенных или ограниченных к обороту; внесение изменений и дополнений в отдельные нормативно-правовые акты.

СПИСОК ЛИТЕРАТУРЫ

1. URL: https/мвд.рф/document /19639152 (дата обращения: 27.09.2020).
2. Земцова С.И., Суров О.А., Галушин П.В. Методика расследования незаконного сбыта наркотических средств, совершенного с использованием интернет-технологий. – М., Юрлитинформ, 2019. – 37 с.
3. Обзор о результатах оперативно-служебной деятельности по линии противодействия незаконному обороту наркотиков в первом полугодии 2019 года // ГУНК МВД России. – 2019. –16 с.

УДК 510.65; 699.8

ХАРАКТЕРИСТИКА СРЕДЫ ВЗАИМОДЕЙСТВИЯ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ МЧС РОССИИ

Синещук Максим Юрьевич
Санкт-Петербургский университет государственной противопожарной службы МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mail: sinegal53@mail.ru

Аннотация. Рассматривается необходимость совершенствования процессов управления в системе МЧС Росси. Обосновывается информационный характер процессов управления. Анализируются особенности построения и функционирования автоматизированной информационно-управляющей системы МЧС. Предлагаются варианты безопасного взаимодействия элементов распределенной информационной системы.

Ключевые слова: управление; автоматизированная система управления; распределенная вычислительная сеть.

CHARACTERISTICS OF THE INTERACTION ENVIRONMENT OF DISTRIBUTED INFORMATION SYSTEMS OF THE EMERCOM OF RUSSIA

Sineshchuk Maxim
Saint-Petersburg University of State Fire Service of EMERCOM of Russia
149 Moskovskiy Av., St. Petersburg, 196105, Russia
e-mail: sinegal53@mail.ru

Abstract. The article considers the need to improve management processes in the EMERCOM system of Russia. The informational nature of management processes is justified. The article analyzes the features of building and functioning of the automated information and control system of the Ministry of emergency situations. Options for secure interaction of elements of a distributed information system are offered.

Keywords: control, automated control system, distributed computing network.

Крупные аварии и катастрофы последних десятилетий определяют необходимость совершенствования систем управления в интересах повышения безопасности населения, экономических и социальных объектов, природных ресурсов. Неизбежность и расширение форм проявления чрезвычайных ситуаций обуславливает значительное повышение требований к управлению силами и средствами МЧС. Необходимость удовлетворения этих требований предполагает широкую информатизацию объектов жизнедеятельности МЧС, высокий уровень автоматизации наиболее трудоемких процессов управления [1].

Учитывая информационный характер процессов управления силами и средствами МЧС можно говорить о новом классе систем управления – автоматизированных информационно-управляющих системах (АИУС).

Наличие в арсенале средств АИУС серверов аудио и видео конференцсвязи, FTP серверов, IP телефонных станций и других современных технических средств, предполагает экспоненциальный рост трафика в ведомственной сети МЧС России. Кроме того, использование Интернет-технологий, электронной почты, корпоративных сервисов интрасети, создают новые возможности при управлении силами и средствами МЧС России.

В организационно- техническом плане АИУС состоит из региональных и территориальных информационно-управляющих центров, оснащенных средствами автоматизации и передачи данных. Формирование сети органов и объектов управления различного иерархического уровня МЧС, автоматизация процессов управления привели к возникновению распределенных информационно-вычислительных сетей (РИВС), обеспечивающих реализацию процессов управления и обеспечение поддержки принятия решения в АИУС [2,3].

РИВС являются материальной(технической) основой реализации АИУС. Они представляют собой сложные системы, предназначенные для обработки, хранения и передачи информации. Необходимость обеспечения эффективной работы РИВС подразумевает выбор и реализацию рационального варианта безопасного информационного взаимодействия и обеспечения контроля функциональности использования, предоставляемых ресурсов и сервисов.

В рамках проведенных исследований предложены варианты безопасного подключения подсистем АИУС РСЧС к ВЦССИУ МЧС России, с использованием сертифицированных средств криптографической защиты данных через сеть Интернет или по выделенным каналам связи.

СПИСОК ЛИТЕРАТУРЫ

1. Синещук Ю.И., Терехин С.Н., Иванов А.И., Погорелов А.В. Информационно-расчетное обеспечение принятия решений по применению сил и средств руководителем ликвидации чрезвычайных ситуаций и тушения пожаров. Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2015. № 1. С. 89-94.
2. Синещук Ю.И., Синещук М.Ю., Пантиховский О.В. Информационно-логическая модель анализа и обеспечения устойчивости функционирования систем управления сложными организационно-техническими объектами. СПбУ ГПС МЧС России, Научно-аналитический журнал Проблемы управления рисками в техносфере №2(22), 2012, с.6-12,
3. I. Kotenko, I. Saenko, Yu. Sineshchuk, Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. Proceedings - 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020, Vasteras, Sweden Conference Paper, 10p. March 2020.

УДК 510.65; 699.8

ОБОСНОВАНИЕ СИСТЕМЫ ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕРРИТОРИАЛЬНОГО ОРГАНА МВД

Синещук Юрий Иванович, Логинова Анна Дмитриевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: sinegal53@mail.ru, annaloginova1212@gmail.com

Аннотация. Рассматривается проблема обеспечения информационной безопасности территориального органа МВД. Обосновывается роль и место организационных мероприятий в комплексе мер защиты информации. Формулируется цель создания и предлагается компонентный состав системы организационных мероприятий обеспечения информационной безопасности.

Ключевые слова: компьютерная преступность, информационная безопасность, организационная защита информации.

JUSTIFICATION OF THE SYSTEM ORGANIZATIONAL MEASURES TO ENSURE INFORMATION SECURITY TERRITORIAL BODY OF THE MINISTRY OF INTERNAL AFFAIRS

Sineshchuk Yury, Loginova Anna
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: sinegal53@mail.ru, annaloginova1212@gmail.com

Abstract. The problem of ensuring information security of the territorial body of the Ministry of internal Affairs is considered. The role and place of organizational measures in the complex of information protection measures is justified. The purpose of creation is formulated and the component structure of the system of organizational measures to ensure information security is proposed.

Keywords: computer crime, information security, organizational information protection.

Бурное развитие информационных технологий привело к тому, что информация стала стратегическим ресурсом государства [1]. Органы внутренних дел МВД России являются важной составляющей сил и средств противодействия информационным посягательствам криминальных сообществ на права и свободы граждан, безопасность государства, общества и личности.

Широкое внедрение и применение в ОВД новых информационных технологий приводит к увеличению числа угроз и различных каналов утечки информации, что, в свою очередь, существенно влияет на оперативность

и конфиденциальность их работы, требования к которым за последнее время существенно ужесточились. При этом, преступные группировки стремятся расширить свои возможности по доступу к информационным ресурсам МВД России. В связи с этим особую важность и актуальность приобретают вопросы обеспечения информационной безопасности органов внутренних дел. От того, насколько грамотно и комплексно организована защита информации в органах внутренних дел, зависит качество, эффективность, оперативность и, наконец, безопасность осуществления ими своих функций по защите прав, свобод и интересов граждан от сил и проявлений криминального характера.

Наличие множества угроз обязывает обеспечивать безопасность информации путем создания надежного механизма ее защиты, где, наряду с правовыми и техническими мерами, системообразующую роль играют организационные мероприятия [2].

Организационная защита информации призвана посредством выбора конкретных сил и средств реализовать на практике спланированные руководством меры по защите информации.

Обоснование системы организационных мероприятий обеспечения информационной безопасности территориального органа МВД России предполагает проведение предварительного анализа возможных угроз информационной безопасности [3]. Система организационных мер по защите информации представляют собой комплекс мероприятий, включающих четыре основных компонента: изучение обстановки на объекте, разработку программы защиты, деятельность по проведению указанной программы в жизнь, контроль за ее действенностью и выполнением установленных правил.

Главная цель организационных мероприятий, предпринимаемых на высшем управленческом уровне, – сформировать политику в области обеспечения безопасности информации и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

СПИСОК ЛИТЕРАТУРЫ

1. Синещук Ю.И. Информационная безопасность в системе национальной безопасности. «Региональная информатика и информационная безопасность». Сборник трудов. Выпуск 5 / СПОИСУ.–СПб., 2018.–549с.,с.167-171.
2. I. Kotenko, I. Saenko, Yu. Sineshchuk, Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. Proceedings - 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020, Vasteras, Sweden Conference Paper, 10p. March 2020.
3. Величко, М. Ю. Информационная безопасность в деятельности органов внутренних дел Теоретико-правовой аспект Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 12.00.01 - Теория и история права и государства; История учений о праве и государстве. -Казань, 2013. -26 с.

УДК 510.65; 699.8

АНАЛИЗ ОСОБЕННОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТЕРРИТОРИАЛЬНОГО ОРГАНА МВД РОССИИ, С ОБОСНОВАНИЕМ ТЕХНОЛОГИИ ПРЕДУПРЕЖДЕНИЯ ПОТЕРИ ДАННЫХ

Синещук Юрий Иванович, Михайлова Виктория Владимировна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: sinegal53@mail.ru, vikki.998@mail.ru

Аннотация. Обосновывается роль информации, информационных систем и технологий в обеспечении деятельности территориального органа МВД России. Формулируется задача выбора технологии предупреждения потери данных. Предлагаются результаты сравнительного анализа систем резервного копирования информации, как основы защиты данных.

Ключевые слова: информационная безопасность, потеря данных, резервное копирование.

ANALYSIS OF THE CHARACTERISTICS OF THE INFORMATION SYSTEM OF THE TERRITORIAL AGENCY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA WITH THE SUBSTANTIATION OF THE TECHNOLOGY OF PREVENTION OF DATA LOSS

Sineshchuk Yury, Mikhailova Victoria
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: sinegal53@mail.ru, vikki.998@mail.ru

Abstract. The article substantiates the role of information, information systems and technologies in ensuring the activities of the territorial body of the Ministry of internal Affairs of Russia. The actual problem of choosing a technology for preventing data loss is formulated. The results of a comparative analysis of information backup systems as the basis for data protection are offered.

Keywords: information security, data loss, backup copying.

Проведенная реформа МВД РФ ознаменовала новый этап внедрения информационных технологий в повседневную деятельность органов внутренних дел. Федеральный закон "О полиции" обязывает сотрудников органов внутренних дел использовать в своей работе достижения науки и техники, информационные системы, средства связи, а также современную информационно-телекоммуникационную инфраструктуру [1].

Мировой опыт свидетельствует о том, что самые совершенные технические средства, достижения в области криптографии и программных средств защиты информации не гарантируют абсолютной ее безопасности. Особую опасность представляет расширение и обострение информационного противостояния правоохранительных органов и преступного мира, располагающего не только современными техническими средствами, но и высококвалифицированными специалистами для организации и ведения собственной разведывательной и контрразведывательной работы.

Информация - ключевой элемент в работе территориального органа МВД. В связи с чем особую важность приобретает проблема исследования особенностей защиты информации в информационных системах органов внутренних дел.

При использовании системы ее функциональность, целостность данных не должны нарушаться. Повреждение или утрата информации в результате влияния различных факторов, случайных или намеренных действий, по сути, является потерей данных (Data Loss). Целостность информации обеспечиваются специализированными компонентами системы, использующими технологии предупреждения потери данных. К современным системам управления хранением данных предъявляются высокие требования. В частности, такие системы должны обеспечивать заданный уровень надежности, производительности и автоматизации процессов копирования, а также достаточную гибкость при настройке параметров, разработке стратегий и алгоритмов сохранения для выполнения конкретных задач [2].

Независимо от источника угрозы основной защитой данных является резервное копирование файлов. Задача резервного копирования состоит в защите данных и системы от ряда катастрофических сценариев. В число подобных рисков входят ошибки программного обеспечения, атаки злоумышленников, вирусы, аппаратные отказы или множество других потенциальных проблем [3].

В традиционных системах резервное копирование приводит к перегрузке локальной сети, файловых серверов и серверов приложений, существенно снижает продуктивность работы пользователей и не обеспечивает достаточной производительности для обработки постоянно растущих объемов данных. Решением проблемы может являться внесерверное резервирование. Использование сетей хранения данных выводит решение задачи резервирования и восстановления данных на новый уровень, появляется возможность осуществлять резервное копирование в несколько раз быстрее, чем раньше, без загрузки локальной сети и серверов, обеспечивая круглосуточную функциональность территориального органа МВД.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон "О полиции" от 07.02.2011 N 3-ФЗ (ред. от 06.02.2020)
2. I. Kotenko, I. Saenko, Yu. Sineshchuk. Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. Proceedings - PDP 2020, Vasteras, Sweden Conference Paper, 10p. March 2020.
3. Синещук Ю.И., Яковлев О.В., Терехин С.Н. Информационный риск в условиях электромагнитного терроризма. Электронный научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России». – № 3. – 2012. с.15-18 –vestnik.igps.ru

УДК 510.65; 699.8

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССОВ УПРАВЛЕНИЯ В СИСТЕМЕ МВД РОССИИ НА ОСНОВЕ КОНЦЕПЦИИ СИТУАЦИОННЫХ ЦЕНТРОВ

Синещук Юрий Иванович, Попова Наталья Сергеевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: sinegal53@mail.ru, natulya98@yandex.ru

Аннотация. Рассматривается необходимость совершенствования процессов управления в системе МВД России за счет использования концепции ситуационных центров. Показаны определяющие факторы, которые влияют на активное использование ситуационных центров в деятельности такого органа управления, как Министерство внутренних дел. Рассмотрены основные структурно-функциональные компоненты ситуационного центра, а также направления повышения эффективности деятельности ситуационных центров.

Ключевые слова: управление, ситуационный центр, мониторинг, ситуационное управление, методы и средства принятия решений.

IMPROVEMENT OF MANAGEMENT PROCESSES IN THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA BASED ON THE CONCEPT OF SITUATION CENTERS

Sineshchuk Yury, Popova Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: sinegal53@mail.ru, natulya98@yandex.ru

Abstract. The need to improve management processes in the system of the Ministry of Internal Affairs of Russia through the use of the concept of situation centers is being considered. The determining factors that influence the active use of situation centers in the activities of such a management body as the Ministry of the Interior are shown. The main structural and functional components of the situation center, as well as directions of increasing the efficiency of the situation centers are considered.

Keywords: management, situation center, monitoring, situation management, methods and means of decision-making.

На сегодняшний момент структурные подразделения МВД России ставят перед собой задачу перехода на более высокий уровень развития и организации методов управления, что достигается путём улучшения технического обеспечения, внедрения инновационных технологий. Современные условия требуют от территориальных органов МВД России построения эффективной системы оперативного принятия управленческих решений с возможность их контроля и последующего анализа результатов реализации. Значимость надежной работы такой системы возрастает при возникновении кризисных ситуаций. При этом, управление, в первую очередь, рассматривается как искусство руководителя правильно оценить ситуацию и выбрать наиболее эффективные методы воздействия на окружающую среду, наилучшим образом отвечающие возникшей ситуации [1].

С учетом эволюции развития методологии ситуационного управления, управленческую ситуацию можно определить, как субъективную оценку конкретных характеристик организации и внешней среды (ситуационных переменных) и связей между ними, имеющих место в настоящее время, но зависящих от произошедших событий и развивающихся во времени и пространстве.

Ситуационное управление должно строиться на следующих положениях:

1. Различные по своей сути проблемные ситуации требуют различающихся подходов к их разрешению.
2. Вероятностные факторы в каждой ситуации должны учитываться в стратегиях, структурах и процессах, влияя при этом на эффективность принятия решения.
3. Любая ситуационная проблема должна быть рассмотрена только во взаимосвязи с другими проблемами.

Материальную основу ситуационного управления составляют ситуационные центры. Ситуационный центр можно определить, как организационно-технический комплекс, предназначенный для информационно-аналитического и коммуникационного обеспечения решения задач управления при развитии кризисных ситуаций в органах государственной власти, на крупных предприятиях, в отраслях экономики.

В настоящее время ситуационные центры, создаваемые в органах государственной власти, являются одним из наиболее бурно развивающихся направлений повышения качества управления сложными системами. Актуальность создания ситуационных центров в МВД России вытекает из темпов развития информационной инфраструктуры, как фактора, определяющего необходимость обработки больших объемов информации при жестких временных ограничениях.

Определяющими факторами, которые влияют на активное использование ситуационных центров в деятельности органов управления, в частности в деятельности Министерства внутренних дел, являются [2]:

– необходимость улучшения методов управления путем привлечения специалистов и обеспечения их эффективного взаимодействия с руководителями и сотрудниками на всех этапах процесса принятия решения;

– необходимость снабжения лиц, разрабатывающих и принимающих решения, оперативной, полной и достоверной информацией о проблеме;

– необходимость повышения качества предварительного анализа информации с помощью современных информационных технологий, обеспечивающих моделирование и визуализацию сведений о ситуации для наглядного представления решаемой проблемы;

Ситуационные центры, оснащенные новейшими программно-техническими средствами, с учётом особенностей решаемых задач в конкретной предметной области деятельности МВД России, должны обеспечить отображение наблюдаемого объекта в исходном, текущем и перспективном состояниях, что позволяет прогнозировать развитие различных ситуаций в режиме реального времени и принимать эффективные решения.

Работа ситуационных центров связана с большим объемом обрабатываемых данных, на основе которых в минимальные сроки должно быть принято решение. Для работы на большом масштабе данных становится целесообразным сочетать машинные методы обработки и методы(модели) структуризации массивов цифровой информации, использовать алгоритмы на основе экспертных правил для того, чтобы явным образом выявить интересующее событие. Цифровая идентификация событий позволяет принимать более обоснованные(точные) решения, автоматизируя этот процесс. Учитывая возрастающие требования к качеству и оперативности решений, принимаемых в условиях все возрастающего количества неполной и нечеткой информации, актуальным становится вопрос применения технологий искусственного интеллекта, обеспечивающих эволюцию функциональных задач ситуационных центров от чисто информационных и расчетных, к задачам оперативного мониторинга обстановки, моделирования и прогнозирования ситуаций.

Технология поддержки принятия решений способна вывести информационную поддержку ситуационного центра на более эффективный уровень реагирования на критические ситуации и их предотвращение. Такая технология должна опираться на методы прогнозирования и мониторинга, как на часть математического обеспечении работы системы [3].

Предназначение системы мониторинга состоит в постепенном снижении до минимального уровня риска воздействие на наблюдаемый объект факторов антропогенного, техногенного и природного характера и минимизация вреда от кризисных ситуаций для общества и окружающей среды. Под кризисной ситуацией следует понимать ситуацию, которая характеризуется резкой сменой состояния параметров определенной группы внешних и внутренних процессов, действующих на наблюдаемый объект, и может повлиять на снижение защищенности этого объекта. Объектом мониторинга является состояние защищенности наблюдаемого объекта. Основной задачей системы мониторинга является информационная поддержка разработки и реализации мер по своевременному прогнозированию, выявлению и предупреждению угроз и кризисных ситуаций в отношении наблюдаемого объекта.

Все вышеперечисленные направления развития предполагают создание иерархической сети ситуационных центров МВД России, применение технологии информационных порталов, необходимых для более тесного системного взаимодействия, координации работы органов управления различного иерархического уровня.

Для более эффективной работы ситуационных центров различной ведомственной принадлежности необходимо формирование единого информационного пространства взаимодействия. Решение этой задачи предполагает необходимость совершенствования нормативно-правового обеспечения взаимодействия пользователей системы, повышения уровня квалификации соответствующих специалистов, обеспечения безопасности единого информационного пространства от различного вида угроз [4].

Вызовы, с которыми столкнулась цивилизация в последнее время, убедительно подчеркивают роль и значение ИС и ИТ, в обеспечении всех сфер жизнедеятельности общества, МВД, государства в целом. При этом, закономерно, обостряется проблема обеспечения устойчивости, безопасности компьютерных сетей, как материальной основы функционирования ИС и ИТ. Тесная интеграция таких, как ситуационный центр - по сути киберфизических, систем в различные технологические процессы делает их более уязвимыми к кибератакам[5]. Поэтому проблема обеспечения информационной безопасности ситуационных центров требует самостоятельного рассмотрения и комплексного решения.

СПИСОК ЛИТЕРАТУРЫ

1. Синещук Ю.И., Терехин С.Н., Иванов А.И., Погорелов А.В. Информационно-расчетное обеспечение принятия решений по применению сил и средств руководителем ликвидации чрезвычайных ситуаций и тушения пожаров. Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2015. № 1. С. 89-94.
2. Филиппович А.Ю. Ситуационные центры: определения, структура и классификация / – М.: Компьютерная неделя, 2008. – 167 с.
3. Denis Y. Minkin, Yuri I. Sineshchuk, Sergey N. Terekhin, and Konstantin S. Yusherov. 2017. A method of constructing a structured database of the typical objects of protection on the basis of cluster analysis. Journal of Theoretical and Applied Information Technology, 95(20), 5331–5339.
4. Синещук Ю.И., Суслин А.В., Примакин А.И., Бобонец С.А. Особенности и задачи подготовки специалистов МВД в области информационных систем и технологий. «Вестник Санкт-Петер-бургского университета МВД». – № 2. – 2016. с. 130-136
5. I. Kotenko, I. Saenko, Yu. Sineshchuk, Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. Proceedings - 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020, Vasteras, Sweden Conference Paper, 10p. March 2020.

УДК 004.4

ПОДХОД К ОПРЕДЕЛЕНИЮ МЕТОДА ГАРАНТИРОВАННОГО УНИЧТОЖЕНИЯ ИНФОРМАЦИИ В МВД РОССИИ НА ОСНОВЕ РАЗРАБОТКИ ПАКЕТА АДАПТИВНЫХ ПРИКЛАДНЫХ ПРОГРАММ

Трофимов Даниил Вадимович, Чудаков Олег Евгеньевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: lifeisonn@mail.ru, oechuda@yandex.ru

Аннотация. Обеспечение безопасности информации в органах внутренних дел (ОВД) Министерства внутренних дел (МВД) России представляет многогранную задачу, решаемую с использованием различных средств. Важным элементом системы обеспечения информационной безопасности является необходимость гарантированного уничтожения информации. Рассматривается подход к выбору варианта уничтожения информации путем создания пакета прикладных программ (ППП), обеспечивающего адаптивный подход к обоснованию варианта уничтожения информации в зависимости от уровня ее конфиденциальности и технологии хранения и защиты информации.

Ключевые слова: безопасность; информация; уничтожение информации: конфиденциальность информации.

APPROACH TO DEFINITION OF THE METHOD OF THE GUARANTEED DESTRUCTION OF INFORMATION IN THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION ON THE BASIS OF DEVELOPMENT OF THE PACKAGE OF ADAPTIVE APPLICATION PROGRAMS

Timofeev Daniil, Chudakov Oleg
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: lifeisonn@mail.ru, oechuda@yandex.ru

Abstract. Ensuring the security of information in the internal affairs departments (IAD) of the Ministry of the Interior (MIA) of Russia is a multifaceted task that can be solved using various means. An important element of the information security system is the need for guaranteed destruction of information. The approach to the choice of information destruction option by creating an application software package (ASP) is considered that provides an adaptive approach to justifying the option of information destruction depending on the level of its confidentiality and information storage and protection technology.

Keywords: safety; information; destruction of information; confidentiality of information.

В настоящее время информация является одним из наиболее значимых ресурсов [1]. Владея определенными ее видами, можно перевернуть множество ситуаций себе на пользу. Следовательно,

информационная безопасность в современных информационных системах является одним из важнейших факторов эффективности их функционирования.

Одной из основных задач информационной безопасности информационной системы является предотвращение ее утечек по различным каналам на всех этапах ее обработки, когда эта информация является актуальной [2, 3]. Но даже после того, как содержание информации становится неактуальным, возникает задача обеспечения гарантированного уничтожения информации на носителе.

Анализ показывает, что существует широкий спектр средств и методов хранения информации, которые могут использоваться в ОВД МВД, что создает определенные трудности с решением задачи гарантированного уничтожения информации в различных организациях.

Проблема гарантированного уничтожения информации состоит также и в том, что в настоящее время существует большое разнообразие носителей информации, имеющие определенные особенности в технологии хранения, а, следовательно, они должны быть учтены при решении задачи уничтожения данной информации.

В современных условиях при наличии большого разнообразия различных средств хранения информации многоразового использования наибольшую актуальность приобретают методы, обеспечивающие гарантированное уничтожение информации без разрушения носителя, что обеспечивает возможность дальнейшего использования данного носителя для хранения информации. Особенно это важно для носителей, где может храниться конфиденциальная информация ограниченного доступа, включая информацию, содержащую сведения, составляющие государственную тайну.

В связи с указанным, актуальность проблемы заключается в том числе и в том, что многие пользователи не могут четко определить, да, как правило и не знают существующие методы и способы уничтожения информации, в результате чего появляется канал утечки информации за счет применения неадекватного метода уничтожения информации. Это связано с тем, что в настоящее время распространенным способом утечки практически любой информации является ее восстановление с носителей. На данный момент существует множество программных и иных способов восстановления информации, что создает такую проблему, как предотвращение утечки данных после их удаления [4].

Для решения данной проблемы существует множество способов, которые объединяет такое понятие, как гарантированное удаление информации [5].

Под гарантированным удалением информации принято понимать способ уничтожения информации для ее защиты от утечек, которые могут возникнуть в связи с неправильной утилизацией запоминающих устройств и их дальнейшим использованием злоумышленником. Может происходить как с уничтожением носителя, так и без уничтожения.

Исходя их данного определения можно заметить, что оно подразумевает в себе два способа:

- с уничтожением носителя;
- без уничтожения носителя.
- Рассмотрим их более подробно. Гарантированное удаление информации с уничтожением носителя включает в себя:
- путем механического уничтожения носителя, т.е. его физическое измельчение;
- путем термического уничтожения носителя, т.е. его нагревание до температуры разрушения основы;
- путем пиротехнического уничтожения носителя, т.е. его взрыва;
- путем химического уничтожения носителя, т.е. его разрушения химически активными веществами.

Исходя из вышесказанного можно заметить, что все эти способы приводят к полной не пригодности носителя, что и приводят к полному отсутствию возможности восстановления с них каких-либо данных.

Второй способ подразумевает следующие манипуляции с носителем:

- путем размагничивания носителя, т.е. помещения его в медленно убывающее магнитное поле, для приведения в нейтральное состояние;
- путем намагничивания носителя, т.е. помещения его в сильное магнитное поле с той же целью;
- путем шифрования носителя;
- при помощи прикладных программных средств.

Данные способы удаляют информацию гарантированно, но не всегда есть возможность определить какой из них, или совокупность каких способов и в какой последовательности целесообразно применить для обеспечения гарантированного уничтожения информации, обеспечивающего невозможность ее восстановления.

В связи с этим, предлагается разработка пакета прикладных программ, позволяющих на основании анализа содержание информации, степени конфиденциальности, носителя, методов хранения информации выработать предложения по вариантам применения методов уничтожения информации, обеспечивающих ее гарантированное уничтожение.

В основу разработки данного пакета положены следующие основные принципы: целесообразность уничтожения; невозможность восстановления; соотношение затрачиваемых средств на уничтожение информации к ценности информации.

С целью обоснования необходимого пакета прикладных программ для гарантированного уничтожения информации целесообразно построить модель процесса гарантированного уничтожения информации, которая должна включать в себя процессы анализа информации, предназначенной для уничтожения, проверка соответствия этой информации сопровождающим документам, формирование набора методов, которые

обеспечивают гарантированное уничтожение данной информации, а также последовательность их применения. При построении данной модели должны быть учтены требования руководящих документов по организации уничтожения конфиденциальной информации, включая информацию, составляющую государственную тайну.

На основании функциональной модели далее предлагается разработать подсистему поддержки принятия решений, обеспечивающую на основе анализа поступившей на уничтожение информации выбрать оптимальное решение по формированию мероприятий, обеспечивающих гарантированное уничтожение информации.

Применение предлагаемого подхода позволит принимать обоснованные решения по гарантированному уничтожению информации различного назначения на различных носителях различного уровня конфиденциальности.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006, № 149 –ФЗ.
2. ГОСТ Р 50922-2006 Национальный стандарт РФ «Защита информации. Основные термины и определения».
3. ГОСТ Р 51275-99. Защита информации. Объект информатизации.
4. Галатенко В.А. Основы информационной безопасности: учебное пособие – 4-е изд. – М.: Бином, 2008. 206 с.
5. ГОСТ 28388-89. Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения.

УДК 681.518 (004.031.42)

ПОДХОД К РАЗРАБОТКЕ ЭЛЕМЕНТОВ ОБУЧАЮЩЕЙ ПОДСИСТЕМЫ, ОБЕСПЕЧИВАЮЩЕЙ САМОСТОЯТЕЛЬНУЮ РАБОТУ КУРСАНТОВ ВУЗА

Харитонова Кристина Михайловна, Потехин Владимир Семенович
Санкт-Петербургский университет МВД России
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mails: kristina.kharitonova.1999@mail.ru, vsp1945@gmail.com

Аннотация: Излагается подход к созданию средств информационной поддержки, обеспечивающих процесс самостоятельной работы обучающегося. Подход предполагает создание автоматизированных рабочих месте обучающихся (АРМ-О). При этом учитываются современные требования, изложенные в федеральных государственных стандартах высшего образования (ФГОС ВО).

Ключевые слова: самостоятельная подготовка; средства информационной поддержки процесса; «единое окно» доступа; обучающая подсистема; автоматизированное рабочее место.

APPROACH TO THE DEVELOPMENT OF ELEMENTS OF A TRAINING SUBSYSTEM ENSURING INDEPENDENT WORK OF UNIVERSITY TRAINEES

Kharitonova Kristina, Potekhin Vladimir
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov str., St. Petersburg, 198206, Russia
emails: kristina.kharitonova.1999@mail.ru, vsp1945@gmail.com

Abstract: An approach to the creation of information support tools to ensure the process of self-study work is described. The approach involves creating automated workstations for trainees (AW-T). At the same time, modern requirements set forth in the federal state standards of higher education (FSES HE) are taken into account.

Keywords: independent training; learning support tools; «single window» for access; training subsystem; workstation.

Следуя источникам [1, 2], под обучающей системой будем понимать совокупность технических и программных средств, а также методических средств и приемов для автоматизации процессов обучения в целях повышения его эффективности. Требования, предъявляемые к обучающим системам, в целом, и подсистемам, обеспечивающим самостоятельную работу обучающихся в ВУЗе, постоянно ужесточаются и уточняются. Так, последним поколением ФГОС ВО, по специальности 10.05.05 [3, п. 7.3.3] и по направлению подготовки 09.03.02 [4, п. 7.3.3] предусматривается использование всей совокупности ресурсов материально-технического и учебно-методического обеспечения дисциплин (УМОД), в том числе средств, обеспечивающих самостоятельную работу. Эти УМОД включают не только традиционные учебно-методические материалы (УММ) в «бумажном» исполнении, но и электронные материалы, размещенные в электронной информационно-образовательной среде (ЭОИС) организации (в виде: внешних электронных библиотечных систем, например [3]; профессиональных баз данных, например [6]; информационно-справочных систем, например [7], и др.).

Однако использование обучающимися упомянутых ресурсов и средств связано с рядом сложностей:

– УММ, размещенные в Интернете, по понятным причинам, не учитывают требований локальных нормативных актов конкретного образовательного учреждения;

– средства информационной поддержки, обеспечивающие работу с УММ в Интернете и применяемые в конкретной учебной организации, что затрудняет их совместное использование.

Устранить упомянутые сложности можно, если на основе современных информационных технологий, обеспечить возможность комплексного использования всех возможностей УМОД с автоматизированного рабочего места обучающегося (АРМ-О), оснащенного средствами информационной поддержки самостоятельной

работы по всем видам дисциплинарной подготовки. Но для этого следует выполнить дополнительные исследования, предусматривающие:

– анализ руководящих документов, регламентирующих процесс самостоятельной работы обучающихся [8]. В ходе анализа будут установлены цели, задачи, принципы, подходы и терминология, которые предполагается использовать при разработке элементов обучающей подсистемы рассматриваемого назначения на последующих этапах исследования;

– анализ имеющихся достижений в исследуемой области и выявление тех средств, которые могут оказаться полезными при организации самостоятельной работы обучающихся [9-14]. Предполагается, что наряду с функциональными средствами, традиционно используемыми в процессах автоматизированного обучения, существенное внимание будет уделено анализу средств, обеспечивающих защиту данных в условиях использования как внутри учебного учреждения, так и при удаленном доступе, что характерно, в частности, для самостоятельной работы обучающихся при подготовке к семинарам, практическим занятиям, курсовым работам, написании рефератов и пр. Кроме того предполагается что будут выявлены элементы обучающей подсистемы, которые не в полной мере отвечают современным представлениям об организации самостоятельной работы и которые потребуют углубленной проработки;

– построение на основе работ [15-19] функциональных и поведенческих моделей, выявленных элементов обучающей подсистемы, которые требуют углубленной проработки. При этом будет осуществлен учет специфики комплексного использования всех учебно-методических материалов (УММ), предусмотренных к использованию учебной программой изучаемой дисциплины, обеспечивая доступ (по желанию обучающегося) и к копиям «бумажных» УММ, и к УММ, хранящиеся в электронной информационно-образовательной среде университета (на серверах: информационно-образовательного центра, выпускающих кафедр, кабинета педагогического мастерства и учебных классов), и к УММ, хранящимся в электронных библиотеках Интернет (электронная библиотечная система «КнигаФонд», президентская библиотека им. Б.Н. Ельцына, библиотека портала edu/garat.ru), а также к профессиональным базам данных (Государственный реестр сертифицированных средств защиты информации, интернет-портал правовой информации Федеральной службы по техническому и экспортному контролю России, интернет-портал нормативно-технической документации ФКУ НИЦ «Охрана») и информационно-справочным системам (Гарант-образование и др.);

– разработку диалога «ЭВМ-обучаемый», обеспечивающего обращение к необходимым УММ по принципу «единого окна» с использованием средств, как локального, так и дистанционного доступа с учетом опыта, опубликованного в работах [9, 12, 13, 18].

Реализация перечисленных направлений исследований, не претендуя на полноту, позволяет, по мнению авторов, составить общее впечатление о возможном подходе к созданию средств информационной поддержки, обеспечивающих процесс самостоятельной работы на автоматизированном рабочем месте обучаемого (АРМ-О) с учетом изменяющихся требований к организации их проведения.

СПИСОК ЛИТЕРАТУРЫ

1. Обучающая система// Энциклопедический словарь [Электронный ресурс] URL: https://1564.slovaronline.com/6844-%D0%BE%D0%B1%D1%83%D1%87%D0%B0%D1%8E%D1%89%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0
2. Автоматизированная обучающая система // Педагогический терминологический словарь [Электронный ресурс]. URL: https://pedagogical_dictionary.academic.ru/23/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BE%D0%B1%D1%83%D1%87%D0%B0%D1%8E%D1%89%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%28%D0%90%D0%9E%D0%A1%29
3. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитета). Утвержден Приказом Минобрнауки России от 19.12.2016 N 1612. // Сайт «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_210993/ (дата обращения 15.07.2020).
4. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии (уровень бакалавриата). Утвержден Приказом Минобрнауки России от 12.03.2015 N 219 // Сайт «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_177552/ (дата обращения 15.07.2020).
5. Доступ к электронно-библиотечной системе «Книгафонд» //Сайт «КнигаФонд» [Электронный ресурс]. URL: https://library.mirea.ru/%D0%9E%D0%B1%D1%8A%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F/78 (дата обращения 15.07.2020).
6. Нормативно-техническая документация ФКУ НИЦ «Охрана» Росгвардии // [Электронный ресурс]. URL: http://nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html (дата обращения 15.07.2020).
7. «ГАРАНТ-Образование» — специальный выпуск системы ГАРАНТ, ориентированный на студентов, аспирантов и преподавателей // Сайт ООО «НПП «ГАРАНТ-СЕРВИС» [Электронный ресурс]. URL: http://technomag.bmstu.ru/doc/52838.html (дата обращения 15.-7.2020).
8. Положение об учебно-методическом обеспечении образовательных программ. Утверждено приказом начальника Санкт-Петербургского университета МВД России № 68 от 12.02.2016 г. / СПб: Изд-во Санкт-Петербургского университета МВД России. 2016 . 24 с.
9. Чудаков О.Е., Куватов В.И., Потехин В.С., Саратов Д.Н. Опыт разработки электронного хранилища документов учебно-методического обеспечения образовательных программ на основе компьютерных технологий // Вестник СПб университета МВД № 2 (74), 2017. С. 184 – 190.
10. Иванников А.Д., Иванов Ю.Л., Кулагин В.П. Перспективы использования WWW-технологии в высшей школе России // Информационные технологии, 1996. № 2. С. 24-29.
11. Кривошеев А. О., Голомидов Г. С., Таран А. Н. Перспективные Internet-технологии информационного обеспечения образовательных услуг / Сайт «МГТУ им. Н.Г. Баумана». URL: http://technomag.bmstu.ru/doc/52838.html (дата обращения 19.07.2020).
12. Потехин В.С. Опыт разработки методических рекомендаций на основе компьютерных технологий для слушателей-заочников, готовящих дипломы по техническим специальностям // Вестник СПб университета МВД № 4, (60), 2013. С. 149 – 155.

13. Кадулин В.Е., Потехин В.С. Об уточнении понятия и классификации автоматизированных рабочих мест, используемых в информационных системах и компьютерных технологиях // Вестник СПб университета МВД № 4 (68), 2015. С. 207 – 210.
14. Весманов С.В., Каспржак А.А., Рачевский Е.Л., Терехов А.А. Концептуальная модель организации интернет-поддержки информационно-образовательного пространства в общем образовании. // В сборнике научных статей «Интернет-порталы: содержание и технологии». Выпуск 1. / Редкол.: А.Н. Тихонов (пред.) и др.; ГНИИ ИТТ «Информика». - М.: Просвещение, 2003. - С. 235-276.
15. Горбаченко В. И., Убиенных Г. Ф., Бобрышева Г. В. Создание функциональной модели информационной системы с помощью CASE-средства CA ERwin Process Modeler 7.3 // Пенза: ПГУ, 2010. 66 с. [Электронный ресурс]. http://window.edu.ru/resource/658/72658/files/stup552.pdf (дата обращения 13.09.2017).
16. Дубейсковский В.И. Практика функционального моделирования с AllFusion Process Modeer 4.1. Где? Зачем? Как? // М.: Изд. Диалог-МИФИ, 2008 –464 с. ISBN 5-86404 192-0.
17. Маклаков С.В. Моделирование бизнес-процессов с AllFusion PM. 2-е изд., испр. и дополн. // М.: Изд. Диалог-МИФИ, 2008. 224 с. ISBN 5-86404-179-3.
18. Лягинова О.Ю. Разработка схем и диаграмм в Microsoft Visio. 2010: учебное пособие //М.: Изд-во: ИНТУИТ, 2014 — 191 с.
19. ГОСТ 19.701-90 (ИСО 5807-85). Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения // М.: «Издательство стандартов», 1991.

УДК 004.021

АВТОМАТИЗАЦИЯ ЗАДАЧ СВЯЗАННЫХ С АНАЛИЗОМ ОПЕРАТИВНОЙ ИНФОРМАЦИИ

Чудаков Олег Евгеньевич, Мясников Илья Олегович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: OEchuda@yandex.ru, unkownsmail@gmail.com

Аннотация. Рассматривается способ автоматизации задач, решаемых сотрудниками оперативных подразделений.

Ключевые слова: автоматизация; анализ; оперативная информация; теория графов; алгоритм.

AUTOMATION OF TASKS RELATED TO INTELLIGENCE ANALYSIS

Chudakov Oleg, Myasnikov Ilya
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
Letchika Pilyutova, st., 1, St. Petersburg, 198206, Russia
e-mail: OEchuda@yandex.ru, unkownsmail@gmail.com

Annotation. The way of automating tasks undertaken by employees of operational units.

Key words: automation; analysis; operative information; graph theory; algorithm.

На сегодняшний день, вместе с развитием информационных технологий, все больше людей регистрируются в социальных сетях. Социальные сети позволяют общаться, создавать сообщества по интересам и участвовать в них, тем самым заменяя живое общение. У молодых людей активность в социальных сетях зачастую сравнима с активностью в реальной жизни. Принимая во внимание факт того, что общение через социальные сети становится все популярнее, нельзя не согласиться с тем, что информация, передаваемая таким путем, и информация о зарегистрированных в них лицах может представлять оперативный интерес.

Как и остальные продукты информационного прогресса, социальные сети хранят и обрабатывают данные, отправляемые своими пользователями. Однако объем этих данных достаточно велик для того чтобы анализировать их вручную. Таким образом, вопрос об информационно – аналитическом обеспечении оперативных подразделений правоохранительных органов приобретает актуальность.

Рассмотрим одну из самых востребованных аналитических задач в оперативной деятельности, которую позволяет решить автоматизированный алгоритм: поиск наименьшей цепочки субъектов, соединяющих двух лиц. Решение данной задачи обуславливается тем, что длина цепочки знакомств между двумя субъектами позволяет оценить, насколько вероятна связь между ними, что является значимым фактором для оперативной обстановки [1].

Как правило, в социальных сетях у каждого пользователя имеется блок «друзья», однако одной этой информации недостаточно для решения представленной задачи. Объем списка друзей может достигать нескольких сотен учетных записей пользователей, потому составление списка «друзья друзей» без использования технических средств не всегда может быть произведено в приемлемых пределах времени.

Данная задача может быть формализована и решена с помощью технических средств. Социальная сеть может быть представлена как граф. Пользователей обозначим точками, а связи между пользователями (наличие в списке «друзья») - линиями, соединяющими соответствующие точки. Для решения задачи будет использоваться алгоритм поиска в ширину.

Данный алгоритм выполняет те же действия, что и человек, который захотел бы найти цепочку людей вручную. Идея этого алгоритма заключается в последовательном посещении вершин графа по уровням: сначала непосредственно связанные с начальной вершиной, затем связанные с начальной вершиной через одну промежуточную и т.д. Уже посещенные вершины запоминаются и повторно не посещаются. В итоге будут посещены все вершины, связанные с начальной вершиной, причем один раз [2].

Затраты времени на выполнение алгоритма поиска в ширину пропорциональны сумме количеству вершин и ребер графа. Еще одним достоинством алгоритма поиска в ширину является его способность работать с

потенциально бесконечными графами: если в бесконечном графе содержится цепочка знакомств между людьми, она будет найдена.

В заключение можно отметить и другую задачу, которая может быть решена с помощью теории графов: поиск сообществ, то есть групп пользователей, все члены которых связаны друг с другом (непосредственно или через других членов группы).

Таким образом, современная вычислительная техника в сочетании с алгоритмическим и программным обеспечением, позволяют автоматизировать решение задач, актуальных для оперативно-розыскных подразделений правоохранительных органов, которые являются слишком трудными для решения вручную.

СПИСОК ЛИТЕРАТУРЫ:

4. Галушин, П.В. Возможности автоматизации аналитической работы с информацией, размещённой в социальных сетях / П.В. Галушин, С.Н. Ефимов // Современные системы безопасности - Антитеррор : материалы конгрессной части X специализированного форума (28-29 мая 2014 г.) / отв. ред. А.В. Букарин. - Красноярск: СибЮИ ФСКН России, 2014. - ISBN 978-5-7889-0218-0. - С. 169-171.
5. Алгоритмы: построение и анализ = Introduction to Algorithms / Томас Х. Кормен и др. - 2-е изд. - М.: «Вильямс», 2006.

УДК 004.62

ПЕРСПЕКТИВЫ ИНФОРМАТИЗАЦИИ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНИКА

Чудаков Олег Евгеньевич, Мясников Илья Олегович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова, ул., 1, Санкт-Петербург, 198206, Россия
e-mail: OEchuda@yandex.ru, unkownsmail@gmail.com

Аннотация. Рассматривается вопрос о необходимости внедрения информационных технологий в деятельность оперуполномоченного органов внутренних дел, способы усовершенствования эффективности оперативно-розыскной деятельности с использованием современных информационных технологий.

Ключевые слова: информационные технологии; оперуполномоченный; анализ; большой объем данных.

PERSPECTIVES OF INFORMATIZATION OF DETECTIVE'S ACTIVITIES

Chudakov Oleg, Myasnikov Ilya
Saint Petersburg University of the Ministry of Internal Affairs of the Russian Federation
Letchika Pilyutova, st., 1, St. Petersburg, 198206, Russia
e-mail: OEchuda@yandex.ru, unkownsmail@gmail.com

Annotation. The question of the need to introduce information technologies into the activities of the operative of the internal affairs bodies, ways of improving the efficiency of operational search activities using modern information technologies are considered.

Key words: Information Technology; operative; analysis; large amount of data.

Современное общество стремительно вступило в эпоху информационных технологий и органы внутренних дел, являясь неотъемлемой частью общества, обязаны идти в ногу со временем для того чтобы эффективно выполнять свои правоохранительные функции. Учитывая данный аспект развития общества, в основополагающий нормативно-правовой акт, регламентирующий деятельность полиции, в целях повышения эффективности её деятельности, был внесён соответствующий пункт [1].

На сегодняшний день, жизнь человека связана с внушительным количеством достижений информатизации, которые способны хранить информацию и заменять живое общение. В совокупности, получив и проанализировав информацию с устройств лица, можно получить его переписку, записи телефонных переговоров и местоположение в определенный промежуток времени. Такая информация, несомненно, может являться критически важной для осуществления оперативно-розыскных мероприятий.

Если ранее оперуполномоченному приходилось собирать данную информацию по различным каналам и оперативным источникам, то в настоящее время, её большая часть содержится в цифровом виде на технических устройствах.

Однако вышеперечисленные данные хранятся безраздельно, в общем массиве вперемешку с большим объёмом незначащей информацией. Вместе с тем, объем информации, представляющей интерес, равно как и не представляющей, становится ещё больше, когда увеличивается количество лиц, попавших в поле зрения оперуполномоченного.

Таким образом, оперуполномоченный имеет возможность получить достаточно большой объем информации о различных интересующих его лицах, используя достижения в сфере информационных технологий, однако для того чтобы эффективно ею воспользоваться, ему необходимо её проанализировать.

Анализ информации, представляющей оперативный интерес, размер которой может достигать нескольких гигабайт, для одного человека или даже группы лиц, является задачей высокой сложности, решить которую без особых знаний и технических средств, зачастую, невозможно. К тому же, как отмечает руководство МВД России, число сотрудников, обладающих соответствующими навыками и умениями, не соответствует потребностям эффективного управления [2].

Все вышеизложенное позволяет сделать вывод о том, что на сегодняшний день оперуполномоченному необходимо иметь многие навыки, позволяющие анализировать и извлекать интересующую информацию из большого количества источников данных, в том числе в режиме реального времени и анализировать ее в целях предупреждения, пресечения, раскрытия и расследованию преступлений [3].

Подводя итог вышеизложенному, можно сделать следующие выводы:

1. Следует признать факт того, что работа с большими объемами данных в правоохранительной деятельности на сегодняшней день уже является повседневной и требует соответствующего обеспечения программно-техническими средствами и сотрудниками, способными их эффективно использовать.

2. Деятельность оперуполномоченного под влиянием объективных процессов, протекающих в современном обществе, трансформируется в сторону аналитики. Оперативный сотрудник будущего - это аналитик, отвечающий за анализ большого объема информации, выявление взаимосвязей и построение моделей поведения субъектов.

СПИСОК ЛИТЕРАТУРЫ:

1. О полиции: Федеральный закон от 07 февраля 2011 г. № 3-ФЗ ст. 11//Собрание законодательства РФ. -2011г. - №7.
2. URL: http://ormvd.ru/pubs/102/some-questions-of-the-organization-of-analytical-work-in-the-administrative-activities-of-inte/ (дата обращения: 20.09.20).
3. Об оперативно-розыскной деятельности: Федеральный закон от 5 июля 1995 г. №144-ФЗ ст. 2//Собрание законодательства РФ -1995г. - №33

КРУГЛЫЙ СТОЛ «ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ»

УДК 334.7

ИНСТРУМЕНТЫ ФИНАНСИРОВАНИЯ В КОРПОРАТИВНОМ СЕКТОРЕ

Горенбургов Михаил Абрамович[1], Сологубова Галина Сергеевна[2]
[1] Федеральный исследовательский центр Кольский Научный Центр РАН
Ферсмана ул., 14, Апатиты, Мурманская обл., 184209, Россия
[2] Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: gorenburgow@mail.ru, en-consalt@mail.ru

Аннотация. По мере роста внедрения новых технологий банки вынуждены предлагать своим корпоративным клиентам продукты, которые поддерживают полностью автоматизированную обработку, а также экономию средств в сочетании с гарантией платежей и вариантами финансирования.

Ключевые слова: ликвидность; цепочки финансов; цепочки поставок; блокчейн, интегративные платформы.

FINANCIAL INSTRUMENTS IN THE CORPORATE SECTOR

Gorenburgov Mikhail[1], Sologubova Galina[2]
[1] Federal research center Kola Research Center of the Russian Academy of Sciences
14 Fersman St., Apatity, Murmanskaya Oblast, 184209, Russia
[2] Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mails: gorenburgow@mail.ru, en-consalt@mail.ru

Abstract. As the adoption of new technologies increases, banks are forced to offer their corporate client's products that support fully automated processing, as well as cost savings combined with payment guarantees and financing options.

Keywords: liquidity; financial chains; supply chains; blockchain; integrative platforms.

Деньги или ликвидность становятся все более значимыми в жизни людей, в бизнесе. Несколько лет назад компании в основном конкурировали за «продукт» (выручка от продаж), сегодня все больше и больше компаний конкурируют с позиций их цепочки поставок (ЦП).

Значение имеет качество (модель) управления цепочкой поставок и ликвидностью. Аналитики Уолл-Стрит в основном смотрят на [1]:

– оборотный капитал и производительность денежных потоков компаний, потому что это хороший показатель эффективного управления;

– определяемые товарные рынки такие как, продукты питания и напитки, для которых характерен высокий уровень насыщения, и очень трудно получить/сохранить долю рынка;

– объём сделок по публичным слияниям и поглощениям (англ. mergers and acquisitions, M&A), которые опять-таки нуждаются в ликвидности.

Нарушения физической цепочки поставок или риски цепочки поставок в случае сбоев приводят к серьёзным потерям и последствиям для всех участников [2, 3].

Таиланд являлся одним из крупнейших производителей жестких дисков во всем мире с большим количеством стратегических поставщиков для своего производства. С момента наводнения (2011 год) он прервал всю цепочку поставок Western Digital. Одним из тяжелейших последствий COVID- 19 для бизнеса признаётся разрушение транснациональных цепочек поставок.

Новая модель торговли финансированием обусловлена внедрением новых технологий, таких как электронные счета-фактуры на основе веб-решений SS, блокчейн, ИИ, интегративные платформы [4].

«Индустрия модных слов» - несколько лет назад никто не говорил о финансировании цепочки поставок, теперь, каждый год проводится 30 - 40 конференций на тему SCF. Опубликованы исследования, выпущен глоссарий терминов и серия руководящих документов, основанных на стандартных определениях для методов финансирования цепочки поставок, был учреждён Global SCF Forum (2016 г.) [5, 6].

Сохраняется запрос на необходимость обеспечивать получение долгосрочной устойчивой ценности для клиентов с помощью методов SCF.

Google Тренды: с 2004 года спрос на тему SCF увеличился в 4 раза, в Китае за последние два года вырос в 10 раз. Интерес к теме SCF перемещается из Европы и США на развивающиеся рынки, где многие люди заинтересованы этим решением.

Таким образом, финансирование цепочки поставок может быть решением, способным обеспечить ликвидность, которая требуется для стратегий нового типа: деньги – не эквивалент обмена, а ресурс (капитал).

Капитализация предприятий, а не прибыль как финансовый результат, становится целью бизнеса.

Финансирование цепочки поставок и блокчейн.

Системы блокчейнов позволяют значительно увеличить скорость расчетов при более низких затратах, предоставляя единый источник «правдивости» в отношении ключевых точек в цепочке поставок, таких как кредитоспособность, уровни запасов поставщиков, получение и утверждение заказов на покупку, получение и утверждение счетов и многое другое [7].

Проверки идентичности и списки «Не продавать», которые часто требуют нескольких независимых проверок, также являются идеальными целями для неизменяемых общих записей, хорошо подходящих для блокчейна.

Распространение IoT по всей цепочке поставок поможет распознавать и автоматизировать задачи, связанные с отгрузкой, доставкой и контролем качества. Поскольку отслеживание IoT стоимостных потоков для доставки полезно, инвентаризация (управление запасами) становится повсеместной операцией.

Интеллектуальные контракты и другие инструменты для автоматизации и финансовых транзакций на блокчейне стали более надежными.

Появилась возможность финансирования из альтернативных источников, таких как кредитные союзы и частные лица, которые получили возможность программного объединения своих средств и увеличили предложение услуг SCF, последние до настоящего времени были доступны только через банки. Это еще больше сократит накладные и административные расходы и увеличит объёмы финансовых средств в экосистеме SCF, а мелким поставщикам станет проще, чем когда-либо, ускорить денежные потоки и развить свой бизнес.

Имеют значение: эффективность при бронировании и утверждении счетов-фактур; понимание тонкостей глобальной цепочки поставок бизнеса для учета отклонений в операциях с иностранной валютой и потенциальных задержек или ошибок в обработке счетов-фактур в узких местах, которые могут привести к каскаду ошибок в цепочке поставок. Рост затрат на координацию взаимодействия в ЦП рассматривается с 2012 года как ключевая проблема управления [8].

Получение выгодных условий оплаты является важным видом деятельности по оптимизации доходов от финансирования цепочки поставок для покупателей - поскольку поставщики используют кредит покупателя вместо своего собственного, условия, выходящие за рамки традиционного соглашения NET 30 (клиент должен заплатить в течение 30 дней со дня выставления счёта), вполне оправданы, а технология блокчейнов все больше коммодитизирует источники финансирования, включая стороннего плательщика, что становится всё более распространенным и выгодным.

По мере того, как технологии, облегчающие финансирование цепочки поставок, распространяются на всех уровнях и в разных отраслях, предельные доходы становятся все более важными, а финансирование цепочки поставок становится доступным для более мелких и разнообразных поставщиков.

СПИСОК ЛИТЕРАТУРЫ

1. Receivables discounting technique / Global supply chain finance forum // URL: http://supplychainfinanceforum.org (Дата обращения 10.07.2020)
2. Алексеева М.Б. Системная диагностика стратегии развития промышленности Арктики / М.Б.Алексеева, В.Ф.Богачев, М.А.Горенбургов // Записки Горного института. 2019. Т. 238. С. 450-458. DOI 10.31897/PMI.2019.4.450
3. Горенбургов М.А. Классификация инноваций в промышленности как предпосылка для принятия оптимальных управленческих решений в бизнесе / М.А.Горенбургов, В.В.Гончаров // Проблемы современной экономики. 2018. № 3 (67). С. 136-339.
4. Сологубова, Г. С. Составляющие цифровой трансформации: монография / Г. С. Сологубова. — М.: Издательство Юрайт, 2018. — 141 с. — (Серия: Актуальные монографии). — ISBN 978-5-534-09306-3.
5. ICC Global Survey 2018: обеспечение будущего роста /International Chamber of Commerce // URL: https://iccwbo.org/publication/standard-definitions-techniques-supply-chain-finance/(Дата обращения 08.07.2020)
6. Trade Finance Principles /The Wolfsberg Group, ICC and BAFT Trade Finance Principles 2019 amendment// URL: https://library.iccwbo.org/content/tfb/pdf/trade-finance-principles-2019-amendments-wolfsberg-icc-baft-final.pdf (Дата обращения 18.07.2020)
7. Supply Chain Finance and Blockchain: The Future Ahead. 2019 / Sofocle Technologies // URL: https://medium.com/sofocle-technologies/supply-chain-finance-and-blockchain-the-future-ahead-a8c5fc26d59 (Дата обращения 18.07.2020)
8. Сологубова Г.С. Уточнение понятий «экономический кластер» и «кластерная экономика». Проблема смыслов. Стр. 30-38. / Журнал «Научно-технические ведомости СПбГПУ» / экономические науки. 1 (235) 2016. Кластерная экономика и промышленная политика. СПб: Изд-во Политехнического университета, 2016. - 193 с.

УДК 004.891.3

МОДЕЛИРОВАНИЕ СЕТИ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ ИДЕНТИФИКАЦИИ ПОЛУЧАТЕЛЯ ГОСУДАРСТВЕННЫХ УСЛУГ

Потапова Анастасия Викторовна[1], Тибилова Галина Саламовна[2], Овчаренко Андрей Вячеславович[2], Дьяченко Наталья Владимировна[3]

[1] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[2] СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Черняховского ул., 59, Санкт-Петербург, 191040, Россия
[3] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mails: anastasia589@mail.ru, tibilova@iac.spb.ru, ovcharenko@iac.spb.ru, nat230209@yandex.ru

Аннотация. В статье рассматривается понятие проактивности и обосновывается ее значимость в сфере предоставления государственных услуг. В качестве инструмента для реализации проактивности предлагаются сети экспертных систем. Авторами введены основные понятия, используемые при моделировании экспертных систем и их сетей, представлена структура и схема работы сети экспертных систем. Была спроектирована топология сети экспертных систем для определения категории получателя для конкретной жизненной ситуации. Описаны преимущества использования сетей экспертных систем в сравнении с одной многоуровневой экспертной системы. Рассмотрены перспективы развития сетей экспертных систем и возможность их использования для решения различных задач.

Ключевые слова: цифровое взаимодействие; цифровая трансформация; проактивность; государственные услуги; экспертные системы.

MODELING A NETWORK OF EXPERT SYSTEMS TO IDENTIFY A RECIPIENT OF PUBLIC SERVICES

Potapova Anastasiya[1], Tibilova Galina[2], Ovcharenko Andrey[2], Dyachenko Natalia[3]

[1] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[2] St. Petersburg State Unitary Firm «St. Petersburg Information and Analytical Centre»
59 Chernyakhovsky St, St. Petersburg, 191040, Russia
[3] Russian State Hydrometeorological University
79 Voronezhskya St., St. Petersburg, 192007, Russia
e-mails: anastasia589@mail.ru, tibilova@iac.spb.ru, ovcharenko@iac.spb.ru, nat230209@yandex.ru

Abstract. The article discusses the concept of proactivity and substantiates its importance in the provision of public services. Networks of expert systems are proposed as a tool for implementing proactivity. The authors introduced the basic concepts used in modeling expert systems and their networks, presented the structure and scheme of the network of expert systems. The topology of a network of expert systems was designed to determine the category of the recipient for a specific life situation. The advantages of using networks of expert systems in comparison with one multi-level expert system are described. The prospects for the development of networks of expert systems and the possibility of their use for solving various problems are considered.

Keywords: digital interaction; digital transformation; proactivity; public services; expert systems.

В рамках национальной программы «Цифровая экономика Российской Федерации» поставлена задача цифровой трансформации предоставления государственных услуг в 2020-2024 годах, которая должна основываться на следующих принципах:

1) реестровая модель предоставления услуг;
2) проактивность предоставления услуг;
3) экстерриториальность предоставления услуг;
4) многоканальность предоставления услуг;
5) исключение участия человека в процессе направления межведомственных запросов и принятия решения при предоставлении услуг.

С точки зрения разработки программного обеспечения наибольшей методологической сложностью является реализация проактивности. Проактивность предполагает, что государство является инициатором предоставления государственных услуг. Должен осуществляться автоматический анализ сведений, известных о гражданине, на основании которых определяется перечень положенных ему государственных услуг. Проактивность в этом случае проявляется в форме человеко-машинного взаимодействия, когда машина сама предлагает или рекомендует услуги пользователю.

Проактивность основана на данных граждан, которые знает государство. Это может быть информация из различных государственных баз данных о том, какими услугами гражданин пользовался раньше, информацией о том, какие запросы он изучал и т.д. [1].

В настоящее время изучаются способы реализации проактивного предоставления государственных услуг в электронном виде. Экспертные системы были предложены в качестве инструмента для создания такого «умного

помощника», который мог бы рекомендовать гражданам государственные услуги. В процессе развития данного инструмента были созданы сети экспертных систем, особенности которых будут рассмотрены в данной работе.

Экспертные системы (далее ЭС) достаточно изучены на сегодняшний день. Их структура, особенности формирования базы знаний и построение механизмов логического вывода описаны в различных источниках [2]. С точки зрения классификации в данной работе используются диагностические или характеристические ЭС [3], основной задачей которых дать характеристику того или иного параметра пользователя.

ЭС строятся с привязкой к некой информационной системе (далее ИС) и встраиваются в ее объектную модель. Основные понятия, используемые в контексте сети ЭС:

1. Узел ЭС – ассоциируется с некими сущностями в предметной области.
2. Утверждение – особая форма предложения, которая в утвердительной форме выдвигает гипотезу относительно некоторого явления.
3. Сеть ЭС – ориентированный ациклический граф, включающий в себя односвязный список ребер (связей) между узлами сети ЭС.
4. Узел сети ЭС – в качестве узла сети ЭС используются: ЭС, узел ЭС, виртуальная ЭС. Начальным узлом в сети ЭС может быть только ЭС. Количество начальных узлов концептуально не ограничено.
5. Виртуальная ЭС в сети ЭС – специализированный узел сети ЭС, выполняющий узкоспециализированную роль. Определены 2 типа виртуальных ЭС:
   - - «Принято» (принятые сетью ЭС варианты решений);
   - - «Отвергнуто» (отвергнутые сетью ЭС варианты решений).
6. Связь в сети ЭС – ребро графа, связывающее один узел сети ЭС с другим узлом сети ЭС.

Поступающие данные к сети ЭС с помощью внешнего приложения переводятся в форму, понятную сети ЭС (утверждения). Сеть ЭС Обрабатывает полученные данные и выводит результат на внешнее приложение, которое преобразует его в информацию, понятную пользователю.

По умолчанию множество утверждений проходят через все ЭС в сети. В случае, если в какой-либо ЭС утверждений, относящихся к ней, обозначено не было, то ЭС автоматически определяет узел «не определено», который направляется на виртуальную ЭС «Отвергнутые».

Для проверки эффективности работы сети ЭС была поставлена задача смоделировать сеть ЭС для определения категории получателя государственных услуг для жизненной ситуации «Рождение ребенка».

В рамках поставленной задачи был предоставлен перечень из 18 государственных услуг. Для решения задачи были созданы и обучены 11 экспертных систем.

Сеть ЭС, спроектированная для конкретной жизненной ситуации, показывала правильные результаты при тестировании различных вариантов анкет. При возникновении ошибок при настройке сети ЭС на предметную область можно легко переобучить отдельно взятую ЭС или изменить топологию самой сети.

Учитывая прошлый опыт в создании одной многоуровневой ЭС для решения подобных задач [4], сеть ЭС более практична в использовании по следующим причинам:

1) В случае, если какие-либо созданные ранее в системе ЭС подходят для новой задачи, то их также можно использовать при моделировании новой сети;
2) В сети создаются максимально простые ЭС, настройка и обучение которых не составляет труда для эксперта предметной области;
3) Обработка утверждений в сети ЭС занимает значительно меньше процессорного времени, нежели работа одной большой многоуровневой ЭС;
4) Сеть ЭС легко встраивается в любую информационную систему;
5) Поскольку сама работа сети ЭС скрыта от пользователя, то можно создавать в сети вспомогательные узлы, которые не будут выводится в качестве результативных, а использоваться внутри сети.

В случае изменения законодательства, появления новых государственных услуг, потребуется лишь изменить или перенастроить отдельные экспертные системы, или переконфигурировать топологию сети без изменения программной части, то есть внешнего приложения. С этой задачей может справиться специалист предметной области без привлечения программистов. Соответственно, трудовые и материальные затраты на необходимые изменения будут минимальны.

В рамках решаемой задачи сети ЭС могут быть использованы как инструмент проактивного предоставления государственных услуг. В то же время, сети ЭС при своей универсальности могут использоваться для различных прикладных задач, где необходимо заменить эксперта в какой-либо предметной области.

СПИСОК ЛИТЕРАТУРЫ

1. Tibilova, G.S., Ovcharenko, A.V., Potapova, A.V. Proactivity and Subsidiarity as the Basic Principles of Digital Transformation of State Interaction with Citizens and Businesses. // CPS&C'2019 Book of Papers, 2019. pp. 601-610. [Электронный ресурс] https://doi.org/10.1007/978-3-030-34983-7_53
2. Чуркин В.И. Экспертные системы: учебное пособие. СПб.: Изд-во Политехн. ун-та, 2005. 68с.
3. Крицкая В. П. Методы и средства моделирования экспертных социально-экономических систем и систем поддержки принятия решений. // В кн.: Международная конференция по мягким вычислениям и измерениям, Санкт-Петербург, 2016, с. 92-95.
4. Потапова А.В., Тибилова Г.С., Овчаренко А.В. Применение экспертных систем при проектировании проактивных государственных услуг. // В кн.: Материалы XI Международной научно-теоретической конференции «Коммуникативные стратегии информационного общества», Санкт-Петербург, 2019. с. 143-152.

УДК 004.891.3

РАЗРАБОТКА МЕТОДИКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВЕННЫХ УСЛУГ

Потапова Анастасия Викторовна[1], Тибилова Галина Саламовна[2], Овчаренко Андрей Вячеславович[2], Дьяченко Наталья Владимировна[3]

[1] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[2] СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Черняховского ул., 59, Санкт-Петербург, 191040, Россия
[3] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mails: anastasia589@mail.ru, tibilova@iac.spb.ru, ovcharenko@iac.spb.ru, nat230209@yandex.ru

Аннотация. В статье рассматриваются вопросы оценки и планирования цифровой трансформации государственных услуг в рамках регионального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации». Рассматривается понятие целевой модели цифровой трансформации государственных услуг, приводятся направления трансформации и подходы к планированию.

Ключевые слова: целевая модель; цифровая трансформация; проактивность; государственные услуги; реестровая модель.

DEVELOPMENT OF A METHODS FOR DIGITAL TRANSFORMATION OF PUBLIC SERVICES

Potapova Anastasiya[1], Tibilova Galina[2], Ovcharenko Andrey[2], Dyachenko Natalia[3]

[1] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[2] St. Petersburg State Unitary Firm «St. Petersburg Information and Analytical Centre»
59 Chernyakhovsky St, St. Petersburg, 191040, Russia
[3] Russian State Hydrometeorological University
79 Voronezhskya St., St. Petersburg, 192007, Russia
e-mails: anastasia589@mail.ru, tibilova@iac.spb.ru, ovcharenko@iac.spb.ru, nat230209@yandex.ru

Abstract. The article examines the issues of assessing and planning the digital transformation of public services within the framework of the regional project «Digital Public Administration» of the national program «Digital Economy of the Russian Federation». The concept of a target model of digital transformation of public services is considered, directions of transformation and approaches to planning are given.

Keywords: target model; digital transformation; proactivity; public services; registry model.

В период с 2000 по 2019 годы осуществлялось построение электронного правительства, которое ставит в центр взаимодействий государство и занимается цифровизацией связей «государство-государство» (межведомственное электронное взаимодействие), «государство-граждане» и «государство-организации» (оказание государственных услуг). Начиная с 2019 года в связи с национальным проектом «Цифровая экономика Российской Федерации» появилось понятие «цифровая трансформация». Цифровая трансформация предполагает постановку в центр Гражданина или Организации за исключением государственных органов. То есть связи, переводимые в цифровой вид, должны быть дополнены следующими видами связей [1]:

- гражданин – гражданин;
- гражданин – организации;
- организации-организации.

При постановке гражданина в центр цифровой трансформации ключевое значение приобретает Жизненная ситуация, а в направлении ИТ – цифровая поддержка решения жизненных ситуаций. Цифровая поддержка решения жизненных ситуаций включает в себя:

- информацию в цифровом виде об услугах, сервисах, возможностях и способах решения жизненной ситуации;
- электронные государственные услуги, соответствующие жизненной ситуации;
- иные сервисы в цифровом виде, а именно сервисы коммерческих компаний, сервисы подведомственных учреждений и предприятий, информационные сервисы, электронные очереди, он-лайн платежи, необходимые и/или полезные для решения жизненной ситуации.

Качество цифровой поддержки решения жизненных ситуаций можно измерить через цифровую зрелость государственных услуг и сервисов.

Для измерения Цифровой зрелости президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности 28.03.2019 была утверждена матрица оценки цифровой зрелости государственных (муниципальных) услуг (далее – Матрица) [2].

При оценке цифровой зрелости государственных услуг в Санкт-Петербурге, согласно Матрице, был зафиксирован ряд методологических проблем, препятствующих объективной оценке уровня «цифровой зрелости» региона с использованием Матрицы. Так, например, описание условий доступности одного

показателя в Матрице соответствует нескольким уровням «цифровой» зрелости, ввиду чего в большинстве случаев выбор одного уровня Матрицы по конкретной услуге невозможен.

Для решения данных методологических проблем в Санкт-Петербурге была разработана собственная целевая модель цифровой трансформации и методика оценки цифровой зрелости государственных услуг и сервисов (далее – Методика).

В методике были учтены принципы цифровой трансформации государственных услуг, обозначенные Минкосвязью России:

1) реестровая модель предоставления услуг;
2) проактивность предоставления услуг [3];
3) экстерриториальность предоставления услуг;
4) многоканальность предоставления услуг;
5) исключение участия человека в процессе направления межведомственных запросов и принятия решения при предоставлении услуг.

Методика предполагает, что цифровая зрелость включает в себя:

- цифровую зрелость государственных (муниципальных) услуг (каждой в отдельности), которая, в свою очередь, включает:
  - оценку экстерриториальности (ЭКС);
  - оценку «цифровой зрелости» в соответствии с матрицей, представленной в Методике;
- уровень «цифровой зрелости» регионального Портала государственных (муниципальных) услуг (в целом), которая, в свою очередь, включает:
  - оценку общей «цифровой зрелости» Портала, его удобства и современности;
  - оценку развитости дополнительных цифровых сервисов.

Методика содержит шкалы оценки и формулы расчета указанных параметров. Кроме того, методика позволяет гибко планировать цифровую трансформацию, повышая цифровую зрелость.

Повысить цифровую зрелость можно:

– за счет повышения цифровой зрелости отдельных государственных услуг, перехода с текущего уровня, на котором находится услуга, на следующий уровень в соответствии с матрицей цифровой зрелости, представленной в Методике. Цифровая зрелость государственных услуг повышается по мере перевода услуг в электронный вид, внедрения принципа проактивности, внедрения автоматического межведомственного взаимодействия, перевода результата предоставления услуги в электронный вид;

– за счет повышения цифровой зрелости, удобства и современности Портала госуслуг. В Методике представлены критерии оценки, например: наличие версий и приложений для мобильных устройств, чат-ботов, интеграции с социальными сетями, адаптации для слабовидящих и незрячих, развитость механизмов обратной связи, способы авторизации на портале, и др.;

– за счет наращивания количества и повышения цифровой зрелости сервисов, не являющихся государственными услугами, среди которых выделяются: сервисы коммерческих компаний, информационные сервисы, в том числе получение гражданином информации о себе из различных источников, сервисы подведомственных учреждений и предприятий, социальные сервисы, способствующие укреплению согласия в обществе и гуманизации общественных отношений, электронные очереди, платежи, суперсервисы, дополнительные сервисы, размещенные на Портале в форме виджетов, ссылок на другие ресурсы.

Для планирования цифровой трансформации с использованием Методики необходимо:

– установить желаемый прирост цифровой зрелости за период в баллах или в долях от количества баллов в базовом периоде;

– выбрать тактику, за счет чего будет осуществляться этот прирост в период планирования (повышение уровня цифровой зрелости государственных (муниципальных) услуг, повышение удобства и современности портала, развитие экстерриториальности, расширение дополнительных сервисов, создание региональных суперсервисов и т.д.);

– установить контрольные даты для измерения цифровой зрелости.

СПИСОК ЛИТЕРАТУРЫ

1. Tibilova, G.S., Ovcharenko, A.V., Potapova, A.V. Proactivity and Subsidiarity as the Basic Principles of Digital Transformation of State Interaction with Citizens and Businesses. // CPS&C'2019 Book of Papers, 2019. pp. 601-610. [Электронный ресурс] https://doi.org/10.1007/978-3-030-34983-7_53
2. Матрица цифровой зрелости https://digital.gov.ru/uploaded/files/matritsa-otsenki-tsifrovoj-zrelosti.pdf
3. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 20.02.2019.
4. Потапова А.В., Тибилова Г.С., Овчаренко А.В. Применение экспертных систем при проектировании проактивных государственных услуг. // В кн.: Материалы XI Международной научно-теоретической конференции «Коммуникативные стратегии информационного общества», Санкт-Петербург, 2019. с. 143-152.

УДК 336.5

ПРОБЛЕМЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ БЮДЖЕТНЫХ РАСХОДОВ ПРИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Смирнова Елена Юрьевна
СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Транспортный пер., 6, Санкт-Петербург, 191040, Россия
e-mail: 7430202@gmail.com

Аннотация. Рассматриваются методические аспекты многомерной оценки эффективности использования бюджетных ресурсов по мере развития и использования информационных технологий в процессе цифровой трансформации государственного управления.

Ключевые слова: эффективное управление бюджетом; результативность затрат; экономичность использования ресурсов; экономия бюджетных расходов; цифровое правительство.

PROBLEMS OF BUDGET PERFORMANCE ASSESSING WITH THE DIGITALIZATION OF PUBLIC ADMINISTRATION

Smirnova Elena
St. Petersburg State Unitary Firm «St. Petersburg Information and Analytical Centre»
6 Transportnyj Per, St. Petersburg, 191040, Russia
e-mail: 7430202@gmail.com

Abstract. The paper considers methodological aspects of multidimensional assessing the budget performance with the development and use of information technologies under the digital transformation of public administration.

Keywords: budgeting performance management; budget cost effectiveness; budget expenditure efficiency; budget spending saving; digital government.

В мировой практике для оценки эффективности при государственном программном планировании и бюджетировании, ориентированном на результат, используются три основные метрики: результативность достижения целевых показателей (effectiveness), эффективность использования ресурсов (efficiency), а также экономичность расходования бюджетных средств. В российском законодательстве сохраняется [1] синонимичность этих терминов, приводящая к вариативным трактовкам при выборе показателей для анализа и планирования бюджетных расходов и оценки эффективности государственного управления.

Проблема оценки влияния использования информационных технологий на результат государственного управления состоит в том, что искомый эффект является нематериальным общественным благом и проявляется долгосрочной перспективе. Специфика цифровизации управления заключается в создании целостных технологических сред (экосистем, платформенных решений), в рамках которых на основе средств вычислительной техники и информационных технологий создается дружественное пользователю окружение для решения целых классов задач, а не отдельных задач (как это происходило на этапе информатизации). Для этого требуется рациональный пересмотр существующих бизнес-процессов с точки зрения работы на конечный результат. Феномен цифровой трансформации в государственном управлении рассматривается как переход от использования технологий для информационно-аналитической поддержки процессов принятия решений к использованию технологий для формирования результатов [2] государственного управления — «цифровое правительство» идет на смену «электронному правительству».

Цифровая трансформация государственного управления ассоциируется с повышением его качества. Межстрановое исследование РАНХиГС [3] на основе статистического анализа данных ООН, Всемирного банка и ВЭФ подтвердило высокую корреляцию между развитием электронного правительства и параметрами качества государственного управления: индексом результативности правительства, индексом контроля коррупции и индексом Doing Business, а также выявило умеренную взаимосвязь между развитием электронных услуг и уровнем эффективности государственных расходов.

Идея «оптимизация» расходов в смысле их минимизации полезна для достижения фиксированного результата, но с точки зрения развития необходимо стремиться к достижению максимального результата при соблюдении установленных бюджетных ограничений, то есть результативность имеет приоритет над экономичностью. В ряду лучших практик государственного планирования сегодня используются обзоры бюджетных расходов [4] на основе пост-факт анализа и экспертного обсуждения их конечной результативности, что выступает инструментом приоритизации направлений использования средств.

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьев Р.С., Голованова Н.В. Понятие эффективности бюджетных расходов: теория и законодательство // НИФИ. Финансовый журнал. 2016. № 1 (29). С. 61-69.
2. Сидоренко Э.Л., Барциц И.Н., Хисамова З.И. Эффективность цифрового государственного управления: теоретические и прикладные аспекты // Вопросы государственного и муниципального управления. 2019. № 2. С.93-114.
3. Добролюбова Е.И., Южаков В.Н., Ефремов А.А., Клочкова Е.Н., Талапина Э.В., Старцев Я.Ю. Цифровое будущее государственного управления по результатам. М.: Издательский дом «Дело» РАНХиГС, 2019. 114 с.
4. Лавров А. М. Логика и перспективы бюджетных реформ в России: в поисках «оптимальной децентрализации». М.: Изд. дом Высшей школы экономики, 2019. 832 с.

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 364.1

СОЦИАЛЬНАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Артюхин Антон Сергеевич
Ленинградский государственный университет им. А.С. Пушкина
Подгорная ул., 17, Выборг, 188800, Россия
e-mail: antsart@yandex.ru

Аннотация. Рассматривается проблема личной безопасности в условиях информационного общества. Падение взаимного доверия в социальных коммуникациях ведёт к усилению страхов и тревог людей в отношении друг друга и создаёт неблагоприятную психологическую атмосферу, способствующую социальной дестабилизации.

Ключевые слова: информационное общество, социальная безопасность личности, потребность в безопасности существования, социальные страхи и тревоги, ценность доверия.

THE SOCIAL SECURITY OF PERSONALITY IN THE MODERN SOCIETY

Artyuhin Anton
The Leningrad State University, named after A.S. Pushkin
17 Podgornaya St, Vyborg, 188800, Russia
e-mail: antsart@yandex.ru

Abstract. The article considers the personal security problem in the information society. The decline of mutual trust in social communications leads to increased human fears and anxieties about each other and creates an unfavorable psychological atmosphere contributing social instability.

Keywords: information society, social security of personality, need for existential security, social fears and anxieties, value of trust.

Современное информационное общество предоставляет людям огромное количество новых возможностей, делающих их жизнь более удобной и лёгкой. Но вместе с тем за достижения современной цивилизации приходится платить большую цену. Технический прогресс влечёт за собой и массу негативных последствий. Наиболее очевидными из них являются всё более учащающиеся в последние годы природные катаклизмы и экологические катастрофы, вызванные человеческим воздействием на окружающую среду, эпидемии и болезни. Ни одно общество, даже самое высокоразвитое, не может избежать и целого ряда социальных проблем: конфликты, насилие, преступность, безработица, бедность. Сегодня остаётся всё меньше оснований считать, что эти проблемы не коснутся нас лично. В условиях всеобщей нестабильности остро встаёт вопрос о личной безопасности человека в обществе, иной раз сводящийся к физическому и социальному выживанию. Может ли человек сам для себя что-то в этой сфере сделать, не уповая только лишь на государство?

Потребность в обеспечении личной безопасности является одной из базовых потребностей, которую Абрахам Маслоу относил к числу экзистенциальных, связанных с отсутствием серьёзных угроз жизни. Субъективное стремление обеспечить безопасные условия своей жизни в обществе во многом направляет и стимулирует деятельность человека. Потребность в безопасности устремляет человека к поиску тех средств, которые позволили бы вернуть ему чувство связанности с другими, избавиться от ощущения ничтожности и незащищённости перед окружающим миром.

Конечно, невозможно достичь состояния абсолютной безопасности, в жизни человека всегда присутствуют случайности (на всё есть «время и случай»). Безопасность – понятие, имеющее вероятностный характер. Главное – достичь ощущения своей безопасности. Понятно, что человек не может отменить объективные закономерности исторического развития общества и существующие угрозы. Но и в этом случае может быть полезен совет, данный древнеримским императором, представителем стоической философии Марком Аврелием: «Измени отношение к вещам, которые беспокоят, и ты будешь от них в безопасности». Но не каждый так может сделать. Да и достигнутое таким путём состояние безопасности может оказаться обманчивым.

Люди во все времена стремились обеспечить себе приемлемый уровень безопасности жизни в обществе, надеясь прежде всего на себя. Эту установку заметил ещё Томас Гоббс, в силу неизбежности взаимного недоверия людей друг к другу «нет более разумного для человека способа обеспечить свою жизнь, чем принятие предупредительных мер, т. е. силой или хитростью держать в узде всех, кого он может, до тех пор пока не убедится,

что нет другой силы, достаточно внушительной, чтобы быть для него опасной» [1]. Недоверие к другим заставляет человека «употреблять насилие в целях самозащиты» [1]. Превосходящей всех силой обладает государство, которое только и может выступать гарантом безопасности народа, особенно при централизации власти. Как заметила американская писательница Уилла Катер, никогда не стоит ставить свою безопасность в зависимость от благородства другого человека. Эгоизм и корыстолюбие в конечном итоге одерживают верх.

Шарль Монтескье считал неотъемлемым условием политической свободы гражданина его безопасность или хотя бы обретение «уверенности гражданина в своей безопасности» [2]. Любое посягательство на жизнь и безопасность человека Ш. Монтескье предложил рассматривать как тяжкое уголовное преступление, наказанием за которое должна быть смертная казнь, которая является «как бы лекарством для больного общества» [2].

В современном обществе с его нарастающим спектром угроз возможность жить, не подвергая себя различным рискам и опасностям, становится всё более значимой ценностью, приобретающий универсальный характер.

Социальную безопасность личности нередко трактуют в узком смысле слова, сводя её к мерам социальной защиты населения и повышению уровня материального благосостояния и социального обеспечения. Но проблема сложнее и должна увязываться с качеством жизни человека в обществе и с восприятием людьми друг друга. Склонны ли люди доверять или бояться друг друга?

Социальная безопасность личности обычно понимается как «система взаимодействия личности как индивида и субъекта деятельности со средой, включающая осознание негативных воздействий социальной среды; умения и навыки самозащиты и предотвращения социальных опасностей, обеспечивающие ей успешное взаимодействие с другими людьми, реализацию способностей и удовлетворение потребностей» [3]. В этом смысле элементами социальной безопасности личности являются физическая, психологическая, духовно-нравственная, гражданско-правовая, информационная безопасности.

В принятых в последние годы международных документах о правах человека говорится о двух компонентах безопасности человека – свободу от страха и свободу от нищеты и бедности. В Итоговом документе Всемирного саммита ООН (2005) в п. 143 говорится: «Мы подчёркиваем право людей жить в условиях свободы и достоинства, будучи избавленным от нищеты и отчаяния. Мы признаём, что все люди, в том числе уязвимые люди, имеют право быть избавленными от страха и нужды, имея равные возможности пользоваться всеми своими правами и в полной мере раскрывать свой человеческий потенциал. С этой целью мы обязуемся обсудить и определить в Генеральной Ассамблее понятие «безопасность человека» [4].

Следует иметь в виду, что людям свойственно превозносить собственную безопасность, добиваться её достижения за счёт безопасности других людей и даже народов.

Всё актуальнее становится принцип равенства безопасности в отношении всех членов общества и мирового сообщества. В силу этого люди призваны сдерживать свои инстинкты, ограничивать эгоистические и враждебные устремления, поддерживать правила мирного общежития.

Данные опроса ВЦИОМ, проведённого в октябре 2019 года, показали, что доля жителей России постоянно испытывающих стресс за последнее десятилетие увеличилась с 3% до 8%, а часто испытывающих стресс – с 15% до 17% [5]. К основным страхам россиян относятся возможный рост социальной несправедливости (68%), риск снижения доходов (63%), лишения бесплатной медпомощи (58%), рост преступности (36%) [6].

В сфере социальных взаимодействий наиболее сильны уличные страхи (30%), связанные с высоким уровнем уличной преступности; страхи во время посещения органов государственной власти (25%), что связано с пренебрежительным отношением чиновников при общении с гражданами; страхи при обращении в медицинские учреждения (23%), что обусловлено опасением столкнуться с некачественной медицинской помощью, могущей нанести вред здоровью, и грубостью персонала.

Безопасность социальных взаимоотношений предполагает бесконфликтный характер взаимодействия между людьми, исключающее проявление агрессии и насилия. Личную безопасность невозможно обеспечить без сохранения в обществе нравственных ценностей и установок, непосредственного влияющих на мотивы социального поведения. Культ материального успеха в ущерб духовному развитию дезориентирует человека и подрывает его нравственное здоровье. Духовная пустота и неосознание необходимости удовлетворения духовных потребностей ведёт к психическим расстройствам и различным формам девиантного поведения, от проявлений которого страдают все окружающие. Создание привлекательного образа из культа силы и агрессии ведёт к терпимости в отношении проявлений экстремизма и терроризма. Весьма распространено неуважение к существующим традициям, чужим взглядам и убеждениям.

Безопасность создаёт необходимые условия и предпосылки для созидательной деятельности людей, улучшения их благосостояния и увеличения общественного богатства.

СПИСОК ЛИТЕРАТУРЫ

1. Гоббс Т. Левиафан, или Материя, форма и власть государства церковного и гражданского. – М.: Мысль, 2001. 478 с.
2. Монтескье Ш. Л. О духе законов. – М.: Мысль, 1999. 672 с.
3. Кисляков П. А. Социальная безопасность личности: функциональные компоненты и направления формирования // Современные исследования социальных проблем. 2012. №5(13) [Электронный ресурс]. URL: http://soc-journal.ru (дата обращения: 08.06.2020).
4. Итоговый документ Всемирного саммита ООН 2005 г. Принят Резолюцией 60/1 ГА ООН от 16 сентября 2005 г. URL:https://www.un.org/ru/documents/decl_conv/declarations/outcome2005_ch4.shtml#t8 (дата обращения: 08.06.2020).
5. Жизнь в стрессе: масштаб проблемы и пути решения. Аналитический обзор ВЦИОМ №4075 от 09.10.2019 г. URL: https://wciom.ru/index.php?id=236&uid=9939 (дата обращения: 10.06.2020).
6. Карта страхов россиян: осень-2019. Аналитический обзор ВЦИОМ №4100 от 12.11.2019 г. URL: https://wciom.ru/index.php?id=236&uid=9999 (дата обращения: 10.06.2020).

УДК 32.019.51

МАССМЕДИЙНОЕ ПРОСТРАНСТВО КОНФЛИКТА

Байчик Анна Витальевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: annabaichik@gmail.com

Аннотация. Массмедийное пространство играет важную, а порой и определяющую роль в динамике социальных конфликтов. Обращение к его характеристике как арене столкновения взглядов, ценностей, идей, посредством массовой информации позволяет выявить пространственные характеристики среды динамики конфликтов, для эффективного использования в противоборстве сторон.

Ключевые слова: конфликт, массмедиа, ценность, медиатизация, массмедийное пространство.

MASS MEDIA SPACE OF CONFLICT

Baychik Anna
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia

Abstract. The mass media space plays an important and sometimes decisive role in the dynamics of social conflicts. Referring to its characterization as an arena for the clash of views, values, and ideas through mass media allows us to identify the spatial characteristics of the environment of conflict dynamics, for effective use in the confrontation of the parties.

Keywords: conflict, mass media, value, mediatization, mass media space.

Изучая влияние массовой информации на возникновение и разрешение социальных противоречий, ученые отдают предпочтение анализу роли СМИ в конфликтах, отражению в них конфликтного процесса. При этом без должного внимания остаются пространственно-временные характеристики медиатизации, имеющие важнейшее значение для дальнейшей концептуализации конфликта [2].

В отличие от достаточно исследованного информационного и медийного пространства, масмедийному не уделено должного внимания. К тому же, активное вторжение в социальное пространство «новых медиа» влияет на смешение понятий медийного и массмедийного пространства, которые применяются как синонимы. Но их отличительные характеристики, имеющие много общего, выявляются при обращении к понятиям «медиа» и массмедиа». Большинство характеристик массмедийного пространства присуще и медийному [3].

Обращение к масмедийному пространству, в котором происходит столкновение взглядов, ценностей, идей, концепций, идеологий позволяет выявить особенности пространственных характеристик среды развертывания различных типов и видов конфликта на основе массовой информации.

В отечественной социологии в самом общем виде понятие медиапространство применяется для обозначения системы средств массовой информации или медийной картины окружающей среды подразумевая под этим совокупность медиатекстов. Медиапространство позиционируется и как особая реальность, являющаяся частью социального пространства и организующая социальные практики и представления агентов системы производства и потребления массовой информации. Зарубежные исследователи применяют понятие как аналог киберпространства и цифровых медиа.

Более вариативный взгляд на медиапространство мы встречаем у Е.М. Ним, считающей, что медийное пространство соотносится с контентом, медиатизированное – со средой его распространения и потребления, медийному пространству соответствуют каналы производства и передачи информации, то есть сами медиа и система их взаимосвязей [4].

Обращение к структуре и архитектуре массмедийного пространства позволяет расширить исследовательский опыт и перейти от единичного субъекта данного пространства в виде СМИ к анализу таких его компонентов, как масмедийное поле, ландшафт, поток, имеющих существенное значение в конфликтогенности общественных отношений.

Массмедийное пространство проявляет себя во всех трех видах среды конфликта: физической, общественно-психологической и социальной. И если при исследовании физической среды мы можем концентрировать внимание на массмедийном ландшафте, а общественно-психологической среды на медиасреде, как структурных элементах (архитектуре) масмедийного пространства, то в полной мере массмедийное пространство, как вся социокультурная реальность, представлено в социальной среде конфликта.

Большинство социальных конфликтов базируется на противоречиях ценностного характера. Любые политические и экономические интересы получают определенное ценностное обрамление, связанное с интерпретацией коренных вопросов мировоззрения, взаимоотношения человека и общества, проблем личной свободы, роли государства и т.д. выстраиваются ценностные противостояния и приоритеты.

Особая роль масмедийного пространства в ценностном конфликте обусловлена тем, что в отличие от конфликтов, развитие которых побуждается социально-политическими и социально-экономическими потребностями и интересами, ценностный конфликт имеет более выраженный морально-нравственный и идеологический характер.

Для понимания роли медиапространства в трансформации конфликтных отношений следует подчеркнуть, что медиапространство – это не простое отражение реальности, это социально конструируемое понимание мира. И это весьма важная характеристика медиапространства в контексте ценностного восприятия окружающего мира. Причем это конструирование носит как хаотичный, так и сознательно управляемый характер.

Оригинален взгляд С.И. Кулибаба на медиапространство как хаотичную систему духовно-ценностной информации, предполагающую в соответствии с различными интересами и потребностями пользователей необходимую духовно-познавательную среду, свободную от диктата и комфортную для социального выбора личностей. Выделяя адаптирующую, социализирующую и социально-интегрирующую функции медиапространства в культуре, ученый выявляет его роль как канала трансляции духовных ценностей [1].

Массмедийное пространство стало полем постановки, рефлексии, поиска решений проблем общественно-политической жизни общества. Это место «встречи» общественных и частных интересов. Эти интересы представлены идеями, взглядами, представлениями, идеологиями, в том числе и ценностями.

СПИСОК ЛИТЕРАТУРЫ

1. Кулибаба С. И. Медиапространство и трансляция духовных ценностей // Сборник материалов 1 Междунар. научн. конф. «Судьба России: вектор перемен». Екатеринбург, 8–10 июня 2007 года. URL: http://ural-yeltsin.ru/usefiles/media/Kulibaba.doc (дата обращения – 13.09.2019).
2. Лабуш Н. С., Пую А. С. Медиатизация экстремальных форм политического процесса: война, революция, терроризм. – СПб.: Изд-во С.-Петерб. ун-та, 2019. – 340 с.
3. Монастырева О. В. Медиапространство: обзор представлений и подходов к пониманию // Вестник АГУ. – 2010. – № 50. С. 56–62.
4. Ним Е. Г. Медиапространство: основные направления исследований // Бизнес. Общество. Власть. – № 14. –2013. – С. 31–44.

УДК 32.019.51

БЕЗОПАСНОСТЬ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВ В ЦИФРОВОМ МИРЕ: ПОИСК ПРИОРИТЕТОВ

Баранов Николай Алексеевич
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: nicbar@mail.ru

Аннотация. В статье рассматриваются современные технологии, расширяющие возможности для развития человека и одновременно обеспечивающие невиданный прежде уровень контроля над обществами, что приводит к противоречию между интересами человека и государства.

Ключевые слова: информационное общество, цифровизация, цифровые права, цифровой паноптикум, цифровой тоталитаризм.

THE SAFETY OF INDIVIDUALS, SOCIETIES AND STATES IN THE DIGITAL WORLD: SEARCHING FOR PRIORITIES

Baranov Nikolay
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: nicbar@mail.ru

Abstract. The article discusses modern technologies that expand opportunities for human development and at the same time provide an unprecedented level of control over societies, which leads to a contradiction between the interests of man and the state.

Keywords: information society, digitalization, digital rights, digital panopticon, digital totalitarianism.

Темпы развития инноваций оказываются настолько быстрыми, что игнорировать высокую динамику изменений без негативных последствий невозможно. Как утверждает петербургский нейролингвист Татьяна Черниговская, «цифровая реальность уже признак отбора в социум. Если представить себе некую страну, которая не может себе позволить войти в цифровой мир, можно считать, что ее вообще нет» [1]. Действительно, соответствие современным инновационным требованиям – это веление времени, а не просто модное увлечение технологиями.

Современные технологии востребованы как человеком, так и государством, которое, обладая широкими ресурсными возможностями, может навязать обществу свое понимание безопасности и административно ограничить свободу в интернете. Для человека новые технологии расширяют границы возможного, используемые в целях собственного развития и жизненного комфорта. Граждане используют технологии для контроля за властью и решения общественных проблем. Поиск оптимальных взаимоотношений между государством и гражданами в инновационной среде – важнейшая задача, стоящая перед социальными науками.

Возрастает роль граждан в производстве государственных услуг: они теперь рассматриваются не только как получатели, но и сопроизводители этих благ, что подразумевает более высокую ответственность в сфере производства и оказания государственных услуг. Резко возросло число мобильных приложений, позволяющих гражданам удовлетворять свои потребности в системе здравоохранения, образования, предоставления социальных услуг.

Составной частью цифрового управления и взаимодействия стала технология «больших данных», определяемая как наборы данных, размер которых превышает возможности стандартных программных средств по их сбору, хранению, управлению и анализу.

С одной стороны, «современные технологии, выстроенные в «цифре», позволяют быстро реагировать на повседневные проблемы жителей, отвечать на их инициативы, на их обращения, реагировать соответствующим образом, а значит, эффективнее и быстрее решать проблемы, с которыми люди сталкиваются в повседневной жизни» [2]. С другой стороны, возникает этический аспект использования больших данных. Государство и крупные корпорации получают доступ к персональным данным, делая это без явного согласия граждан или в обход законов. Более того, применяемые технологии анализа больших данных в сфере безопасности могут допускать ошибки, например, в процессе идентификации преступников или террористов, что приводит к дополнительным проверкам простых граждан или применению насилия к ним со стороны правоохранительных органов [3, с. 153].

Цифровизация наряду с возможностями для расширения демократических процедур несет с собой опасность уязвимости программного и аппаратного обеспечения, повышение конфликтности в киберпространстве, ограничения в обеспечении защиты цифровых прав и цифрового суверенитета как государства, так и граждан. Доступ к сети Интернет на международном уровне признан одним из базовых прав человека и закреплен в международном праве, что явилось основанием для создания в некоторых странах движений в защиту «цифровых прав». Так, Генеральная Ассамблея ООН «признает глобальный и открытый характер Интернета и стремительное развитие информационно-коммуникационных технологий в качестве одной из движущих сил ускорения прогресса на пути развития в его различных формах» [5]. Вместе с тем, этим же документом подтверждается право на неприкосновенность личной жизни.

В условиях пандемии COVID-19 проблема безопасности актуализируется, на что обращает внимание заместитель председателя Совета Безопасности Российской Федерации Д.А. Медведев. В своей статье «Сотрудничество в сфере безопасности в период пандемии нового коронавируса» он пишет о важности «провести чёткое разграничение между благами, которые даёт цифровизация, и угрозой появления «цифрового Большого Брата», ограничения фундаментальных прав и свобод человека. Экономическая эффективность, которую несёт цифровизация, - по его мнению, - не может быть куплена ценой «цифрового тоталитаризма» [4].

В Докладе, подготовленном к началу работы Давосского экономического форума в 2019 г., акцентируется внимание на технологической неустойчивости и вводится понятие «Цифровой паноптикум» («Digital Panopticon»), под которым понимаются новые формы социального контроля: «Распознавание лиц, анализ походки, цифровые приложения, аффективные вычисления, микрочипирование, цифровое чтение по губам, датчики, считывающие отпечатки пальцев – благодаря распространению этих технологий, мы движемся в мир, в котором все данные о нас собраны, хранятся и подвергаются проверке через алгоритмы искусственного интеллекта» [8]. Искусственный интеллект (ИИ) уже рассматривается в качестве новой реальности электронного правосудия [7], что может привести в дальнейшем к цифровой диктатуре ИИ.

Технологические переломные моменты в современном глобальном мире, называемые К. Швабом глубинными изменениями, оказывают противоречивое социальное воздействие, сопровождаемое как положительными, так и отрицательными эффектами. Среди негативных сторон кардинальных перемен отмечаются такие, как нарушение частной жизни, возможности наблюдения за человеком, обеспокоенность сохранностью личной информации, увеличение числа манипуляций, нарушение конфиденциальности и даже экзистенциональная угроза человечеству [6, С.141-190]. Больше половины глубинных изменений подвержены негативным эффектам, связанным с возможным вторжением в частную жизнь человека со стороны как государственных, так и корпоративных структур. Бюрократия всегда готова скорее запрещать, чем разрешать, однако пандемия продемонстрировала неожиданную тенденцию – согласие государственных структур на снятие некоторых регуляторных барьеров на пути цифровых технологий.

В политико-культурный контекст современных стран вплетаются потребности общества в создании безопасной цифровой среды, в которой заинтересованы и граждане, и государство. Возникает коллизия, связанная с поиском баланса полномочий государственных органов по обеспечению безопасности личности, общества и государства, с одной стороны, и недопустимостью их вторжения в частную сферу - с другой стороны. Данное противоречие актуально практически для всех современных государств независимо от политического режима и идеологических приоритетов. Выход видится в сочетании безопасного информационного пространства, создаваемого в решающей степени усилиями государства, и максимального использования возможностей цифровых технологий с пользой для человека посредством предоставления гражданам широких информационных прав.

СПИСОК ЛИТЕРАТУРЫ

1. «В мире рухнуло сразу всё». Татьяна Черниговская о цивилизации праздности и недоверии к информации // Центр стратегических оценок и прогнозов. 08.05.2020. URL: http://csef.ru/ru/nauka-i-obshchestvo/445/v-mire-ruhnulo-srazu-vsyo-tatyana-chernigovskaya-o-czivilizaczii-prazdnosti-i-nedoverii-k-informaczii-9165 (дата обращения: 04.07.2020).
2. Заседание Совета по развитию местного самоуправления. 30 января 2020 года. URL: http://www.kremlin.ru/events/president/news/62701 (дата обращения: 04.07.2020).
3. Косоруков А. А. Модель цифрового управления: открытые и большие данные // Политика и управление государством: Новые вызовы и векторы развития: Сборник статей / Под ред. А.И. Соловьева, Г.В. Пушкаревой. М.: Издательство «Аспект Пресс», 2019. С. 142-159.
4. Медведев Д.А. Сотрудничество в сфере безопасности в период пандемии нового коронавируса // Россия в глобальной политике. 17.06.2020. URL: https://globalaffairs.ru/articles/bezopasnost-v-period-pandemii/ (дата обращения: 01.07.2020).
5. Резолюция Генеральной Ассамблеи ООН от 18 декабря 2013 г. № 68/167 «Право на неприкосновенность личной жизни в цифровой век». URL: https://undocs.org/pdf?symbol=ru/A/RES/68/167 (дата обращения: 04.07.2020).
6. Шваб К. Четвертая промышленная революция: пер. с англ. М.: Эксмо, 2019. 209 с.
7. Numa A. Artificial intelligence as the new reality of e-justice. URL: https://e-estonia.com/artificial-intelligence-as-the-new-reality-of-e-justice/ (дата обращения: 04.07.2020).
8. The Global Risks Report 2019. 14th Edition. Geneva: World Economic Forum, 2019. 107 p. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (дата обращения: 04.07.2020).

УДК 004

ТЕХНОЛОГИИ ПОЛИТИЧЕСКОГО МАНИПУЛИРОВАНИЯ В ИНФОРМАЦИОННОЙ СРЕДЕ

Борщенко Виктор Владимирович
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: boss-victor@yandex.ru

Аннотация. В работе рассматривается манипуляционный потенциал в информационной сфере. Проводится классификация основных методов политического манипулирования. Рассматривается вопрос возрастающих возможностей методов и технологий политического манипулирования в информационном пространстве.

Ключевые слова: Манипуляционный потенциал, методы манипулирования, оценка возможностей, классификация методов, технологии манипулирования.

TECHNOLOGIES OF POLITICAL MANIPULATION IN THE INFORMATION ENVIRONMENT

Borshchenko Viktor Vladimirovich
North-West Institute of management Ranepa 57 Sredny Prospekt, Saint-Petersburg, 199178, Russia
e-mails: boss-victor@yandex.ru

Abstract. The paper considers the manipulative potential in the information sphere. The main methods of political manipulation are classified. The issue of increasing possibilities of methods and technologies of political manipulation in the information space is considered.

Key words: Manipulative potential, methods of manipulation, assessment of opportunities, classification of methods, manipulation technologies.

В последние годы методы скрытого управления постоянно видоизменялись и совершенствовались. Это, в первую очередь, можно связать с изменением условий инфокоммуникационных процессов и появлением такого нового технологического уклада как информационное общество, также известное, как общество знаний.

Важной составляющей любого процесса взаимодействия между конкретными социальными группами, людьми, общественными, политическими и другими организациями, как способом скрытого управления, является манипулирование.

Особую значимость к изменяющимся условиям распространения информации имеет политическое манипулирование. В самом общем виде оно представляет собой систему методов с целью сформировать политические установки или вызвать политическое поведение определенной направленности.

К основным методам политического манипулирования относятся: методы обмана; сокрытия информации; уход от обсуждения темы; информационной перегрузки; введения в заблуждение; дезинформации; отчуждения; индокринации; пропаганды; агитации; и другие.

Данные методы могут классифицироваться по таким признакам как достижение конкретных политических целей или воздействие на аудиторию.

Рассмотрим некоторые виды политической манипуляции:

1. Действия, вовлекающие группы людей и организаций в проект, который был создан, и в действия, которые проводятся для реализации данного проекта.

Одним из принципов сдерживания является принцип «двойных стандартов». Основной целью зарубежных стран в отношении Российской Федерации является ее сдерживание на международной арене. В качестве примера можно привести факт того, что в некоторых странах ограничивают действие российских СМИ (Украине, Прибалтике, Молдове), и это нормально, а если в России закрывают экстремистские СМИ, то американцы это называют ограничением свободы слова;

2. Действия, предназначенные для дискредитации чувств противников проекта.

Особенно ярко политическая манипуляция в этом направлении представлена демонизацией влиятельных политических деятелей.

3. Психологического давления на объект с целью изменить его поведение.

В данном случае применяются методы и приемы, которые призваны спровоцировать политического деятеля подчиниться. Главным мотивом выполнения распоряжений в данном случае является страх перед негативными санкциями.

В зависимости от воздействия на аудиторию можно выделить действия, направленные на изменение: поведения отдельных личностей, в первую очередь лидеров; политических взглядов общества в целом; взглядов и поведения групп людей.

На основе вышеизложенного, можно построить психологическую и рациональную модели политического манипулирования.

В рациональной модели манипулирование осуществляется посредством предоставления недостоверной информации.

Сущность манипулирования заключается в выборе стимулов, провоцирующих именно те психологических механизмы, вызывающие реакцию, удовлетворяющую потребности манипулятора. При таком

подходе индивид действует по принципу: стимул — реакция.

Методы политического манипулирования могут применяться для влияния на индивидуальное и массовое сознание.

Информационно-коммуникативные процессы современного общества способствуют созданию специальных манипуляционных технологий, в основе которых лежат методы политической манипуляции. Эти технологии представляют собой совокупность приемов, средств и методов, используемых для достижения целей.

Успешность любого технологического процесса, зависит от качества его информационного обеспечения. Имеющаяся информация напрямую влияет на принятие важных политических решений. Основными манипуляционными технологиями следует считать: ситуационное информационно-политическое манипулирование; систематическое информационно-политическое манипулирование; массированное информационно-политическое манипулирование.

В современном информационном обществе возможности методов и технологий политической манипуляции резко возрастают. Это обусловлено высокой скоростью создания и распространения информационных контентов. Распространение информации через интернет позволяет в сжатые сроки осветить интересующее событие, и передать мнение официальных источников или газет о нем, осветить комментарии очевидцев, предоставить им свое мнение. Наличие технической возможности обуславливает высокую потенциальную доступность всего общества. Модификация и навязывание политической информации в широких пределах путем распространения большого количества многократно повторяющегося материала образует предпосылки к формированию и появлению коллективного мнения, ведущего к действиям.

Можно сделать вывод, что значительное место среди методов информационной борьбы занимают технологии политического манипулирования. В их основе находятся как формирование, так и навязывание информационных контентов, основной задачей которых является влияние на политические взгляды различных категорий людей.

Информационное общество сегодня позволяет распространять информацию в модифицированной форме за счет развития информационных технологий и инфокоммуникационных структур в реальном времени.

Это создаёт предпосылки для повышения эффективности методов политического манипулирования путём развития различных манипуляционных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Кара-Мурза С.Г, Смирнов С. Манипуляция сознанием 2 [Электронный ресурс] URL: http://www.xliby.ru/politika/manipuljacija_soznaniem_2w/index.php (дата обращения: 05.08.2020).
2. Ланге О.В. К вопросу о специфике современных подходов к природе манипулятивных технологий в политике / О. В. Ланге // Вестник Кемеровского государственного университета – 2014. – №3 (59). – Т1. – С. 100 -105.
3. Левкин И.М., Микадзе С.Ю. Добывание и обработка информации в деловой разведке. Санкт-Петербург, 2015.
4. Кефели И.Ф. Актуализация проблемы информационно-психологической и когнитивной безопасности. Москва, 2017.
5. Goodin R. E. Manipulatory Politics. — L., 1980.

УДК 32.019.51

ПРОФЕССИОНАЛЬНЫЕ РИСКИ И ФАКТОРЫ СТРЕССА В ДЕЯТЕЛЬНОСТИ ЖУРНАЛИСТА ТЕЛЕВИЗИОННЫХ НОВОСТЕЙ

Виноградова Ксения Евгеньевна[1], Шадрина Виктория Андреевна[2]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
[2] Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mails: vinogradovamail@gmail.com, viktoriaspshadrina@gmail.com

Аннотация. В докладе анализируются факторы воздействия на психоэмоциональную сферу и поведение новостного журналиста, оцениваются профессиональные риски, связанные с его трудовой деятельностью.

Ключевые слова: стрессогенные факторы, профессиональные риски, репортер, фрустрации, психологическая безопасность.

PROFESSIONAL RISKS AND STRESS FACTORS IN THE WORK OF THE JOURNALIST OF TELEVISION NEWS

Vinogradova Ksenia[1], Shadrina Victoria[2]

[1] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
[2] The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: vinogradovamail@gmail.com, viktoriaspshadrina@gmail.com

Abstract. The report analyzes the factors affecting the psycho-emotional sphere and behavior of a news journalist, assesses the professional risks associated with his work.

Keywords: stress factors, occupational risks, reporter, frustrations.

В силу своих профессиональных обязанностей журналисты ежедневно подвергаются воздействию стрессогенных факторов. Под стрессогенными факторами С.В. Бабурин понимает совокупность раздражителей, влияющих на психофизическое состояние человека и его поведение [1].

В психологии же специалисты определяют стрессоры как неблагоприятные, значительные по силе и продолжительности внешние и внутренние воздействия, ведущие к возникновению стрессовых состояний.

Большую часть творческих задач в редакции новостного канала выполняют репортеры. От того, как они организуют съемочный процесс, зависит качество полученного сюжета.

К работнику службы новостей предъявляются высокие требования: он должен быть оперативным, мобильным, обладать адаптивностью, стрессоустойчивостью, умением быстро переключаться с одного задания на другое и, как отмечает М.С. Петрова, обладать особым «репортерским нюхом» на интересную информацию [2].

Деятельность журналиста новостного канала связана с высокой социальной ответственностью: сложно просчитать последствия его неаккуратного обращения с фактами. На журналиста информационного канала возлагается огромная ответственность, так как он выступает перед многомилионной аудиторией, транслирует картину мира. Высокий темп производства, ненормированный рабочий день, непредсказуемость каждого рабочего дня создает дополнительное напряжение, которое при длительном воздействии приводит к нервному истощению.

Профессиональные риски непосредственно связаны с трудовой деятельностью. Под профессиональным риском отечественные специалисты понимают «...вероятность возникновения профессиональных личностных деструкций и формирования неблагоприятных функциональных состояний у работников при выполнении трудовых функций из-за длительного воздействия негативных социально-бытовых и производственных факторов при недостаточном личностном и средовом ресурсе» [3].

Деятельность журналиста телевизионных новостей связана с психофизиологическими факторы риска, возникающими из-за физических перегрузок и перегрузок нервно-психической системы.

Исследователь Е. А. Балезина предлагает разделять риски социально-профессиональных групп, к которой мы можем отнести репортеров, на три категории.

В первую группу входят риски, связанные с особенностями профессиональной деятельности; во вторую те, которые возникают в процессе производства, третья группа включает в себя риски, формируемые внешними факторами институциональной и социетальной среды [4].

В работе журналистов телевизионных новостей мы можем выявить риски каждой из указанных групп. В процессе подготовки сюжета журналист сталкивается с рисками информационных и психоэмоциональных перегрузок; многочисленная коммуникация с разнообразным контингентом людей и повышенная ответственность перед аудиторией формируют риск возникновения эмоционального выгорания, депрессии, возникновения психосоматических расстройств.

Особенности труда репортеров определяются мультизадачностью, требованиями виртуозного владения техническими средствами подготовки и трансляции новостей и соответствующими компетенциями.

Помимо поиска информации, ее обработки, от журналиста требуются: а) умение работать с базами данных, статистикой; б) навыки пользования аудио-, видеотехникой; в) владение стратегиями продвижения «своей новости» посредством интернет-каналов, г) умение готовить текст, «видеть картинку», собирать факты, вступать коммуникацию, планировать сюжет, готовить сценарий и т.д.

Институциональная и социетальная среда в настоящее время не являются поддерживающими для журналистов. Многочисленные эксперты отмечают сложную ситуацию со свободой выражения журналистами собственной позиции. Редакции находятся в финансовой зависимости от владельцев, которые большей частью используют СМИ как инструмент влияния на власть. Отмечается зависимость контента от политических трендов. В целом существующие стрессовые факторы и психологические риски негативным образом сказываются на ощущении журналистом психологической безопасности и самовосприятии репортеров, являются причиной возникновения фрустрации и тревожности, негативно влияют на их эмоционально-личностную сферу и отношение журналистов к своей профессии.

СПИСОК ЛИТЕРАТУРЫ

1. Бабурин С.В. Психолого-педагогические основы пенитенциарной стрессологии: учебное пособие / Бабурин С. В., Чирков А. М. – Вологда: ВИПЭ ФСИН России, 2014. – 576 с.
2. Петрова М.С. Когнитивная компетенция будущего журналиста (сущность, структура, содержание) // Психология и педагогика: методика и проблемы практического применения. 2010. №17. С. 372-379.
3. Корнеева Я.А., Симонова Н.Н., Дегтева Г.Н. Понятия «Психологического риска» в профессиональной деятельности работников вахтовых форм труда на примере нефтегазодобывающих предприятий в условиях Крайнего Севера // Гигиена и санитария. 2013. №4. URL: https://cyberleninka.ru/article/n/ponyatiya-psihologicheskogo-riska-v-professionalnoy-deyatelnosti-rabotnikov-vahtovyh-form-truda-na-primere-neftegazodobyvayuschih (дата обращения: 08.07.2020).
4. Балезина Е.А. Риски социально-профессиональных групп: понятие и типология // Социальные и гуманитарные науки: теория и практика. 2018. № 1 (2). С. 344-352.

УДК 004

КАТАСТРОФИЗАЦИЯ СОБЫТИЙ В МЕДИА: ПРОЯВЛЕНИЯ ЭКСТРЕМИСТКОЙ НАПРАВЛЕННОСТИ

Гришанина Анастасия Николаевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: a.grishanina@spbu.ru

Аннотация. В докладе анализируется круг вопросов, связанных с размещением в медиа текстов на тему катастроф, содержащих элементы экстремизма; освещается проблема катастрофизации общества под влиянием материалов мессенджеров и комментариев к ним. Представлены первичные исследования мотивов переписки на темы роликов и изображений, а также некоторые данные опросов.

Ключевые слова: экстремизм, социальные сети, речевое поведение, мотивация, медиа, актуальное состояние, катастрофизация.

CATASTROPHIZATION OF EVENTS IN THE MEDIA: MANIFESTATIONS OF EXTREMIST ORIENTATION

Grishanina Anastasiia
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: a.grishanina@spbu.ru

Abstract. The theses analyze the range of issues related to the placement of texts on the topic of catastrophes in the media containing elements of extremism; the problem of catastrophizing society under the influence of messenger materials and comments on them is studied. Primary research on the motives of correspondence on the topics of videos and images, as well as some survey data, is presented.

Keywords: extremism, social networks, speech behavior, motivation, media, current state, catastrophization.

Текущий год стал показательным в плане расстановки приоритетов и выбора стратегий представления материалов в медиасреде: средства массовой информации, блоги, социальные сети, подкасты. Во многих текстах присутствуют язык вражды (hate speech, риторика ненависти), «нагнетание» эмоций в освещении событий, катастрофические предсказания журналистов («мы все умрем»).

Психологи отмечают, что на протяжении жизненного пути «психическое здоровье человека может подвергаться различным колебаниям и находиться в некотором балансировании между нормативным и ненормативным состоянием». Эти состояния могут носить как кратковременный характер, так и более или менее затяжной. Могут возникать состояния ремиссии, когда больной человек становится продуктивным на какое-то время [1].

Пандемия, очевидно, поменяет границы состояния психического здоровья и нормативности личности не только в отдельной стране, но и во всем мире. Медиа играют в этом процессе огромную роль, так как в период самоизоляции человек потребляет информацию исключительно из гаджетов и экрана телевизора.

В социальных сетях в конце марта – начале апреля появилось множество клипов, фейковых интервью, репортажей, которые рассказывали о скором конце света, о необходимости спасаться от коронавируса. Методом сравнительного анализа установлено, что во многих текстах и картинках есть экстремистские проявления, прямые и косвенные призывы к неповиновению власти, к нарушению режима самоизоляции и другие.

Основные интенции авторов сводились к следующему:

- эмоции и восклицания типа: «Не может быть!», «Ужасно!»;
- оценка ситуации в роли экзаменатора: «Что происходит?» без попытки разобраться, ставка на неудовлетворительную оценку;
- самозначимость и судьбоносность выводов для понимания настоящего и будущего.

Философ и психолог И.А. Ильин писал: «Болезнь есть как бы таинственная запись, которую нам надо расшифровать: в ней записано о нашей прежней неверной жизни и потом о новой, предстоящей нам мудрой и здоровой жизни. Этот шифр мы должны разгадать, истолковать и осуществить. В этом – смысл болезни» [5, 6].

Первичный опрос о восприятии текстов и изображений, касающихся пандемии, среди пользователей мессенджеров WhatsApp, Viber показал высокую степень тревожности респондентов: люди воспринимают друг друга как помеху в достижении личных целей. При нарастании паники возникают отношения нетерпимости, агрессия. В ответ на публичные сообщения идут ругательства и оскорбления.

Пандемия показала, что людям не хватает психологического знания, культуры человеческих отношений для того, чтобы справиться с такой ситуацией. Большой процент опрошенных высказал желание отключить мессенджеры, чтобы не испытывать информационно-психологического давления, однако не может этого сделать из необходимости постоянной связи с близкими.

Общение в такой период часто носит враждебный характер. А.А. Денисова определяет язык вражды как совокупность языковых средств, которые выражают негативное отношение по отношению к оппонентам, то

есть к носителям другой системы ценностей. По её мнению, язык вражды может быть формой проявления расизма, сексизма, гомофобии и других видов социальной нетерпимости [4]. При этом стереотипы отрицательно характеризуют социальные субъекты. Такие высказывания формируют или поддерживают враждебное отношение по отношению к кому-либо или чему-либо.

Весной 2020 г. появился новый сленг (карантинка, ковидка) и актуализировалась специализированная лексика (антитела, карантин, симптомы и др.).

Языку вражды в социальных сетях и мессенджерах пользователи пытаются противопоставить язык согласия, главный посыл которого – перестать быть «врагом» для своего собеседника, понять его и не выдвигать тезисов о грядущей катастрофе.

Язык согласия может выражаться в вежливых формах фраз, в речевых поддержках и речевых подхватах (завершениях или дополнениях реплик), уважительных номинациях по отношению к собеседнику, сообщениях, подтверждающие правильность высказываний оппонента. Также диалогическое единство, то есть явление, когда один из собеседников запрашивает речевую поддержку и получает её в ответ, является сигналом языка согласия [3, с. 76; 6, с. 163].

Отмечено: текст, диалог переписки, комментарии могут расцениваться как материал, содержащий признаки вражды, если они не имеют вежливой формы оформления мыслей. Например, отсутствие формы приветствия, реакции на текст собеседника, слова с осуждающей семантикой.

Д.В. Петросян указывает, что человеку важно осваивать «совокупности социальных практик поведения и сочетания их освоения с постижением культуры городского пространства» [2, с. 108].

Важно отметить, что данная попытка первичных исследований выявила многие проблемные зоны взаимодействия в медиа. Об этом говорят сами пользователи, согласившиеся ответить на вопросы, эксперты – специалисты, занимающиеся медиатекстами, а также данные опросов. Любой разговор о языке чрезвычайно важен, потому что с помощью него формируется языковая картина мира.

А.А. Данилова определяет языковую картину мира как представление об окружающей действительности в целом, её элементах и процессах, которые нашли отражение в языке; а также изображение с помощью языка человека, природы и мира [3, 179].

Автор справедливо отмечает важную особенность языковой картины мира, так как она отражает социальные ценности и дает прогноз развития общества.

СПИСОК ЛИТЕРАТУРЫ

1. Белоцерковская О.Л. Норма и патологи личности // Психологическая газета. 2020 19 июня. // https://psy.su/feed/8326/
2. Гришанина А.Н., Петросян Д.В. Городская культура повседневности в подготовке специалиста коммуникационного профиля // Рекламное и PR-образование в условиях информационно-технологических перемен: актуальные вопросы и тренды. Сб. мат-лов II междунар. науч.-практ. конф. / под общ. ред. К.В. Киуру. – Челябинск: Челяб. гос. ун-т, 2020. – С. 107–111.
3. Данилова А.А. Манипулирование, словом, в средствах массовой информации. – М.: Добросвет КДУ, 2011. 2002 с.
4. Денисова А. А. Язык вражды в российских СМИ: гендерное измерение // http://www.owl.ru/win/womplus/2002/denisova2.htm
5. Ильин И.А.О противлении злу силою. – М.: Изд-во: Эксмо-Пресс, 2017. – 160 с.
6. Язык вражды и язык согласия в социокультурном аспекте современности. Колл. монограф./ отв. ред. И.Т. Вепрева, Н. А. Купина, О.А. Михайлова. – Екатеринбург: Изд-во Уральского ун-та, 2006. – 516 с.

УДК 32

ПСИХОЛОГИЯ НАРЦИССИЗМА И НОВЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гуторов Владимир Александрович
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: gut-50@mail.ru

Аннотация. Рассматриваются различные интерпретации психологических аспектов информационной безопасности, связанных с стремительным развитием цифровых технологий в XXI в. Выявляются причины распространение в современном мире нарциссизма как одного из наиболее опасных симптомов политической нестабильности.

Ключевые слова: психология информационной безопасности, политическое лидерство, власть, социальная патология, нарциссизм.

PSYCHOLOGY OF NARCISSISM AND NEW THREATS TO INFORMATION SECURITY

Gutorov Vladimir
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: gut-50@mail.ru

Abstract. Various interpretations of the psychological aspects of information security associated with the rapid development of digital technologies in the 21st century are examined. The causes of the spread of narcissism as one of the most dangerous symptoms of political instability in the modern world are revealed.

Keywords: psychology of information security, political leadership, power; social pathology, narcissism.

Одной из наиболее примечательных тенденций в современных социальных науках является решительный поворот многих ученых к анализу многообразных аспектов психологической интерпретации проблем национальной и международной безопасности [1]. Новый этап информационной революции, связанный со стремительным развитием цифровых технологий в XXI в., значительно усилил данную тенденцию, способствуя возникновению междисциплинарного направления – психология информационной безопасности [2]. Психологическая составляющая сама по себе является наглядным доказательством и своеобразным гарантом того, что информационная безопасность в настоящее время уже не рассматривается как чисто техническая дисциплина, ограниченная проблемами антивирусного программного обеспечения, контроля доступа, шифрования и т.п. Об этом свидетельствует и ее тесное взаимодействие, например, с такими субдисциплинами как, например, «операционная психология», представители которой активно исследуют вызовы по противодействию угрозам национальной безопасности и смягчению их последствий, в том числе и в контексте консультативной поддержки, оказываемой политическим лидерам [3].

Причины диверсификации психологических исследований, затрагивающих проблемы политического лидерства, вполне очевидны. Например, сторонники либерального направления современной политической теории постоянно акцентируют внимание на двух взаимосвязанных факторах, ведущих к реструктуризации власти в результате информационной революции. Они утверждают, что, с одной стороны, информационная революция все более расширяет круг политических акторов, предоставляя им доступ к более или менее мощным инструментам для быстрого сбора, производства и распространения информации в мировом масштабе. Поскольку многие из либеральных теоретиков рассматривают информацию как центральный источник власти, с другой стороны, утверждается, что индивиды, ответственные за перераспределение информационных ресурсов, значительно усиливают свое влияние и, как следствие, стремятся утвердить свой авторитет в различных проблемных областях, что неизбежно приводит к перестройке глобальных властных отношений и нестабильному перераспределению власти [4].

По мнению многих специалистов, одним из наиболее опасных симптомов политической нестабильности является повсеместное распространение в современном мире нарциссизма как политического и культурного феномена. В социальном и психологическом плане нарциссизм рассматривается как регрессия к инфантильным нормам самооценки: нарциссические типы личности, постоянно ощущая собственную агрессивность, обычно не воспринимают адекватно идею усовершенствования и неспособны признать необходимость совета или помощи, полученных от кого-то другого. Относительная стабильность этой формы патологии объясняется тем, что локальные и глобальные зависимости и взаимодействия между индивидами, группами и социальными институтами становятся все более непрозрачными и рискованными. Это связано с возрастающим значением сверхсложных абстрактных систем, создаваемых для поддержания средств массовой коммуникации, финансов, энергетики, инфраструктуры безопасности, а также социальных и культурных учреждений. Эти системы требуют знаний и навыков специалистов.

Таким образом, культурный и политический нарциссизм является побочным следствием появления групп профессионалов нового типа, не только удовлетворяющих растущие потребности, но и создающих новые [5].

Тезисы подготовлены при поддержке Российского фонда фундаментальных исследований и Экспертного института социальных исследований, проект № 20-011-31349 «Либеральные ценности в современном мире: основные тенденции трансформации».

СПИСОК ЛИТЕРАТУРЫ

1. Howell A. Madness in International Relations: Psychology, Security, and the Global Governance of Mental Health. – London; New York: Routledge, 2011. – 186 p.
2. Zinatullin L. The Psychology of Information Security: Resolving Conflicts between Security Compliance and Human Behavior. – Cambridge: IT Governance Publishing, 2016. – 116 p.
3. Operational Psychology: A New Field to Support National Security and Public. Th. J. Williams, M. A. Staal, S. C. Harvey (eds.). – Santa Barbara, California; Denver, Colorado: Praeger, 2019. – 380 p.
4. Power and Security in the Information Age: Investigating the Role of the State in Cyberspace. M. D. Cavelty, V. Mauer, S. F. Krishna-Hensel (eds). - Burlington: Ashgate, 2007. ─ 167 p.
5. Klimczuk A. Experts and Cultural Narcissism: Relations in the Early 21st Century. – Saarbrücken: Lambert Academic Publishing, 2012. – 77 p.

УДК 32.019.51

КОММУНИКАТИВНЫЕ РЕСУРСЫ ПОЛИТИЧЕСКОГО ЭКСТРЕМИИЗМА (НА ПРИМЕРЕ АРАБСКИХ МЕДИА)

Дегтярева Ольга Викторовна
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: olgaspb2008@mail.ru

Аннотация. Глобальные процессы в области психологической защиты и информационной войны рассмотрены недостаточно. Важно проанализировать социально-психологические механизмы функционирования экстремистских организаций.

Ключевые слова: терроризм, экстремизм, геополитическая безопасность.

COMMUNICATIVE RESOURCES OF POLITICAL EXTREMISM (ON THE EXAMPLE OF ARAB MEDIA)

Degtyareva Olga
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: olgaspb2008@mail.ru

Abstract. The global processes haven't analyzed enough in the field of psychological defense and information war. The socio-psychological mechanisms of the functioning of extremist organizations is important to analyze more.

Keywords: terrorism, extremism, geopolitical security.

Для современного мира характерно становление и развитие информационного сообщества, в котором информация становится созидательной или разрушительной силой. Силой, способной не только объединять, восстанавливать, но также и разрушать мировое информационное и политическое пространство. Именно эта способность информации всегда привлекала радикально настроенные политические и религиозные общности. В Обращении к Генеральной Ассамблее ООН о приоритетах Генерального секретаря на 2020 г. [4]. Антониу Гутерриш, говоря о четырех надвигающихся угрозах – «эпической геополитической напряженности, климатическом кризисе, глобальном недоверии и технологических недостатках» – призвал «привести в порядок «Дикий Запад» (Wild West) киберпространства: террористов, расистов и других, кто сеет ненависть, эксплуатирует Интернет и социальные сети; ботов, которые распространяют дезинформацию, разжигая поляризацию и подрывая демократию» [2, с. 222]. Терроризм стремится дегуманизировать врага, то есть лишить его обычных человеческих диспозиций. Подобный дискурс преследует цель сплотить потенциальных террористов и усилить их самоидентификацию. В содержательном плане, помимо религиозных различий, наиболее эффективным является общая для членов группы политическая катастрофа, например, потеря своей государственной автономии, лидерства в регионе, смерть вождя, и т. п. [3, с. 34].

Исследователь Роберт Штернберг (Robert Sternberg (2003) разработал трехкомпонентную модель психологии ненависти, согласно которой пропаганда ненависти имеет, как правило, три цели: 1) отрицание положительной эмоциональной оценки враждебной группы; 2) разжигание страстей: злости и страха (замечательный пример – описанные Джорджем Оруэллом в «1984» «пятиминутки ненависти»); 3) генерирование решений, основанных на ошибочных когнитивных выводах и порочном критическом мышлении.

«Хизб ут-Тахрир аль Ислами» является одной из таких политических партий, которая в медийном пространстве позиционирует себя как организация, распространяющая ислам посредством замены мыслей, чувств и законов общества для того, чтобы сделать эти мысли общепринятыми и побудить людей жить с Аллахом. Партия имеет собственное издательство «Al-Khilafah Publications», которое публикует в сети журнал «Khilafah». В своих публикациях партия пропагандирует идею о том, что государство Халифа является единственным исполнителем, носителем и хранителем Ислама, а Ислам – единственным гарантом мира, а потому только достойный лидер сможет вывести нацию из темноты к свету.

В июле 2017 г. в интернет-издании «Аль-Джазира» была размещена новость, в которой сообщалось, что Индонезия запретила группировку Хизб ут-Тахрир в соответствии с противоречивым президентским указом. По словам Фредди Хари, генерального директора Министерства юстиции и прав человека, был отменен правовой статус Хизб ут-Тахрир, выступающей за то, чтобы Индонезия приняла исламский закон. Около 2000 человек из исламских групп протестовали против порядка в Джакарте, осуждая правительство как репрессивное и тираническое. Акции протеста возобновлялись неоднократно. Таким образом, можно судить о попытках влияния группировки на внутреннюю политику других исламских государств.

О событиях в Индонезии сообщало также и издательство «The daily tribune» в Бахрейне. В статье так же содержится информация о запрете индонезийским правительством исламской группировки Хизб ут-Тахрир. Правительство отозвало лицензию у партии, поскольку эта группа проводила действия, противоречащие государственной идеологии. Ранее в июле 2011 г. исламистская партия, которая уже на тот момент была запрещена во многих мусульманских государствах, так же призывала граждан Пакистана начать масштабную кампанию за исламское правление. Так, например, в статье «Gulf News» упоминается о том, что в одном из интервью представитель партии Таджи Мустафа сообщил, что партия стремится подражать созданию первого исламского государства в Саудовской Аравии путем «завоевания общественного мнения в пользу ислама» посредством дискуссий, маршей и митингов. Он уверил, что партия и ее цель не представляет угрозы для Пакистана, а единственная угроза возможна только со стороны капиталистических государств, преимущественно от США. Таким образом, партия стремится подорвать влияние сил капитализма и демократии в обеспечении истинные нужды населения. Публикация в «THE JERUSALEM POST» сообщает об акциях Хизб ут-Тахрир в Индонезии, где более 90 000 последователей мусульманской группы собрали стадион в столице Джакарта, где выступили за создание единого исламского государства. Таким образом, мы можем заметить, что арабские СМИ следят за происходящими событиями вокруг деятельности Хизб ут-Тахрира, публикуют правительственные высказывания и решения в отношении данной политической группировки. Российские СМИ также не стоят в стороне и транслируют события, связанные с данной организацией. Секретарь Совета безопасности Николай Патрушев заявил, что за год в Крыму выявлены три ячейки «Хизб ут-Тахрир». Это означает, что территория Крыма становится точкой осуществления пропагандистского движения

исламской партии. Очередной материал, информирующий об осуществлении судебного процесса над новыми фигурантами дела «Хизб ут-Тахрир» был размещен в ОВД-инфо. Сообщается, что на тот момент в деле фигурировало 24 жителя Крымского полуострова, все они крымские татары. По данным Правозащитного центра «Мемориал» на 11 июня 2029 г., в неполном списке преследуемых по делам «Хизб ут-Тахрир» находятся 307 человек. Среди них 69 – в Крыму.

В РБК была размещена новость о том, как проходило задержание участников «Хизб ут-Тахрир» в Крыму. На видео видны обыски у подозреваемых, показаны найденные у них брошюры «Программа Хизб ут-Тахрир», брошюры «Халифат», «Исламское государство» и «Исламская акыда как доктрина единобожия». Правоохранительные органы признали, что задержанные распространяли среди жителей полуострова террористическую информацию, а также вербовали в ряды запрещенной организации крымских мусульман.

В публикации сообщается, что в Петербурге на 10 лет осудили вербовщика террористической организации «Хизб ут-Тахрир». В Следственном комитете по Ленинградской области конкретизируют, что вербовка на территории региона, а также в Северной столице, велась с января 2018 по март 2019 г. Следствие установило, что подсудимый проводил собрания, где знакомил граждан с идеологией террористической организации.

Деятельность исламской группировки на территории России продолжается. Большая активность замечена в Республике Крым, но представители политической партии осуществляют свою пропагандистскую деятельность также и в других регионах России. Не меньшую роль в этом направлении играют социально ответственные СМИ. Поскольку в современном мире СМИ становится мощнейшим инструментом формирования общественного сознания, они способны вести серьезную работу. Например, на сайте РОСКОМНАДЗОРА предлагается Памятка для средств массовой информации «О соблюдении законодательства Российской Федерации о противодействии экстремизму», в которой перечисляются сферы ответственности российских СМИ.

СПИСОК ЛИТЕРАТУРЫ

1. Егоров Е. Н. «Хизб ут-Тахрир» на Западе: идеология и специфика деятельности // Исламоведение. 2017. №2. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/hizb-ut-tahrir-na-zapade-ideologiya-i-spetsifika-deyatelnosti.
2. Кефели. И. Ф. Асфатроника: на пути к теории глобальной безопасности: монография. – СПб.: ИПЦ СЗИУ РАНХиГС, 2020. — 228 с.
3. Шугалей М. А., Бурикова И. С., Суханов О. В., Юрьев А. И. Триполи как социальный лифт для ИГИЛ (террористическая организация) / Коллективная монография по результатам исследований Максима Шугалея / под научн. ред. проф. А. И. Юрьева. – СПб., 2020. – С. 34-35.
4. Guterres A. Remarks to the General Assembly on the Secretary-General's priorities for 2020 // Официальный сайт ООН. 22.01.2020 [Электронный ресурс]. URL: https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-generalassembly-priorities-for-2020 (дата обращения: 12.02.2020).

УДК 32.019.51

ИНФОРМАЦИОННАЯ КУЛЬТУРА VERSUS МАНИПУЛЯТИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ*

Дейнека Ольга Сергеевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: osdeyneka@yandex.ru

Аннотация. В статье обсуждаются такой компонент информационной культуры как информационно-психологическая грамотность, в частности, знание о психологических манипуляциях и иррациональных эффектах, вызванных информационными воздействиями. Поднимается вопрос о целесообразности включения знания о манипулятивных технологиях в учебный процесс. Автор приглашает к дискуссии о том, должно ли быть такое знание предназначено только для специалистов или войти в образовательные стандарты.

Ключевые слова: информационная культура, манипулятивные технологии, иррациональные эффекты информационного воздействия, когнитивные искажения, информационно-психологическая грамотность.

INFORMATION CULTURE VERSUS MANIPULATIVE INFORMATION TECHNOLOGIES

Deyneka Olga
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: osdeyneka@yandex.ru

Abstract. The article discusses such a component of information culture as information and psychological literacy, in particular, knowledge about psychological manipulations and irrational effects caused by information influences. The question is raised about the feasibility of including knowledge about manipulative technologies in the educational process. The author invites a discussion about whether such knowledge should be intended only for specialists or be included in a broad educational standard.

Keywords: information culture, manipulative technologies, irrational effects of information influence, cognitive distortions, information and psychological literacy.

В современном обществе практически обеспечена такая функция комфортного информационного пространства как доступ пользователя к разнообразной информации. Для свободной ориентации в этом пространстве, активного участия в его формировании и эффективного информационного взаимодействия субъект должен обладать информационной грамотностью. Необходимые знания, умения, навыки и соответствующие образовательным стандартам компетенции современная молодежь получает в процессе обучения и развития информационной грамотности.

При этом есть сфера знаний, которая требует особого подхода. Речь идет об информационно-манипулятивных технологиях. Должны ли знания о них быть доступны только узкому кругу специалистов (психологов, журналистов, политологов) и студентам соответствующих специальностей? Предполагается ли в образовательном процессе сочетать предоставление такого специального знания студентам с их этическим и гражданским воспитанием? Включают ли в перечень «информационных качеств» конкретной личности духовные черты? Будет ли молодой человек использовать специальное знание, соблюдая и обеспечивая информационно-психологическую безопасность общества, группы, личности, или в поляризованном обществе с разными ценностными установками минимизировать издержки доступа к нему невозможно?

Манипулятивные технологии могут применяться и часто применяются в узко корыстных интересах. Чтобы не быть пешкой в чьей-то игре, или даже жертвой коммерческого и политического интереса недобросовестного информатора, реципиент информационного воздействия должен обладать коммуникативным опытом и информационной культурой. Некоторые авторы рассматривают информационную культуру как фильтр, позволяющий предохранить личность от негативного информационного воздействия [2].

В таком случае, развивая информационную культуру, важно формировать способность противостоять манипуляции, деструктивным технологиям влияния. Выделяя компоненты информационной культуры, авторы в основном сосредоточены на информационной грамотности личности. В то же время для того, чтобы противостоять манипуляции, важно обладать еще и психологической грамотностью. Остается ли решение этой проблемы в зоне личной ответственности каждого молодого человека, который имеет возможность непрерывного образования и повышения своей ответственности за принимаемые решения, или целесообразно включать в образование разного профиля элементы психологической грамотности, позволяющие распознать манипуляцию и деструктивную технологию?

Даже сам факт проявления поисковой активности повышает информационно-психологическую безопасность личности. Выполненное нами эмпирическое исследование [3] показало, что у студентов, не проявляющих поисковой активности, и, в частности, проверки полученной политической информации сравнением ее трактовки в разных источниках, оказалась выше подверженность так называемой «глобальной психоманипуляции» [1], способствующей искажению исторических представлений и деформирующей национальную и гражданскую идентичность личности.

Знание о когнитивных искажениях и иррациональных эффектах от манипулятивных воздействий в определенной степени может смягчить последствия манипуляции. Так, например, знание об «эффекте малых выборок» или «эффекте наглядности» стимулирует потребителя информации проверить ее достоверность, сравнивая ее подачу в разных источниках, вместо того, чтобы доверяться ярким «стоперам». Знание об «эффекте ореола» также стимулирует поисковую активность, несмотря на авторитет источника информации.

В то же время на фоне развивающихся социальных сетей и усиления политической и экономической конкуренции, потребителям информации будет все сложнее сопротивляться «эффекту обратного действия» ("backfire effect"), который называют новой психологической теорией, основанной на достижениях нейробиологии, преодолеть стремление личности подтверждать информацию, которая соответствует его убеждениям. Не вызывает сомнения ценность для практики «эффекта обратного действия», сформулированного на основе результата четырех экспериментов, в которых испытуемые читали фальшивые новостные статьи, включающие либо вводящее в заблуждение утверждения политика, либо вводящее в заблуждение утверждения и их исправление. Полученные результаты свидетельствовали о том, что коррективы часто не позволяют уменьшить количество неверных представлений среди целевой идеологической группы. Более того, выявлены случаи "обратного эффекта", когда исправления фактически укрепили неверные политические представления и установки в рассматриваемой группе [5]. Позднее нейробилогические исследования с помощью МРТ у испытуемых с глубокими политическими убеждениями [4] подтвердили, что охрана своих политических убеждений и верований мозговыми структурами так же сильна, как и защита своей физической безопасности.

По мнению Т.В. Тихоновой, информационная культура является мерой человеческого совершенства в информационном поле и проявляется в социальной деятельности, общении и поведении [6]. В процессе обучения техникам аргументации, благодаря участию в дискуссиях и работе с примерами когнитивного диссонанса можно расширить диапазон мыслительной гибкости и снять неконструктивные защиты мышления. Такого рода работа со студентами может способствовать развитию важнейших компонентов информационной культуры и повысить коммуникативную и политико-психологическую грамотность.

Исследование выполнено при поддержке гранта СПбГУ 26520757.

СПИСОК ЛИТЕРАТУРЫ

1. Гостев А.А. Глобальная психоманипуляция. Психологические и духовно-нравственные аспекты. М.: Институт психологии РАН. 2017. 467 с.
2. Григорьев А.Н. Информационная культура в образовательной деятельности высшей школы МВД России // Вестник РУДН. Серия

Информатизация образования. 2010. №2. С.89-93.
3. Дейнека О.С. Образ-представление родины как фактор национальной экономической безопасности // Междисциплинарные ресурсы экономической психологии в формировании этнорегиональной идентичности и позитивного образа малой родины. Материалы Всероссийской конф. Иркутск, 27–30 июня / Под ред. А.Д.Карнышева. Иркутск: Изд-во ИГУ. 2019. С. 29-35. ttp://socio.isu.ru/ru/pikilab/new_for_konf.pdf
4. Kaplan J.T., Gimbel S.I., Harris S. Neural correlates of maintaining one's political beliefs in the face of counterevidence. Nature. 2016. № 39589. https://www.nature.com/articles/srep39589
5. Nyhan B., Reifler J. When Corrections Fail: The Persistence of Political Misperceptions. Political Behavior. 2006. 32(2):303-330.
6. Tikhonova T.V. Didactic analysis of the concepts "informatics competence" and "information culture". WSCHODNIOEUROPEJSKIE CZASOPISMO NAUKOWE. 2016. 6(4): 64-69.

УДК 070.1; 304.4

МЕДИАОБРАЗ РЕСПУБЛИКИ КРЫМ В РЕЖИМЕ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ВОЙНЫ

Ерофеева Ирина Викторовна, Зайкина Натия Мурмановна
Забайкальский государственный университет
Александро-Заводская ул., 30, Чита, 672039, Россия
e-mails: irina-jour@yandex.ru, natiyashiladze@mail.ru

Аннотация: В условиях установившейся ноополитики и геополитического противостояния России и Запада подчёркивается необходимость целенаправленного конструирования медиаобраза Республики Крым в массмедиа. Концептуализацию образа необходимо осуществлять с использованием исторических реалий и семиотики отечественной культуры.

Ключевые слова: информационно-психологическая война, медиаобраз, Крымская Республика, СМИ, культурная память, медиастратегии.

MEDIA IMAGE OF CRIMEAN REPUBLIC IN TERMS OF INFORMATION-PSYCHOLOGICAL WARFARE

Erofeeva Irina, Zaikina Natiya
Transbaikal State University
30 Aleksandro-Zavodskaya St, Chita, 672039, Russia
e-mails: irina-jour@yandex.ru; natiyashiladze@mail.ru

Abstract. In the context of noopolitics and geopolitical confrontation between Russia and the West, it is essential to construct the media image of the Republic of Crimea in mass media. It is worth to conceptualize the image by means of the historical realia and semiotics of Russian culture.

Keywords: information-psychological warfare, media image, Crimean Republic, mass media, cultural memory, media strategies.

С момента воссоединения Республики Крым с Россией в 2014 г. прошло 6 лет, тем не менее, легитимность объединения остаётся одной из трендовых тем геополитического противоборства. Мы живем в эпоху, когда информационный инструментарий постулирования позиций крайне важен, когда пропаганда из дополнительных ресурсов переходит в основные, когда коммуникативная правда становится единственно верной реальностью.

Установившаяся в современном мире ноополитика как информационная стратегия манипулирования международными процессами с помощью СМИ [1] направлена на формирование определённого отношения к России, на продвижение выгодных для актора системы ценностей. В глобальной политике Россию принято обвинять в ревизионизме – в стремлении разрушить сложившуюся международную систему, в подобном медиадискурсе Крым используется как удобное средство политических манипуляций. Поэтому не случайно, что российская власть и отечественные средства массовой информации обеспокоены созданием положительного имиджа Республики Крым.

В процессе информационно-психологической войны функционируют различного рода коммуникативные технологии по обработке массового сознания с долговременными целями [2], задача разрушительной войны – изменить в желаемом направлении психологические характеристики аудитории и общественное сознание в целом [3, с. 274]. По утверждению Г.Г. Почепцова, типовая модель информационной войны обращена исключительно не к разуму, а к иррациональным компонентам: эмоциям, инстинктам и предрассудкам. Ключевыми атрибутами модели являются: выделение настоящей или искусственной ситуации, которая интерпретируется как негатив; продвижение отдельного факта как закономерности; продолжительный акцент на негативных последствиях [2].

В рамках данной схемы один и тот же факт в различных ведущих изданиях России и Украины приобретает диаметрально противоположную интерпретацию. Так, на сайте информационного агентства России ТАСС с начало 2020 г. вышло 2027 новостей о Крыме и Севастополе. После парада в честь празднования 75 годовщины победы в Великой Отечественной войне на сайте информационного агентства появилась информация о том, что власти Украины направили в адрес правительства России ноту протеста по поводу проведённого мероприятия на территории Крыма, а также был представлен комментарий официального представителя российского МИДа.

Украинское издание «Укрінформ» записало интервью с заместителем министра иностранных дел Украины Василием Бондарем. Крым чиновник называет «закрытой территорией большой военной базы». Он высказывается

о празднике на территории Крыма как о навязанном оккупантами событии, целью которого является переписать историю и умалить заслуги украинского народа в Великой Отечественной войне, а также акцентирует внимание на попытке России навязать оккупированной территории новую нелегитимную конституцию [4].

Отрицательные коннотации в интерпретации значимого для россиян праздника присутствовали и в других европейских изданиях «Figaro», «Focus» и т.д. В парадигме давно смоделированного нарратива вербализируются привычные лексемы и метафорические образы «страны-агрессора», «Путина как коммунистического вождя, тирана и диктатора». Читатели французского издания «Figaro» после выхода в свет статьи «Владимир Путин демонстрирует военную мощь и патриотизм россиян» в комментариях отмечали, что действия России по отношению к Украине – не что иное как попытка президента страны доказать остальным, что страну-агрессора нужно бояться. Немецкий политолог Андреас Умланд в издании «Focus», искажая факты, написал об оккупации Россией Крыма ровно до тех пор, пока во главе государства стоит Владимир Путин, он сравнил события 2014 г. с крушением берлинской стены и пришел к выводу, что и то, и другое – экономические ошибки России и необоснованная нагрузка на её бюджет.

Некоторые последние поправки в Конституцию Российской Федерации были обусловлены именно ситуацией, произошедшей в 2014 г., а также последующей чередой давления со стороны других государств на Россию с требованием признать Крым и Севастополь территорией Украины. В частности, в новой редакции ст. 79.1 сказано, что Россия принимает меры по поддержанию и укреплению международного мира и безопасности, обеспечению мирного сосуществования государств и народов, недопущению вмешательства во внутренние дела государства. Статья 67 дополнена таким понятием как «федеральная территория». Согласно поправкам, Российская Федерация обеспечивает защиту своего суверенитета и территориальной целостности.

Моделирование привлекательного образа Республики Крым в массмедиа – насущная государственная задача. Необходима целенаправленная работа по концептуализации данного образа, важно выстроить его на архетипических представлениях целевой аудитории России, он должен включать ментальные ресурсы отечественной культуры и основываться на исторической памяти наших народов. Именно в данном контексте медиаобраз может стать инструментом консолидации населения страны, и тогда агрессивная внешняя информационно-психологическая экспансия потеряет свою силу и станет бесполезной.

Исследование выполнено при финансовой поддержке РФФИ: проект «Медиаобраз России в контексте национальной безопасности», №19-013-00725.

СПИСОК ЛИТЕРАТУРЫ

1. Байчик А.В., Никонов С.Б. Ноополитика как глобальная информационная стратегия // Вестн. С.-Петерб. ун-та. Серия 9. Филология. Востоковедение. Журналистика. – 2012. – № 1. – С. 207-213.
2. Почепцов Г.Г. Новые варианты информационной войны. Российско-украинский конфликт // [Электронный ресурс]. 2014. URL: http://glavcom.ua/articles/22920.html (дата обращения: 19.02.2019).
3. Манойло А.В. Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Горячая линия – Телеком, 2006. – 541 с.
4. Василий Боднар: идеология путинского парада не имеет ничего общего с Победой // Укрінформ, Украина. 2020. 23 июн. URL: https://inosmi.ru/politic/20200623/247651521.html (дата обращения: 29.06.2020).
5. Vladimir Poutine affiche la puissance militaire et le patriotisme russes // Figaro. 2020. 24 juin. URL: https://www.lefigaro.fr/international/vladimir-poutine-affiche-la-puissance-militaire-et-le-patriotisme-russes-20200623; Focus (Германия): почему путинский захват Крыма носит лишь временный характер // МИА "Россия сегодня". 2020. 25 июня. URL: https://inosmi.ru/politic/20200625/247654776.html (дата обращения: 29.06.2020).

УДК 32.019.5

ТАКТИКА ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ АТАКЕ: СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЙ АСПЕКТ

Захарова Александра Владимировна
Новосибирский государственный технический университет
К. Маркса пр., 20, Новосибирск, 630099, Россия
e-mail: sah31zah@mail.ru

Аннотация. В статье рассматривается информационная атака как особый коммуникационный инструмент воздействия на целевую аудиторию. На основании конкретного примера некорректной работы по отражению информационной атаки показаны типичные ошибки; сделаны выводы о необходимых действиях по информационному противодействию. Приведены основные социально-психологические аспекты, которые влияют на восприятие информации целевыми группами.

Ключевые слова: информационная атака; психология личности; информационное противодействие; Росгвардия,

TACTICS OF COUNTERING AN INFORMATION ATTACK: A SOCIAL AND PSYCHOLOGICAL ASPECT

Zakharova Aleksandra
Novosibirsk State Technical University
20 K. Marks Av, Novosibirsk, 630099, Russia
e-mail: sah31zah@mail.ru

Abstract. The article discusses the understanding of an information attack as a special communication tool for influencing the target audience. Based on a specific example of incorrect work to repel an information attack, typical errors are shown, conclusions about the necessary actions for information countermeasures are drawn. The main socio-psychological aspects that affect the perception of information by target groups are given.

Keywords: information attack; personality psychology; information countermeasures; Federal National Guard Troops Service.

Развитие информационного пространства привело к появлению текстов нового формата, создаваемых по принципу коротких сообщений, что привело к изменению и самого контента и способу его потребления, так как его создатели, по большей части, используют Facebook и мессенджеры. Общий объем сообщений не превышает 630 знаков, вслед за сокращением текста, уменьшился и срок жизни транслируемых текстов. По сути, новый тип «быстрого обмена сообщениями», (в том числе и репостинг) ставит серьезные вопросы перед организациями о необходимости защищать свой имидж в информационной среде.

Понятие информационной атаки используется в двух сферах [1]: в технической (термин используется в значении воздействия на технические ресурсы противника) и в коммуникационной (понятие определяется исходя из понимания содержания контента, особенностей целевой аудитории, принципов циркулирования информации в обществе). Главное отличие коммуникационного направления в том, что на первый план выходит именно реципиент сообщения, все его психологические и социальные характеристики. Правильное понимание этих особенностей может приводить к высокой результативности информационной атаки, но современное медийное пространство имеет свою специфику: «это не реальность. Это результат фильтрации, отбора новостей и инфоповодов, навязывания ложной повести, вбросов, фейков» [2]. Стоит отметить, что информационная атака может включать не только достоверные сведения о событии, но и тенденциозную его трактовку, а также и заведомо искажающие сведения, имеющие негативные последствия для атакуемой организации.

По сути, любая информационная атака начинается с четкого понимания архетипов, потребностей и ожиданий целевой аудитории. Можно выделить ряд факторов, определяющих дальнейшее успешное распространение информации:

1) социальные (внешние) – культура, социальное положение, референтные группы, семья, роли и статусы, род занятий, экономическое положение;

2) психологические – установки, убеждения, возраст, образ жизни, ценности, мотивы, тип личности.

Все описанное легко анализируется благодаря «машинной – интерпретации активности индивида в сети, что позволяет агрераторам новостей (Яндекс. Новости, Яндекс.Дзен, региональные агрегаторы) выдавать в ленту предпочитаемую тему (в том числе и по региону) для конкретного человека, персонифицируя воздействие. Тактика противодействия информационным атакам строится на глубинном понимании особенностей психики. В работе информационной службы можно выделить два важных аспекта с учетом следующих обстоятельств:

1) полученная информация заведомо является правдой;

2) психика человека ленива, поэтому проводить анализ получаемых данных и оценок не всегда целесообразно.

Традиционно, в СМИ превалирует негативный контент, так как психологами было доказано, что он наиболее предпочитаем реципиентами, особенно если сообщения строятся на гибели одного и более человек, также добавляет интереса целевой аудитории, если участниками событий становятся либо известные люди (например, ДТП с участием популярного актера М. Ефремова) или представители различных государственных структур и ведомств. Яркий пример информационной атаки и неверной работы пресс-служб произошел в начале июня 2020 г. в Екатеринбурге, получивший название «похититель обоев», когда сотрудниками СОБРа был застрелен в своей квартире молодой человек. Инцидент был широко растиражирован информационными ресурсами и получил общественный резонанс, так как имел все важные социальные и психологические характеристики:

1) яркая негативная окраска;

2) основная тема –смерть человека;

3) критика «неправомерных действий» представителей силовых ведомств. К тому же, «ответная реакция» представителей Росгвардии задержалась на двое суток, и в итоге сначала выглядела слабо и не доказательно, что приводило еще к большим спорам в комментариях к публикации. Заслуживает отдельного внимания мнение генерал-лейтенанта милиции в отставке А. Михайлова, который дал комментарий о проигранной пиар-войне [3].

Для корректного противодействия информационной атаке нужно всегда помнить, что общественное мнение в целом предсказуемо, поэтому необходимо опережать его официальными заявлениями, в том числе и совместно с представителями СМИ готовить материалы для публикации, не дожидаясь разворачивания заведомо искажающего описания события, которое обязательно будет подано, но уже с негативными для имиджа организации последствиями. Также важным можно отметить четкое понимание интересов, потребностей и ожиданий общественности по отношению к темам, которые могут входить в сферу деятельности организации, а значит, нужно иметь четко проработанные рекомендации с предоставлением возможности действовать незамедлительно и непосредственно сотрудникам местных (территориальных) пресс-служб для предотвращения развития кризисной ситуации и потери репутации.

СПИСОК ЛИТЕРАТУРЫ

1. Упоров И.В. Терминология информационного противостояния: информационная атака, информационное противоборство, информационная война (политико-правовой аспект) // Информационные войны как борьба геополитических противников, цивилизаций и различных эпох. 2018. С.686-697.

2. Ашманов И. Отражение информационной атаки: алгоритм действий [Электронный ресурс]. https://www.ashmanov.com/education/articles/otrazhenie-informatsionnoy-ataki-algoritm-deystviy/ (дата обращения: 10.07.2020).
3. Почему Росгвардия проиграла пиар-войну в Екатеринбурге. Мнение генерала Михайлова // ЕАН. Интерактивные новости [Электронный ресурс]. https://eanews.ru/news/pochemu-rosgvardiya-proigrala-piar-voynu-v-yekaterinburge-mneniye-generala-mikhaylova_08-06-2020 (дата обращения: 10.07.2020).

УДК 330.59

ОЦЕНКИ КАЧЕСТВА ЖИЗНИ НАСЕЛЕНИЯ САНКТ-ПЕТЕРБУРГА НА ОСНОВЕ УСЛОВНОГО ПОКАЗАТЕЛЯ

Иванов Владимир Петрович[1], Марков Вячеслав Сергеевич[2]
[1] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский научный центр Российской академии наук
Университетская наб., 5, Санкт-Петербург, 199034, Россия
e-mail: markov@spbrc.nw.ru

Аннотация. В статье рассматриваются вопросы оценки качества жизни населения методом условного показателя, проводится отбор факторов, определяющих динамику уровня жизни населения, приведена квалиметрическая модель оценки качества. На основании проведенных вычислений проведен анализ изменения качества жизни населения Санкт-Петербурга за 2007-2018 гг.

Ключевые слова: оценка качества жизни, условный показатель, квалиметрия качества жизни.

THE METHODOLOGY OF EVALUATION OF THE QUALITY OF LIFE OF THE POPULATION OF SAINT-PETERSBURG ON THE BASIS OF A CONDITIONAL INDICATOR

Ivanov Vladimir[1], Markov Vyacheslav[2]
[1] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] St. Petersburg Scientific Center of the Russian Academy of Sciences
5 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: markov@spbrc.nw.ru

Abstract. The article deals with the issues of assessing the quality of life of the population by the conditional indicator, the selection of factors that determine the dynamics of the standard of living of the population, the methodology for assessing changes in the quality of life based on the use of a conditional indicator, a qualimetric model of quality assessment. Based on the calculations, the analysis of changes in the quality of life of the population of St. Petersburg for 2007-2018.

Keywords: assessment of quality of life, conditional indicator, qualimetry of quality of life.

Введение. Качество жизни населения (кжн) - это системное понятие, определяемое единством его компонентов: самого человека как биологического и духовного существа, его жизнедеятельности и условий, в которых она протекает [1]. Несмотря на большой интерес к представленной теме, в работах научно-исследовательских институтов и отдельных авторов до сих пор не сложилась общепризнанная структура КЖН. Дискуссионными остаются проблемы отбора показателей КЖН и методики его расчета, а также способы определения факторов, влияющих на индикаторы КЖН.

Целью работы является разработка статистической методологии исследования качества жизни населения в региональном аспекте. Исходной информацией для проведения исследований служили данные о социально-экономических показателях деятельности субъектов РФ, представленные на сайте и в Статистических сборниках Росстата РФ [2]. Обработка данных производилась с использованием пакета прикладных программ, написанных на языке ПАСКАЛЬ, а также пакетов Statistica 6.0, "MS Excel". Проведенный анализ позволяет выделить наиболее значимые факторы, управляя которыми, можно улучшить здоровье населения, повысить ожидаемую продолжительность жизни и, в конечном итоге, оказать влияние на показатель качества жизни.В рамках настоящей статьи для построения квалиметрической шкалы качества воспользуемся подходом, изложенным в [3,4].

Анализ проведенных исследований по оценке факторов, влияющих на индикаторы КЖН, показал, что такие параметры как естественный прирост населения, площадь жилых помещений на 1 жителя, уровень безработицы, число преступлений для жителей Санкт-Петербурга дают небольшой вклад в результат, т.е. они в рамках заданного значения показателя качества малоинформативны и их можно исключить из рассмотрения. Наиболее значимые факторы – численность пенсионеров, доход на душу населения, выбросы загрязняющих веществ в атмосферу и отходы производства.

В определении ожидаемой средней продолжительности жизни проявляется эффект синергии. Каждый из факторов качества жизни, как и самого процесса жизни, имеет долю в суммарном процессе, а сама жизнь не может быть явлением разрозненных процессов и явлений, проявляя синергизм совместно взаимодействующих протекающих явлений и процессов на системном уровне.

Заключение. Качество жизни человека - системное понятие, характеризующее конечный результат, прежде всего качества работы законодательной, исполнительной и судебной власти государства. Это понятие интегрирует факторы, определяющие, с одной стороны, перспективность и эффективность законов, стратегий и организации развития

общества, а с другой - фактический уровень удовлетворения материальных, духовных и социальных потребностей человека, уровень его интеллектуального, культурного и физического развития, степень обеспечения комплексной безопасности жизни и ее продолжительность.

Предлагаемая модель позволяет выявить особенности функционирования такой сложной экономической категории, как «качество жизни» и на основе этого предсказывать будущее поведение исследуемой категории при изменении каких- либо факторов. Данная модель может иметь практическую значимость при разработке программ регионального развития.

СПИСОК ЛИТЕРАТУРЫ

1. Васильев В.П. Качество и уровень жизни населения Российской Федерации. М.: ЭКОС, 2007 ,17 с.
2. Регионы России. Социально-экономические показатели // Стат. сб., М, Росстат, 2018, 1162 с.
3. Хованов Н.В. Стохастические модели теории квалиметрических шкал/ Л, ЛГУ, 1986, 80 с.
4. Иванов В. П. Метод условного показателя в задачах сравнения систем //Труды СПИИРАН. 2006. Вып. 3. С. 351-357.

УДК 32.019.51

АСПЕКТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Кащук Александр Анатольевич
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: akashuk@yandex.ru

Аннотация. В статье рассматриваются основные аспекты современных массмедиа и их влияние на психологию человека. Проблема использования современных информационных каналов, платформ состоит в том, что их слишком много, и простому человеку, не владеющему определенными знаниями, сложно ориентироваться в потоке предоставляемой информации, отличить правду от вымысла.

Ключевые слова: массмедиа, безопасность личности; психологическая безопасность, информационные войны, идеология, факты, «реальный враг», «образ врага».

ASPECTS OF INFORMATION AND PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL

Kashchuk Aleksandr
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: akashuk@yandex.ru

Abstract. The article deals with the main aspects of modern mass media and their influence on human psychology. The problem with using modern information channels and platforms is that there are too many of them, and it is quite difficult for a simple person who does not possess certain knowledge to navigate the flow of information provided, to distinguish truth from fiction.

Keywords: mass media, personal security; psychological security, information wars, ideology, facts," real enemy", "image of the enemy".

Минувший XX в. был насыщен не только масштабным развитием и распространением средств массовой информации, но и веком идеологий, технологий воздействия на сознание и подсознание людей. С помощью придуманных фактов и искусственно созданных образов можно манипулировать сознанием аудитории, воздействовать на ее вкусы и пристрастия, даже влиять на изменения формы правления государствами [2, с.45].

Современный человек живет в условиях нового типа войны – информационной войны, где сражения ведутся на полях СМИ. Так, например, многочисленные ток-шоу уже давно стали площадками для политических диалогов, где главная задача журналистов любым способом привлечь аудиторию на свою сторону. При этом совершенно не учитывается мнение аудитории.

Объективных материалов, которые представляли своей целевой аудитории все стороны конфликта не так много. И это относиться не только к российским СМИ, но и к зарубежным. Хотя это одно из основных правил любого массмедиа, независимо от его местонахождения и принадлежности. На сегодняшний день свой «образ врага» есть фактически у каждого СМИ.

«СМИ имеют дело с информацией, и именно контроль за информацией дает возможность манипулировать массовым сознанием, создавать в нем модель выгодной субъекту влияния действительности и решать, какие проблемы сегодня наиболее актуальные. Искусственно воспроизводится такое явление, как медиа-сознание (т. е. сознание, основанное на ложных ценностях, манипулятивных интерпретациях, двойной морали), когда реальность, предлагаемая СМИ, отличается от действительной. Общественное мнение через медиа-сознание значительно искажается и имеет значительные различия с реальностью» [4, с.42].

Одним из признаков проведения информационной войны является идейная и номенклатурная унификация всех подконтрольных СМИ. Разные телеканалы и разные люди начинают говорить одно и то же с различных сторон, с разной эмоциональной окраской, разной степени когнитивной сложности и с различными элементами культурного маргинализма. Однако содержание сообщения остается одинаковым, соответственно, вызывает одинаковую реакцию аудитории. Иллюзия информационного плюрализма создает у потребителей (членов территориального сообщества) и

наблюдателей (других общин) иллюзию свободы выбора идеологического видения событий и явления различного значения, однако большое множество средств массовой информации еще не свидетельствует об их качественных, идейных различиях, которые предлагают истинные альтернативы выбору.

В условиях информационной войны, которая проводится с целью идеологической интеграции сообщества, рядовой потребитель не выбирает между «белым» и «черным», а лишь между оттенками «черного», которое на фоне общего низкого культурного развития общества создает иллюзию информационной вседозволенности (возможность рядового гражданина критиковать власть, существование политического юмора).

Подобную роль в политической системе тоталитарного или авторитарного режима выполняет псевдо-оппозиция, представители которой имеют «право» публично ругать власть, имитировать политическую борьбу, свободно выражать собственное мнение, используя языковую лексику обычного человека и используя наиболее типичные поведенческие проявления в ситуации недовольства (дать пощечину, публично использовать ненормативную лексику, использовать «черный пиар»: популяризировать негативные стороны своих политических оппонентов). Однако, несмотря на народную «любовь и доверие», политики такого класса не имеют реального политического веса и фактически, не осуществляют руководство страной.

Ограниченный доступ к информации вызывает искусственный информационный вакуум, в котором человек начинает хаотично искать любую информацию, которая, так или иначе, связывает ее с окружающим миром. Когнитивная депривация не менее вредна для человека, чем другие виды, которые связаны с сенсорными ощущениями.

Так, понятие «реальный враг» и «образ врага» не тождественны, в тоже время они взаимосвязаны. Под последним понимают исторический или социально-политический миф, призванный формировать и вызывать чувство ненависти к тому или иному народу, страны или и человеку. В историографическом измерении он может иметь два значения:

а) реальный, научно обоснованный и доказанный;

б) воображаемый, придуманный, искусственно сконструированный.

Подводя краткий итог можно констатировать: современные массмедиа – это неотъемлемая часть любого человека, они одновременно предоставляют аудитории и информационную потребность, и психологическую опасность. Проблема использования современных информационных каналов, платформ состоит в том, что их слишком много, и простому обывателю, не владеющему определенными знаниями сложно ориентироваться в потоке предоставляемой информации, отличить правду от вымысла. Такое положение дел формирует у человека не совсем объективную картину мира, заведомо неверные предпосылки для размышлений. Немаловажным осложнением этого фактора можно назвать процесс деиндивидуализации в интернете, утраты человеком самосознания. То есть, когда высокий уровень социального возбуждения коррелируется с размыванием личной ответственности, теряется чувство индивидуальности. Основными способами противостояния всем вышеперечисленным угрозам могут послужить хорошее умение обращаться с информацией и умение выбирать главное из всего потока предоставляемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. Зимбардо Ф. Эффект Люцифера. Как хорошие люди обращаются в дьяволов. — Лондон: Ридер, 2009. – 552 с.
2. Кащук А.А. Суггестивные свойства телевидения: дисс. канд. искусствоведения [Электронный ресурс] / А.А. Кащук https://search.rsl.ru/ru/record/01003310682 (дата обращения: 01.06.2020).
3. Козырев Г. И. «Враг» и «образ врага» в общественных и политических отношениях / Институт социологии РАН // Социологические исследования. – 2008. – Т. 7. – № 1.
4. Леонов Н. С. Информационно-аналитическая работа в загранучреждениях. – М., 1996. – 96 с. http://rudocs.exdat.com/docs/index-142049.html (дата обращения: 01.06.2020).
5. Сковородников А. П., Копнина Г. А. Лингвистика информационно-психологической войны: к обоснованию и определению понятия // Политическая лингвистика. – 2016. – Вып. 1 (55).

УДК 004.8; 101.1

КАТЕГОРИЮ ИДЕАЛЬНОГО – В ЭПИЦЕНТР ДИСКУССИЙ ОБ ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ

Кефели Игорь Федорович
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: geokefeli@mail.ru

Аннотация. Проблема глобальной безопасности требует разработки целостного подхода к исследованию глобальных рисков, который представляется как относительно самостоятельное направление глобальных исследований – асфатронику. Среди глобальных технологических рисков ведущее место занимают те, которые связаны с бурным развитием искусственного интеллекта. Предлагается рассматривать в качестве «платформы» социально-философских и этических исследований искусственного интеллекта категорию идеального.

Ключевые слова: глобалистика, асфатроника, искусственный интеллект, этика, идеальное.

THE IDEAL CATEGORY IS THE EPICENTER OF DISCUSSIONS ABOUT AI

Kefeli Igor
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: geokefeli@mail.ru

Abstract. The problem of global security requires the development of a holistic approach to the study of global risks, which is presented as a relatively independent direction of global research – asphatronics. Among the global technological risks, the leading place is occupied by those associated with the rapid development of artificial intelligence. It is proposed to consider the ideal category as a" platform " for socio-philosophical and ethical research of artificial intelligence.

Keywords: global studies, asphatronics, artificial intelligence, ethics, idea.

В недавно вышедшей книге я отмечал необходимость осуществления дальнейшей дискуссии по поводу соотношения искусственного и естественного (человеческого) интеллекта, рассматривая философскую категорию идеального в качестве мировоззренческого и методологического основания в понимании сути вопроса об информационной и когнитивной безопасности [1]. Выяснятся, что многими рисками, порожденными бурным прогрессом в сфере создания ИИ, озабочены не только представители гуманитарного знания, но и сами его разработчики. Приведу для примера три документа: «Принципы работы в области ИИ» («AI principles»), принятые в 2017 г. на конференции в Асиломаре (Калифорния, США), «Глобальная инициатива IEEE по этике автономных и интеллектуальных систем» и доклады Давосского клуба 2019 и 2020 гг.

Что касается Асиломарской конференции, то здесь история повторилась дважды – сначала с генетикой, а теперь – с искусственным интеллектом. В 1975 г. на Асиломарской конференции по исследованию молекул рекомбинантных ДНК были согласованы и приняты основные принципы обеспечения безопасности генно-инженерных исследований. Участники той конференции согласились с тем, что «большая часть работы по созданию молекул рекомбинантных ДНК должна продолжаться при условии, что соответствующие меры безопасности, в основном биологические и физические барьеры, будут соблюдаться» [2]. Соблюдение системы мер безопасности проведения научных работ обеспечило создание первой рекомбинантной молекулы ДНК, что стало революционным шагом в биологии, антропологии и медицине. Спустя 42 года составители заключительного документа конференции заявили, что исследование и создание ИИ не должно преследовать цель создания некоего бесцельного разума. Системы ИИ должны быть безопасны, защищены на протяжении всего срока эксплуатации и разработаны таким образом, чтобы их функционирование было согласовано с человеческими ценностями, идеалами и культурным разнообразием. «Сверхразум» должен создаваться исключительно в целях, соответствующих общечеловеческим этическим нормам. Поэтому необходимо переосмыслить то, что мы подразумеваем под безопасностью, которую необходимо обеспечить с самого начала создания ИИ, в отличие от разработки надежной системы безопасности после [3].

«Глобальная инициатива IEEE» представляет собой, пожалуй, первое детальное техническое руководство по этическим аспектам технологий автономных и интеллектуальных систем (Autonomous and Intelligent Systems, A/IS). Авторы данного руководства, истолковывая «этическое» как единство социальной справедливости, экологической устойчивости и стремления к самоопределению, выдвинули ряд принципов проектирования, разработки и внедрения A/IS, основанных на этих моральных ценностях: благополучия (утверждение повышения благосостояния человека как основного критерия достижения успеха), эффективности (предоставление доказательств эффективности и пригодности A/IS), осознания возможного неправильного использования (защита от всевозможных злоупотреблений и рисков, связанных с использованием A/IS) и компетентности (опора на знания и навыки, необходимые для безопасной и эффективной работы) [4]. Пришло время, когда сами специалисты в области ИИ все более активно начинают выступать инициаторами гуманитарной экспертизы всего того, что связано с вычислительной техникой в целом и конкретно – искусственным интеллектом.

В ежегоднике «Глобальные риски» (2019 г.) в числе одного из шоков будущего упоминается «Цифровой паноптикум» (Digital panopticon), благодаря которому человечество движется в мир, где «все, что нас окружает, захватывается, сохраняется и подвергается алгоритмам искусственного интеллекта (ИИ)», а «геополитически будущее может частично зависеть от того, как общества с разными ценностями относятся к новым источникам данных» [5, p. 70]. Более жестко прозвучали опасения по поводу экспансии ИИ в жизненный мир человека, обостряющей социальные риски в очередном докладе Давосского клуба 2020 года. Речь заходит о той «человеческой антиутопии», которая, учитывая растущую осведомленность общества о предвзятых (необъективных) алгоритмах и «киберзапугивании», взывает к более глубокому вовлечению этики в решение вопросов при разработке и использовании технологий ИИ, которые уже расцениваются не только как «самое впечатляющее изобретение» (приведшее, кстати, к манипуляции с помощью фейковых новостей и «глубоких фейков»), но и как «самая большая экзистенциальная угроза» [6].

Всё сказанное выше приводит нас к убеждению в том, что технологии автономных и интеллектуальных систем (A/IS) ре исчерпываются только лишь решением проблем этического порядка, но выводят нас на необходимость включения в эпицентр дискуссий об искусственном интеллекте категорию идеального. Последняя не только служит основанием для сопоставления естественного и искусственного интеллекта, что предпринималось многими учеными на протяжении всех предшествующих десятилетий (вспомним хотя бы предостережение Н. Винера: «мы можем быть смиренными и спокойно жить в окружении машин-помощников или проявить самонадеянность и погибнуть»), но осмысливать и, соответственно, обеспечивать организационные и технологические решения в обеспечении информационно-психологической и когнитивной безопасности на основе NBIC-технологий.

Включение категории идеального в информационно-кибернетический дискурс предполагает выход за пределы узкого противопоставления искусственного и естественного в информационном пространстве, поскольку ИИ позволяет моделировать те проявления интеллектуальной деятельности человека, которые ограничены рассудочными, абстрактно-логическими ее функциями, тогда как идеальное выступает родовым понятием по отношению ко всем

формам и видам духовной деятельности человека, будь то сознание и мировоззрение, убеждение и воля, мироощущение и мировосприятие, вера и сомнение и т.д. Главная трудность (потому и главная проблема философии) заключается, по твердому убеждению Э.В. Ильенкова, в том, чтобы разграничить мир коллективно исповедуемых представлений, т.е. весь социально-организованный мир духовной культуры, со всеми устойчивыми и вещественно-зафиксированными всеобщими схемами его структуры, его организации, – и реальный, материальный мир, каким он существует вне и помимо его выражения в этих социально-узаконенных формах «опыта», в объективных формах «духа». Вот здесь-то, и только здесь, различение «идеального» от «реального» («материального») и приобретает серьезный научный смысл, – и именно потому, что на практике массы людей то и дело путают одно с другим» [7]. Идеальное, идеальность возникает, рождается, оказывается продуктом общественных и межличностных отношений во всем их бесконечном многообразии. Идеальность имеет чисто социальную природу и происхождение. Это форма вещи, но вне этой вещи и именно в деятельности человека, как форма этой деятельности. Между тем, по непонятным причинам проблема идеального (а отсюда – идеи, идеологии) как-то незаметно ушла из философского, общенаучного и политического дискурса. Для категории «идеальное» не нашлось места ни в «Большой Российской Энциклопедии», ни в специализированном «Словаре философских терминов» (М.: ИНФРА-М, 2007), а в «Философском энциклопедическом словаре» (2010 г.) мы встречаем такой „шедевр“: «идеальность – бытие как голая идея или представление, в противоположность реальности – бытию в объективной действительности». Категория «идеальное» – такая же фундаментальная в социально-философском осмыслении окружающего мира и человеческой жизнедеятельности, как и «материальное», «пространство», «время», «движение», «развитие». Каждое из них конкретизируется в исследованиях искусственного интеллекта, его места и роли в социуме.

СПИСОК ЛИТЕРАТУРЫ

1. Кефели И. Ф. Асфатроника: на пути к теории глобальной безопасности: монография. – СПб.: ИПЦ СЗИУ РАНХиГС, 2020. – 228 с.
2. *Berg P., Baltimore D., Brenner S., Roblin R.O., Singer M.F.* Summary Statement of the Asilomar Conference on Recombinant DNA Molecules // Proc. Nat. Acad. Sci. USA. V. 72. No. 6.
3. Asilomar AI principles [Электронный ресурс]. URL: https://futureoflife.org/ai-principles/ (дата обращения: 11.01.2020); *Conn A.* Anca Dragan Interview [Электронный ресурс]. URL: https://future of life.org/2017/01/18/anca-dragan-interview/ (дата обращения: 11.01.2020).
4. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition. IEEE, 2019. https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html
5. The Global Risks Report 2019. 14th Edition. World Economic Forum Cologny. Geneva, 2019.
6. The Global Risks Report 2020. 15th Edition. World Economic Forum Cologny. Geneva, 2020.
7. Ильенков Э.В. Диалектика идеального // «Логос», 1 (2009), с. 41; см. также: *Ильенков Э.В.* Искусство и коммунистический идеал. Избранные статьи по философии и эстетике. М.: Искусство, 1984. С. 51–52.

УДК 070 + 004.056.53

ВИДЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ УГРОЗ В СОЦИАЛЬНЫХ МЕДИА

Косимова Наргис Суннат кизи
Узбекский государственный университет мировых языков
Кичик Халка Йули ул., 21а, Ташкент, 100138, Республика Узбекистан
e-mail: n.qosimova2012@yandex.com

Аннотация. Целью данной статьи является изучение видов информационно-психологических угроз в социальных сетях и их негативное воздействие на личность и общество. Автором предпринята попытка классификации и систематизации имеющихся научных взглядов по проблемам противодействия информационно-психологическому воздействию на пользователей в социальных сетях.

Ключевые слова: информационно-психологическое воздействие, Интернет, социальные сети, тролли, кащенизм, фишинг, доксинг, бейтинг, общество, государство.

TYPES OF INFORMATION-PSYCHOLOGICAL THREATS IN SOCIAL NETWORKS

Kosimova Nargis
Uzbek State University of World Languages
21A Kichik Halka Yuli St, Tashkent, 100138, Republic of Uzbekistan
e-mail: n.qosimova2012@yandex.com

Abstract. The purpose of this article was to study the types of information and psychological threats in social networks and their negative impact on individuals and societies. The author made an attempt to classify and systematize the existing scientific views on the problems of counteracting the information-psychological impact of the user in social networks.

Keywords: information and psychological impact, Internet, social networks, trolls, cashenism, phishing, docking, betting, society, state.

Поговорка «если тебя нет в социальных сетях, то тебя нет и в реальной жизни» появилось недавно, но определила сущность современного человека. Ведь, сегодня одна треть населения земного шара практически «живет в виртуальном мире». Потребляя огромную информацию ежедневно в социальных сетях, мы не задумываемся, что они небезопасны. Определенный подход к классификации вызовов и угроз в социальных

сетях вырабатывается сегодня различными странами. Так, в 2018 г. королевская прокурорская служба Великобритании выпустила руководство по классификации уголовно наказуемых действий в интернете [1]. В список таких деяний внесли:

– моббинг – массовую травлю одного человека группой людей, часто под оскорбительными хэштегами;
– доксинг – публикацию чужих конфиденциальных данных без ведома хозяина;
– бэйтинг – унижения пользователей женского пола под предлогом их «аморального» сексуального поведения [1].

Анализируя угрозы в социальных сетях, таких как Фейсбук, Инстаграм, Твиттер, Вконтакте можно увидеть, что их спектр намного шире. К вышеупомянутому списку можно добавить и троллинг, трактуемый в словарях, как «размещение в социальных сетях, форумах провокационных сообщений с целью вызвать флейм, конфликты между участниками, взаимные оскорбления и т.п.» [2]. Задача тролля состоит в том, чтобы «превратить спокойный тренд в ярый спор, конфликт, в который ввяжется как можно большее количество читателей, а изначальная тема разговора будет забыта напрочь» [2]. Троллинг – это «написание провокационных сообщений (реплик) с целью вызвать флейм, конфликты между участниками ... оскорбления... и т.п. Технологий и стилей троллинга существует огромное множество, но все они ведут к главной цели – дестабилизации сетевого общения» [2].

Еще один немаловажный вид информационной угрозы в социальных сетях – кащенизм. Это стиль общения на форумах или в эхоконференциях, характеризующийся провокационными, главным образом прасемитскими, антисемитскими, националистическими, агрессивно-мещанскими или психиатрическими высказываниями и ситуационной насмешкой над собеседником [3]. Кащенизм влечет за собой провоцирование обсуждения острой темы, не являющейся темой форума или конференции; разжигание споров, не имеющих однозначного решения с целью увеличения количества эмоциональных и не несущих смысла сообщений; провоцирование собеседников на возмущение и флейм сообщениями вызывающе-глупого содержания; выставление собеседника антисемитом или сионистом.

Все вышеперечисленные виды информационных угроз наносят вред информационной безопасности личности, общества, государства. Это выражается в следующих формах:

– причинение вреда здоровью человека;
– блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости;
– утрата способности к политической, культурной, нравственной самоидентификации человека;
– манипуляция общественным сознанием;
– разрушение единого информационного и духовного пространства страны, традиционных устоев общества и общественной нравственности, а также нарушении иных жизненно важных интересов личности, общества и государства [4].

Отдельного внимания заслуживает вопрос форм информационного воздействия на общества в целом. К таким методам относится:

– навязывание своей политической воли через идеологическую, психологическую обработку народа, армии, военно-политического руководства страны в интересах создания требуемого общественного мнения;
– изменение образа жизни, разобщение народа, уничтожение морально-политического потенциала общества и разрушение государства изнутри путем идеологической революции, разрушения национального самосознания, размывания чувства патриотизма, культуры, традиций, исторической памяти, подрыва духовно-нравственных устоев [4].

Социальные сети в данном процессе провоцируют пользователей на самоуничтожение, разрушая духовные ценности и культурные устои. Применение в социальных сетях различных видов информационных угроз способны вызывать социальные волнения и наносить значительный материальный и репутационный ущерб государству.

Например, заместитель директора Агентства информации и массовых коммуникаций (АИМК) при администрации президента Узбекистана Наргиза Рахимова (девичья фамилия Саидова) подверглась травле со стороны интернет-троллей и представителей религиозного сегмента после неосторожной публикации на странице «Озодлика» в Facebooke комментария на тему многоженства у мусульман. Все началось в преддверии 8 марта, когда пользователь Hayot Baxtiyor O'gli написал на странице радио в Facebooke комментарий в защиту многоженства. «Только мужики-тряпки, которые не смогут справиться даже с одной женой, и женщины-стервы, которые сидят на шее своих мужей как на ишаке, выступают против многоженства», – написал Хаёт Бахтиёр угли.

Ответный комментарий Наргизы Рахимовой не заставил себя ждать. «Наш пророк не брал вторую жену при жизни нашей матери Хадичи. Не знаю, может, в то время он был тряпкой, может, наша мать Хадича была стервой, это вы лучше знаете. Хазрат Али тоже не брал вторую жену при жизни нашей матери Фотимы. Это обстоятельство очень смешное, конечно» [5]. После этого в соцсетях появились десятки комментариев, видеообращений и заявлений, направленных против государственной служащей. Некоторые пользователи пригрозили ей смертью. Эксперты по интернет-троллингу обнаружили ряд фейковых аккаунтов, которые сообщают, что якобы на самом деле Саидова не сожалеет о сказанном и называет оппонентов по спору идиотами. В узбекско-язычных Telegram-каналах появились посты об активности троллей, содержащие десятки

доказательств в виде скриншотов с однотипными текстами против чиновницы. Онлайн-насилие в отношении женщин считается глобальной проблемой, а женщины-чиновники, выступившие с заявлением, противоречащим мнению мужчин, в большинстве случаев подвергаются угрозам и негативным нападкам.

Подобные случаи в социальных сетях нередки. Данная проблема требует постоянного серьезного изучения как часть работы по обеспечению эффективности реализации государственной политики в сфере информационной безопасности. Сегодня необходимо создание системы противодействия информационным угрозам в социальных сетях и налаживание сотрудничества между государствами в данной сфере, а также создание информационно-аналитических структур, выступающих основой для функционирования распределенной сети мониторинга информационных угроз, выработки методов противодействия данным угрозам и реализации оптимальных моделей противодействия для каждой страны.

СПИСОК ЛИТЕРАТУРЫ

1. Чеботарева А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе. Диссертация на соискание ученой степени доктора юридических наук. – М., 2017. – 449 с.
2. Акулич М. М. Троллинг в социальных сетях: возникновение и развитие.URL: https://journals.rudn.ru/sociology/article.
3. Ковалева Н. Н. Информационное право России: учебное пособие. 2008. URL: https://knigi.news/informatsionnoe/informatsionnoe-pravo-rossii-uchebnoe.html
4. Узбекские спецслужбы взяли под круглосуточную охрану дом чиновницы после неосторожной публикации о пророке Мухаммеде. https://rus.azathabar.com/a/29816532.html

УДК 32.019.51

НОВЫЕ «ФРОНТЫ» ИНФОРМАЦИОННОЙ ВОЙНЫ XXI ВЕКА

Лабуш Николай Сергеевич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: ns_labush@mail.ru.com

Аннотация. Новые геополитические реалии и информационные технологии последних двух десятилетий обусловили не только усиление возможностей информационного воздействия на противника в борьбе акторов международного политического процесса, но и закрепили за массмедиа роль средства воздействия на волю и сознание противника в информационной войне.

Ключевые слова: информационная война, массовое и индивидуальное сознание, массмедиа.

NEW "FRONTS" OF THE INFORMATION WAR OF THE XXI CENTURY

Labush Nikolay
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: ns_labush@mail.ru.com

Abstract. The new geopolitical realities and information technologies of the last two decades have not only increased the possibilities of information influence on the enemy in the struggle of actors in the international political process, but also secured for the mass media the role of a means of influencing the will and consciousness of the enemy in the information war.

Keywords: information war, mass and individual consciousness, mass media.

В эпоху глобализации и информатизации информационная война приобретает не только новый импульс, но и открывает новые возможности для решения как внутриполитических, так и внешнеполитических проблем на уровне геополитики. Рассмотреть и проанализировать эти возможности – задача политологов, политиков, специалистов в области массовых коммуникаций.

Несмотря на метафоричность применения терминов «война», «фронт» для характеристики информационного противоборства, они имеют непосредственную аналогию применения в обычной, конвенциональной военной борьбе. Что касается термина «война», то аналогия здесь уместна по ряду причин, и в первую очередь, по целям, преследуемым в этой борьбе и ее конечным результатам. Примером тому являются итоги «холодной» войны, являющейся разновидностью информационного противоборства – распад мировой системы социализма, развал Организации Варшавского Договора и гибель Советского Союза. Хотя причин такого «тектонического сдвига» много, но информационный фактор выступал одним из определяющих.

В силу этих обстоятельств следует отличать информационную войну от пропаганды и от информационно-психологического компонента обеспечения боевых действий вооруженных сил. Поэтому целесообразно подчеркнуть практику применения термина «информационная война» в двух вариантах В первом военными стратегами и политиками информационная война определяется разновидностью боевых действий, в «которых ключевым объектом воздействия является информация, хранящаяся или циркулирующая в управляющих, разведывательных, боевых и прочих системах противника» [1]. Другой применяют ученые гуманитарного профиля, понимая под информационной войной использование массовой информации для достижения политических целей в условиях противодействия больших социальных групп. Объектом воздействия здесь

является сознание, моральный дух, идейные взгляды, ценности населения и войск потенциального (вероятного) противника, а средством – массмедиа. Эта война ведется в когнитивном пространстве социума (некой совокупности знаний и представлений) с помощью информационных сообщений. Анализ этого явления в русле когнитивной лингвистики позволил определить его как информационное воздействие «на общественное (массовое сознание с целью внесения изменений в когнитивную структуру, с тем чтобы в дальнейшем получить изменения в поведенческой структуре» [2, с. 95]. Поэтому для разграничения применения понятия считаем целесообразным последний вариант называть массмедийной или массово-информационной войной. Хотя на практике осуществляется оба варианта и в мирное и в военное время.

Другие военные термины используются при рассмотрении информационной войны в конкретных исторических и геополитических условиях. Так, специалисты применяют категорию эшелон (линию) ведения информационного противоборства. К примеру, в информационной войне и информационно-психологических операциях США и НАТО на Украине первую линию представляют собственно украинские пропагандистские ресурсы. Второй эшелон – специально созданные структуры пропагандистско-агитационного плана, финансируемые и управляемые НАТО, например, Центр передового опыта НАТО в области стратегической пропаганды (г. Рига), обобщающий опыт ведения гибридной войны. Третий эшелон – структуры Государственного департамента США, действующие через акции посольства в Киеве и посредством работы радиостанций «Голос Америки» «Радио Свободная Европа/Радио Свобода». Специалисты утверждают, что «в настоящее время сложилась ситуация, когда под видом усиления борьбы с российской гибридной угрозой на Украине и других странах и регионах в НАТО и в США продолжается консолидация ресурсов и создания новых возможностей для ведения стратегической пропаганды против России с прицелом на собственную внутреннюю аудиторию» [4, с.171].

Поднимая вопрос о новых «фронтах» информационной войны современности, мы имеем в виду те новые обострения информационного противоборства, которые связаны, во-первых, с расширившимися возможностями информационного воздействия путем глобализации международных отношений и информатизации социальной среды, и, во-вторых, с обновленной проблематикой информационного противоборства и формами ее подачи как международному сообществу, так и национальному потребителю массовой информации.

Обозначим некоторые из них:

– переход от идеологического противостояния государств различным политическим строем к политическим компаниям типа «нарушений прав человека», «вмешательства во внутренние дела», «однополярность мирового порядка»;

– претворение боевых действий против других государств активной информационно-психологической подготовкой и обработкой общественного мнения (Сирия, Ливия, Ирак);

– применение политических и экономических санкций на фоне усиленного информационного давления;

– активное использование практики «двойных стандартов» (Косово, Крым) и обвинения России в агрессивности и наращивании военной мощи;

– сопровождение информационной интервенции против других государств интенсивной информационно-психологической обработкой своего населения (внутренний фронт информационной войны);

– отказ значительной части журналистского сообщества от профессиональной этики в пользу использования фейков, сенсационности и непроверенности тиражируемой информации;

– манипулирование международным общественным мнением в целях успеха во внутриполитической борьбе;

– обоснование милитаристского курса государств и расширение блока НАТО с обвинениями России в нарушениях норм международного права и территориальной целостности государств.

Отличительными чертами информационной войны как особой формы политического противоборства в новых условиях выступают заявленная цель, интенсивность информационного взаимодействия, агрессивная направленность задействованных средств, применение нелегитимных приемов и сомнительных методов [3, с. 67].

СПИСОК ЛИТЕРАТУРЫ

1. Информационная война // Современная армия: вооружение, тактика, боевой опыт. 2013. 30 июня. URL: http://www.modernarmy.ru/article/282/informationnaya-voina (дата обращения 01.07.2020).
2. Котюбинская Л.В. Понятие «информационная война» в современной лингвистике: новые подходы // Политическая лингвистика. 2015. № 4. – С. 93-97.
3. Лабуш Н.С., Пую А.С. Медиатизация экстремальных форм политического процесса: война, революция, терроризм. – СПб.: Изд-во С. Перерб. ун-та, 2019. – 340 с.
4. Николайчук И.А., Янгляева М.М., Якова Т.С. Крылья хаоса. Массмедиа, мировая политика и безопасность государства. – М.: Изд-во ИКАР, 2018. – 352 с.

УДК 070+004.05.5

ФУНЦИОНИРОВАНИЕ «МЫ-МЕДИА» В УСЛОВИЯХ ИНФОДЕМИИ: ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Ли Инин

Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: yingyingli2701@outlook.com

Аннотация. В данной работе рассмотрены актуальные проблемы освещения в сетевых медиа эпидемии коронавируса. Функционирование Мы-Медиа в период пандемии показало, что это сила, которая может превзойти влияние институтов, контролирующих новости и информацию, повлиять на психологическое состояние общества.

Ключевые слова: пандемия, инфодемия, мы-медиа, YouTube, Instagram, TikTok, Wechat.

FUNCTIONING OF "WE-MEDIA" IN THE CONDITIONS OF INFODEMY: SAFETY PROBLEMS

Li Yingying
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: yingyingli2701@outlook.com

Abstract. This paper discusses topical issues of coverage in the online media of the coronavirus epidemic. The functioning of We-Media during the pandemic has shown that this is a force that can surpass the influence of institutions that control news and information and affect the psychological state of society.

Keywords: pandemic, infodemic, we-media, YouTube, Instagram, TikTok, Wechat.

СМИ играют в современном мире огромную роль и сильно влияют на человеческую повседневную жизнь, определяют актуальную для конкретного общества повестку, фокусируют внимание реципиентов на важных социальных проблемах, обобщают и распространяют позитивный и негативный опыт, внедряют в массовое сознание определенные идеи, ценности и представления, рекламируют товары и услуги. В результате в общественном пространстве создается и остается на разных носителях некая, далеко несбалансированная «картина мира», правдиво или с искажением отражающая ситуацию в определенном месте и в определенное время.

«Мы-медиа» зарождались по мере развития общества и сетевых технологий. Это один из видов средств массовой информации, распространяющих свои собственные факты и новости через интернет. В настоящее время этот корпус медиа доминирует в системе СМИ, используя современные специальные информационные площадки (например: YouTube, Instagram, TikTok, Wechat, Facebook и т. д.) для передачи официальной и неофициальной информации неопределенному большинству или конкретному человеку [2]. Эти трансформации в журналистике позволяют выпускать, анализировать и распространять новости и информацию через Интернет в социальных сообществах, которые географически могут находиться далеко друг от друга. Таким образом, у каждого человека есть шанс стать журналистом или информатором, каждый может быть причастен к сюжету и оказывать влияние на аудиторию. Отношения между традиционными средствами массовой информации и гражданами меняются. Экология СМИ подверглась беспрецедентному сдвигу, и сегодня «мы-медиа» характеризуются интерактивностью и автономностью, что значительно улучшает свободу прессы.

В наше время одна из важных задач современной теории журналистики - изучение медийных материалов, способных повлиять коренным образом на социальную практику. Поэтому в данной работе рассмотрены актуальные проблемы освещения эпидемии коронавируса.

В начале весны 2020 г. весь мир охватила пандемия, связанная с распространением COVID-19. Это давно забытое слово возвращено в широкий общественный оборот благодаря традиционным и новым СМИ. Повсеместное распространение непонятной и могущественной коронавирусной инфекции внезапно изменили жизнь во всем мире: это явление оказалось больше, чем болезнь, и больше, чем эпидемия. Извержение коронавируса стало огромном социально-культурным, экономическим, даже политическим событием практически для всех современных людей и стран.

В СМИ развернулась дискуссия: является ли новый коронавирус биологическим оружием, созданным в китайской лаборатории, или чем-то, что основатель Microsoft Билл Гейтс создал, чтобы получить прибыль от возможной вакцины? Или вирус вообще существовал всегда? В прессе высказывались сомнения о целесообразности самоизоляции людей (например, об этом публично заявляли в Швейцарии лидеры протестов против изоляции и сторонники теории заговоров). «Мы-медиа» в этот момент использовали кризис для распространения слухов и охвата аудитории.

Все это является частью «инфодемии» (термин Всемирной организацией здравоохранения – ВОЗ): во время глобальной вспышки коронавируса «мы-медиа» использовались для сбора и распространения «чрезмерной массы информации, в том числе, и реальных и фиктивных материалов – что затрудняло людям поиск надежных источников информации». Непроверенные утверждения о происхождении вируса, симптомах и потенциальных способах лечения постоянно опровергались правительственными органами и министерствами здравоохранения с помощью достоверных сведений.

Тем не менее, новые исследования показывает, что дезинформация о COVID-19 в мире, хотя и присутствует, но не так широко распространена в России и Китае, как в некоторых странах, где поляризация, низкий уровень доверия к государственным институтам и неразвитость науки заставляют людей делиться в социальных сетях непроверенными сведениями, сомневаться в официальном информировании о вирусной инфекции.

Исследование, опубликованное в British Medical Journal, показало, что более четверти самых популярных видеороликов YouTube о коронавирусе содержат вводящую в заблуждение информацию. Эксперты предупреждают, что страх приводит к опасном действиям.

Эта вводящая в заблуждение информация включает в себя расистские высказывания, фейковые заявления о том, как распространяется вирус новой короны, фейковые советы по здоровью и пропаганду откровенной теории заговорах [4]. Широко распространялось в «социальных коммьюнити» опасная теория, согласно которой новый коронарный вирус является плановым методом контроля популяции. Ряд «мы-медиа» утверждали, что фармацевтические компании уже имеют лекарство, которое могло бы вылечить от нового вируса, но до сих пор держат это в секрете.

Исследователи медиа утверждают, что более 250 миллионов просмотров самых популярных релевантных видеороликов на YouTube и 62 миллиона просмотров видео, содержащих значительной степени ложную информацию о новом вирусе, могут нанести серьезный ущерб общественному здоровью и обществу [3].

В исследованиях также отмечается, что, хотя сила социальных сетей заключается в большом тематическом разнообразии, в генерации и распространении полезной информации, они также имеют большой потенциальный вред. Распространение дезинформации усиливает расизм и страх за себя и близких и приводит к деструктивному и опасному поведению, например, к массовому «захвату» туалетной бумаги в супермаркетах или краже масок во время эпидемии коронавируса. Люди, живущие под угрозой вируса, испытывали особый страх. Каждый день, возвращаясь домой, они тщательно дезинфицируют свои личные вещи и моют руки, носят маски во время нахождения на улице, сохраняют социальную дистанцию в общественных местах.

По мере распространения эпидемии коронавируса организации общественного здравоохранения должны лучше использовать мы-медиа» для предоставления своевременной и точной информации и минимизации распространения дезинформации. Это, вероятно, сыграет важную роль в успешном контроле вспышки.

Операторы «мы-медиа» стремятся к своевременности информации, большинство информаторов не имеют профессиональных знаний в таких областях, как здравоохранение, технологии и т. д. Кроме того, по сравнению с традиционными средствами массовой информации, для них затруднен доступ к профессиональным ресурсам в этих областях, и, следовательно, они не могут гарантировать достоверность публикуемой информации. Некоторые из них вызывают панику в обществе, поскольку СМИ публикуют для привлечения аудитории непроверенные новости. Пандемия новой коронавирусной инфекции COVID-19 уже оказала беспрецедентное влияние на различные области человеческой жизнедеятельности, в том числе на ее современный технологический уклад.

Состояние с информированием общества о развитии эпидемии остается тревожным, что заставляет вновь поднимать в научном дискурсе вопрос об информационной безопасности. Проведенный анализ показал, что основным риском информационной безопасности являются беспрецедентные атаки социальной инженерии, спекулирующие на теме нового коронавируса как «приманки» для населения.

Всплеск сообщений со словами «карантин», «инфекция», «борьба», «пандемия», «врач», «смерть» в социальных сетях наблюдался в России в апреле 2020 г. (более 1,5 млн. сообщений в день) (что связано с открытым совещанием В. Путина по эпидемии). Наибольшую популярность в социальных сетях имели посты известных людей о вирусе (доктор Комаровский и другие блогеры). С марта 2020 г. популярная у молодежи социальная сеть «ВКонтакте» впервые стала опережать «Facebook» в объемах обсуждения темы коронавируса [1], которое обнажило, в частности проблему COVID-диссидентства.

Существует проблема информационной безопасности для тех, кто работает в дистанционном режиме. Во время профилактики эпидемий дистанционная работа является альтернативным решением организации для переходного периода. Однако телекоммуникационные сети также становятся уязвимыми перед лицом информационных угроз, нередко сталкиваются с риском использования конфиденциальных документов хакерами, а также вирусными атаками вымогателей. Права доступа к интрасети утрачиваются, происходит утечка информации и кражи коммерческой тайны. Осуществляется чрезмерный сбор SMS, адресных книг, местоположения, записей и другой конфиденциальной информации пользователя. Часто это происходит без согласия пользователя на сбор и распространение информации. Недостаточная защищенность удаленных рабочих мест являлась причиной возникновения компьютерных инцидентов в корпоративных и ведомственных информационных системах. Не случайно в рекомендациях Национального центра сказано о необходимости внимания сотрудников к фишинговым атакам, связанным с тематикой COVID-19, так как эта информация беспрепятственно попадает потом с «сетевые сообщества».

Апробация в рамках победы над эпидемией в Китае, например, «приложений облачных, супер и когнитивных вычислений, смарт-слияния сенсорных сетей, квадрокоптеров, персональных гаджетов и смартфонов, цифровых биологических и санитарных двойников продемонстрировала эффективность информационных технологий» [5]. Также примечательным стало повышенное внимание к информационной безопасности, что неизбежно обозначило проблемные вопросы кибербезопасности информационных систем всех уровней – от персонального до международного.

Функционирование мы-медиа в период пандемии показало, что это сила, которая может превзойти влияние институтов, контролирующих новости и информацию и повлиять на ситуацию как позитивно, так и негативно. Именно поэтому в научном сообществе назрел вопрос о противодействии корпусу фальшивых новостей (fake news) и дезинформирующих сообщений и разработке метода их детектирования.

СПИСОК ЛИТЕРАТУРЫ

1. Дейнека О.С., Мельник Г.С., Духаниа Л.Н, Максименко А.А. 27 апр. 2020 Психологическое состояние общества в условиях инфодемии // Инновационное развитие : потенциал науки и современного образования: сборник статей VI научн.-практ. конф. Пенза: МНЦС «Наука и просвещение», 2020. С. 194-197.

2. Дейл Пескин, Эндрю Начисон. Мы-Медиа: Новейшие СМИ меняют глобальное общество. – eJournal USA. – Том 7. –№ 3. Март 2006 года // Электронная публикация: Центр гуманитарных технологий. – 21.08.2006.
3. Малькова В.К. Коронавирус в российском информационном пространстве. – Институт этнологии и антропологии им. Н.Н. Миклухо-Маклая РАН, 2020. С. 206–224.
4. Марков А. Информационная безопасность в условиях пандемии COVID-19 // Эксперт-онлайн. 09.04.2020. Электрон. ресурс. https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-covid-19 (дата обращения - 29 сентября 220).
5. Об угрозах безопасности информации, связанных с пандемией коронавируса (COVID-19.). НКЦКИ,
6. 2020. – ALRT-20200320.1 (20 марта 2020 г.). – 4 с. URL: https://safe-surf.ru/upload/ALRT/ALRT-20200320.1.pdf

УДК 004.05.5

СТРАТЕГИИ РЕЛИГИОЗНО-ПОЛИТИЧЕСКИХ МАССМЕДИА В ВОЙНЕ ЦИВИЛИЗАЦИ И СМЫСЛОВ

Мельник Галина Сергеевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: melnik.gs@gmail.com

Аннотация. В статье рассматриваются коммуникативные стратегии религиозно-политических текстов экстремистской направленности, оказывающих информационно-психологическое воздействие на массовую аудиторию. Коммуникативные стратегии направлены на десакрализацию традиционных ценностей, святынь, основных положений религиозных учений.

Ключевые слова: СМИ, когнитивная безопасность, тактика, религиозно-политический дискурс, война цивилизаций, смыслы.

STRATEGIES OF RELIGIOUS-POLITICAL MASS MEDIA IN THE WAR OF CIVILIZATIONS AND MEANINGS

Melnik Galina
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: melnik.gs@gmail.com

Abstract. The article discusses the communication strategies of religious and political texts of an extremist orientation, which have an informational and psychological impact on a mass audience. Communicative strategies are aimed at the desacralization of traditional values, shrines, the basic tenets of religions.

Keywords: media, cognitive security, tactics, religious and political discourse, war of civilizations, meanings.

Введение. В научном дискурсе суть современных гибридных войн характеризуется как переход от противостояния в идеологической сфере к конфронтации цивилизационной, т.е. к войне цивилизаций и смыслов их существования [1]. В цивилизационную войну вступают организации, использующие религиозные догматы в политических целях. В их целенаправленной и системной информационной деятельности используется широкий диапазон инструментов и коммуникационных стратегий для ведения гибридных войн, направленных, прежде всего, на когнитивную сторону мировоззрения, то есть внутренний мир человека, его чувства, мысли, мировоззрение, индивидуальное и общественное сознание.

Как показывает анализ массива политико-религиозных дискурсов, представленных на исследование в Центр экспертиз СПбГУ, их основными коммуникативными стратегиями являются: 1) десакрализация традиционных ценностей, святынь, пророков, религиозных деятелей и основных положений базовых религий; 2) формирование образа врага; 3) запугивание (ужас, страх, отвращение, паника, сочувствие и сопереживание) и принуждение к смирению или, напротив, борьбе; 4) угроза и мотивация насилия; 5) убеждение аудитории следовать авторитету; 6) воздействие на коллективное бессознательное («нас большинство» и «за нами правда»); 7) подавление воли человека и сознания; 8) внушение адептам избранности и превосходства над другими культурами, религиями; 9) установка идеологических ловушек для сомневающихся и ищущих смысла людей; 10) использование символов, которым приписывается магическое значение и др.

Религиозно-политические мотивы используются в псевдомусульманских текстах, пропагандирующих создание Исламского Халифата; исламские лозунги и элементы учения ислама становятся идеологической платформой для вербовки сторонников. Информационные ресурсы ИГИЛ обширны (Cyber Caliphate; Global Islamic Caliphate, агентство «Аль-Фуркан» и др.) Ислам противопоставляется православию; куфра – исламскому халифату, истинная вера глобальному обществу потребления («русский народ возродится и преумножится ... как часть единой целой уммы, наделённой особой миссией»). Для радикальных направлений ислама характерны: мусульманский энтузиазм, воинственный характер, фанатизм, стремление к мировому господству и превосходство над неверными [2]. Анализ смыслового и эмоционально-экспрессивного содержания текста позволяет выявить ключевые слова медийных текстов – существительные и глаголы действия: «борьба», «бой», «битва», «бунт», «сражения», «схватка» «Судный день», «оружие»: «Пусть свершится Аллаха Всевышнего воля:/Я с тобой навсегда, вплоть до Судного Дня/Не страшит нас угроза страданий и боли,/Мы пойдем на Джихад, в сердце Веру храня». В текстах приводятся аргументы для доказательства закономерности исламизации

России: «Ислам – это мировая религия, которая рано или поздно будет доминировать. Другого пути нет и не будет» и вредности Христианства. С помощью внушения формируются негативные установки против «неверных», которые именуются не иначе как «гнусный кафар», «кафарский смрад», «кафарские группировки», «жиды» и т.д.

В широких масштабах распространяет радикальные идеи и псевдохристианская организация «Свидетели Иеговы», принуждающая человека отказаться от собственной личности для повседневного служения Богу Иеговы. Журналы «Сторожевая башня» и «Пробудитесь!» (издательство Watch Tower Bible and Tract Society of Pennsylvania) попали в книгу рекордов Гинесса как самые массовые с ежемесячным тиражом в 46 и 36 миллионов экземпляров. Свидетели Иеговы живут в 236 странах и территориях и насчитывают более 8 миллионов человек. Мишенью их пропагандистских усилий становятся чувства, надежды, смыслы существования человека. Идеи свидетелей вызывают неприязнь к образу жизни, культуре, традициям, а также религиозным обрядам лиц других вероисповеданий. Главная стратегия – использование страха для достижения цели. Земная история должна закончиться кровавым Армагеддоном, когда Христос в виде Архангела Михаила сойдет на землю в Своем Втором пришествии. Он возглавит воинство Иеговы, и все неверные будут физически истреблены. В битве верные иеговисты будут наслаждаться зрелищем истребления неверных. Для свидетелей человеческое общество и государство есть не что иное, как «мир Сатаны», истинные верующие, согласно такому подходу, вправе не признавать их установления [2].

Неоязычество – новое направление религии, ее идеологи большими тиражами в Церковном издательстве «АСГАРДЪ» (Омск) выпускают литературу о религиозном назначении славян и ариев, распространяют идеи инглизма, основывающиеся на вере в богов и полубожеств, которые якобы помогают людям справиться с типичными жизненными трудностями и покровительствует Родам. Так, «Славянско-Арийские Веды» предлагают читателям «испить из сего источника живую силу Древней Мудрости, Утоляя жажду познания». Авторы обращаются к чадам Расы Великой и потомкам Рода Небесного». Тактика продвижения расистских идей основана на принципе контраста (плохое/хорошее, черное/белое, за/против, друг/враг, темное/светлое). Некоторые аналитики указывают на происхождение новодела – это тот же Бруклин (США), штаб-квартира «Свидетелей Иеговы». Цель рекрутинга последователей учения – возможно еще одна попытка отвратить верующих от Русской православной церкви. «Библия» объявляется «искусственной мифологией», книгой, которая «умышленно искажает и фальсифицирует прошлое народов мира». Авторы сокрушаются: «прискорбно, но факт, что сейчас белые люди, особенно славяне, явно не дотягивают то того, чтобы их воспринимали как Богов».

Заключение. На государственном уровне мощным информационным потокам, исходящим от религиозно-политических организаций, может противостоять контроль, системная пропаганда духовных ценностей и выстроенная государственная система прогнозирования, обнаружения и противодействия распространению экстремистской псевдорелигиозной идеологии.

Исследование выполнено в рамках НИР СПбГУ, проект: М1_2018 - 1: Инновационные методологии обеспечения информационной безопасности Российской Федерации: 2020

СПИСОК ЛИТЕРАТУРЫ

1. Кефели И. Ф. Асфатроника: на пути к теории глобальной безопасности: монография. – СПб. : ИПЦ СЗИУ РАНХиГС, 2020. – 228 с.
2. Жуков А.В. Теология и антропология современного иеговизма / А.В. Жуков // Государство, религия, церковь в России и за рубежом. – М., 2010. – № 1. – С. 165–171.
3. Шугалей М.А., Бурикова И.С., Суханов О.В., Юрьев А.И. Триполи как социальный лифт для ИГИЛ (террористическая организация) / Колл. монография по результатам исследований Максима Шугалея / под науч. ред. проф. А.И. Юрьева. – СПб., 2020. – 96 с.

УДК 32.019.51

ЛОЖЬ КАК ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЙ МАРКЁР НЕГАТИВИЗАЦИИ ОБРАЗА РОССИИ В МАССМЕДИА ГЕРМАНИИ

Мисонжников Борис Яковлевич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: bmiss20550@mail.ru

Аннотация. В качестве одного из методов пропагандистской деятельности массмедиа Германии рассматривается ложь. С ее помощью осуществляется негативизация образа России, что является фактором информационно-психологической манипуляции и наносит репутационный урон стране, создает угрозу ее безопасности.

Ключевые слова: ложь; массмедиа; качественная печать Германии; Россия; пропаганда; репутационный урон.

LIES AS AN INFORMATION-PSYCHOLOGICAL MARKER OF NEGATIVATION OF THE IMAGE OF RUSSIA IN GERMANY MASS MEDIA

Misonzhnikov Boris
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: bmiss20550@mail.ru

Abstract. As one of the methods of propaganda of the mass media of Germany, a lie is considered. With its help, the image of Russia is negated, which is a factor of information-psychological manipulation and inflicts reputation damage on the country, creates a threat to its security.

Keywords: lying; mass media; high-quality printing in Germany; Russia; propaganda; reputation damage.

По мере обострения отношений на межгосударственном уровне противоборствующие стороны с целью негативизации образа соперника зачастую используют приемы, которые, согласно этическим нормам, считаются непристойными. Среди них – ложь, направленная на придание объекту уничижительных и резко отрицательных черт. Она инспирируется в основном политиками и журналистами, и тексты, её содержащие, транслируются при помощи массмедиа на широкую аудиторию не только как сугубо информационный материал, но и предполагающий соответствующие психологические эффекты, создающий почву для манипулирования. По утверждению П. Экмана, «многие политологи считают, что ложь предусмотрена самой международной дипломатией и ставится под сомнение лишь тогда, когда не служит национальным интересам» [1, с. 169].

В зависимости от ситуации ложь, артикулированную в общественном пространстве, могут называть «фейком», «мистификацией», «подделкой», «фальшивкой» и подобными словами, но суть их от этого практически не меняется. Это клеветнические высказывания, к которым прибегают с определенной корыстной целью, когда нет реальных и правдивых аргументов. В современном политическом мейнстриме, к сожалению, ложь стала общим местом, и даже президент США Д. Трамп вынужден был обратиться в суд с исковым заявлением против крупнейших американских изданий, уличенных в подтасовке фактов.

Ложь становится и отличительной особенностью массмедиа Германии. М. Новрот, корреспондент сетевого издания WiWo Online, которое входит в медиагруппу Handelsblatt, так сформулировал свой вопрос в интервью: «В Германии дело дошло до того, что представители некоторых групп говорят о „лживой прессе“. Почему возникает это недоверие?» Интервьюируемый – один из ведущих немецких журналистов У. Викерт – ответил: «Немецкая пресса целенаправленно дискредитируется, и это происходит не только изнутри нашего общества, но также извне. Мы переживаем актуальное событие: российское государство использует пропаганду против немецких журналистов, чтобы поколебать доверие к ним. Лично я не могу исключить то, что понятие „лживая пресса“ в Германии распространила русская секретная служба». Ответ прозвучал столь странно, что даже М. Новрот возразил: «Это для меня нечто новое, разве не в движении **Pegida (правопопулистская организация.** – *Б.М.*) **употребили это слово**?» У. Викерт подтвердил, но тут же заметил, что **Pegida** финансируется русской спецслужбой. Еще более озадаченный М. Новрот поинтересовался: у вас, мол, есть доказательства? Ответ У. Викерта: «Нет. Ни в коем случае. Я не говорю, что это так. Но мы должны об этом думать!» [2]. Ответ не выстроен логически: тезис, содержащий ложное утверждение, используется как аргумент и тут же опровергается самим субъектом. Но нужный эффект достигнут. К слову сказать, У. Викерт – действительно авторитетный журналист. Его отец – знаменитый дипломат и писатель Э. Викерт, который в годы существования Третьего рейха критиковал гитлеризм, однако вступил «по служебной необходимости» в национал-социалистическую немецкую рабочую партию – «это ведь было обязательно». А вот про деда сам Э. Викерт говорил, что тот «нацист и убежденный антисемит» [3]. Видимо, всё это не могло не повлиять на подсознательном уровне и на мировоззрение У. Викерта.

Ложь в качественной печати используется, как правило, ненавязчиво, незаметно. Так, корреспондентов респектабельной Frankfurter Allgemeine Zeitung (FAZ) трудно уличить в откровенной неправде, но многие события интерпретируются ими столь предвзято, что трудно признать это честным исполнением профессиональных обязанностей. Это касается, в частности, освещения событий в Сирии, в которой до появления российских вооруженных сил наступила гуманитарная катастрофа. Благодаря ударам российской авиации была разрушена инфраструктура ИГИЛ, предоставлена военная и гуманитарная помощь, причем российская сторона последовательно выступала за то, чтобы применение силы осуществлялось под контролем ООН. Тем не менее FAZ обвинила Россию в «военных преступлениях» против населения. При этом газета не провела собственного расследования, даже не сослалась на свидетельства очевидцев, а использовала примитивную пропагандистскую схему. Редакция воспроизвела опубликованное в таблоиде Bild высказывание специалиста по внешней политике CDU Н. Рёттгена. Политик заявил об «отвратительном военном преступлении» российской авиации, которая произвела «целенаправленную бомбардировку гражданского населения», и потребовал ужесточения санкций в отношении России [4]. Редакцию качественной FAZ не смутила репутация бульварной Bild да и самого Н. Рёттгена, политическая карьера которого была, как подчеркнула газета Die Rheinische Post, «ухабистой» [5]. Зато частное мнение второразрядного политика дало повод FAZ поставить крупным кеглем и прописными буквами подзаголовок «ВОЕННЫЕ ПРЕСТУПЛЕНИЯ В СИРИИ», а в заголовке упомянута Россия, которой нанесен репутационный урон. То есть корреляция недвусмысленная и весьма жесткая, требующая доказательства, которого в публикации нет.

Исследование выполнено при финансовой поддержке РФФИ: проект «Медиаобраз России в контексте национальной безопасности», №19-013-00725.

СПИСОК ЛИТЕРАТУРЫ

1. Экман П. Психология лжи / пер. с англ. 4-е изд. – СПб.: Питер, 2013. –288 с.
2. Nowroth M. Ulrich Wickert: "Medien haben ein falsches Verständnis von Toleranz"**.** "Die russische Propaganda richtet sich gegen deutsche Medien" // WiWo Online [Электронный ресурс]. URL: https://www.wiwo.de/politik/deutschland/ulrich-wickert-die-russische-propaganda-richtet-sich-gegen-deutsche-medien/12890660-2.html (дата обращения: 29.06.2020).

3. Kulke U. Ein undiplomatischer Diplomat und die Freiheitsliebe // Die Welt. 2007. 9. Apr.
4. KRIEGSVERBRECHEN IN SYRIEN: Röttgen fordert Sanktionen gegen Russland // Frankfurter Allgemeine Zeitung. 2020. 18. Febr.
5. Der politische Werdegang von Norbert Röttgen // Die Rheinische Post [Электронный ресурс]. URL: https://rp-online.de/nrw/landespolitik/norbert-roettgen-der-werdegang-des-politikers_bid-8921821 (дата обращения: 29.06.2020).

УДК 316.772.5

СЕТЕВОЙ ТРОЛЛИНГ КАК УГРОЗА ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Пак Екатерина Максимовна
Северо-Западный институт управления РАНХиГС
Черняховского ул., 6/10, Санкт-Петербург, 191119, Россия
e-mail: EMPak@yandex.ru

Аннотация. Сегодня интернет в некотором смысле стал некой заменой реальной коммуникации. Каждая возрастная категория устремлена к поиску наиболее удобных способов общения. Однако, всемирное виртуальное общение по своим психологическим последствиям крайне неоднозначно. Можно стать жертвой троллей. В статье автор изучает причины возникновения сетевого троллинга и степень его угрозы на психологическую безопасность личности.

Ключевые слова: троллинг, сетевые коммуникации, агрессия в интернете, безопасность личности, психологический прессинг.

NETWORK TROLLING AS A THREAT TO PSYCHOLOGICAL SECURITY OF THE INDIVIDUAL

Park Ekaterina
The North-West Institute of Management of RANEPA
6/10 Chernyakhovsky St, Saint Petersburg, 191119, Russia
e-mail: EMPak@yandex.ru

Abstract. Today the Internet has become a substitute for real communication. Each age group strives to find the most convenient ways to communicate. However, worldwide virtual communication is extremely ambiguous in its psychological consequences. You can become a victim of trolls. In the article, the author studies the causes of network trolling and the degree of its threat to the psychological security of the individual.

Keywords: trolling, network communication, aggression on the internet, security of person, socio-psychological characteristics, psychological pressure.

Сегодня главным трендом современной онлайн-среды является социализация интернета. Особенно остро это стало ощущаться в период пандемии, которая, в прямом смысле этого слова, свела все жизненные ресурсы человека в виртуальную плоскость, неизмеримо увеличивая не только число интерактивных, персональных и профессиональных площадок, но и количество межличностных взаимодействий. Так особую популярность получила такая форма коммуникативной практики как троллинг. Первоначально данное явление воспринималось как безобидное занятие. Однако, в последние годы оно стало представлять угрозу психологической безопасности личности, поскольку из стихийно провокационной деятельности перешло в стадию спланированного процесса агрессии, выходящий уже за пределы сетевого общения [1-5]. В результате этого у потенциальной жертвы может наблюдаться эмоциональная нестабильность, нервозность, ответная агрессивность, депрессия и многое другое. Именно поэтому учеными феномен троллинга исследуется одновременно в нескольких направлениях: в области изучения социально-психологических свойств личности, занимающейся троллингом, в анализе поведенческих проявлений «троллей», в исследовании методов применения технологии троллинга в разных сферах жизнедеятельности [4].

Сейчас троллинг представляет собой рациональное выстраивание своего образа для других как агрессора, нацеленного творить зло и причинять вред путем вызывающего поведения, нарушения этических, моральных и правовых норм и настойчивого продвижения своей лжетеории, ослабляя, таким образом, чувство взаимного доверия в обществе. Отметим, что благоприятной средой для развития троллинга были социальные сети. Создав мнимое чувство безопасности из-за удаленного общения и условия анонимности, абсолютно все интернет-пользователи получили полную свободу экспериментировать со своими идентичностями и свободно проявлять свою активность. Именно здесь впервые стала наблюдаться мотивационная и инструментальная агрессия как самоценность. То есть, когда вброс провокационной информации и грамотно построенный процесс сетевого конфликта стал основой для привлечения интереса к своей личности со стороны участников, косвенных наблюдателей и администраторов социальных ресурсов. Именно тогда технология троллинга стала применяться не только для оживления топиков, но и для повышения активности посетителей каких-либо форумов, чатов, групп, сообществ с помощью применения стратегии анонимного стравливания участников. Посеять раздор, нарушить баланс, выявить уязвимые стороны конфликтующих сторон, - вот на чем зиждется мотивационная деятельность троллей.

Сейчас этот процесс стал все менее и менее контролируемым. Троллинг можно встретить не только в сети интернет, но и в повседневной жизни, и в средствах массовой информации. Более того, по наблюдениям Ю.М. Коняевой, анонимный троллинг становится персонифицированным и используется для эпатирования общества

[2]. Самыми распространенными стратегиями являются троллинг в форме высмеивания и публичного унижения и троллинг-провокация. Строятся они на эпатажности, самоутверждении и самовыражении. Коммуникативная практика использования данных стратегий крайне непредсказуема и имеет многовекторные исходы со стороны той личности, в отношении которой оказывают психологическую атаку. Сами тролли-провокаторы по социально-психическим особенностям обладают устойчивой нервной системой и притупленным чувством вины. Поэтому уязвимым звеном в этой ситуации является тот, против кого используются сфальсифицированная и намеренно искаженная информация.

Разные тролли ведут себя по-разному. Одни нацелены на кратковременную, моментальную агрессию, которая выражается в коротком провокационном высказывании. Другие применяют набор манипулятивных технологий (медиатака, подстрекание, навешивание ярлыков, провокация и мн. др.). Третьи, занимаются самолюбованием и самоутверждением, интеллектуально втаптывая своего оппонента в грязь. Тролли достаточно сплоченное сообщество с выверенными методами провокационных тактик. Можно предположить, что с дальнейшим развитием интернета это явление будет качественно развиваться и трансформироваться, распространяясь более глобально. Отказаться от интернета в наше время не представляется возможным. Однако в наших силах разобраться в опасных формах психологического прессинга, выработать стратегии по снижению уровня восприимчивости деятельности троллей и сохранить здоровую психосоматику.

СПИСОК ЛИТЕРАТУРЫ

1. Дементьев О. М., Дубровина М.М. Интернет-троллинг – шалость, правонарушение или преступление. Тамбов: Тамбовск. гос. ун-т // Научная электронная библиотека «КИБЕРЛЕНИНКА» // [Электронный ресурс] URL: https://cyberleninka.ru/article/n/internet-trolling-shalost-pravonarushenie-ili-prestuplenie/viewer (дата обращения 03.07.2020)
2. Коняева Ю.М. Троллинг как коммуникативный феномен // Научные ведомости. Серия Гуманитарные науки. 2015. №18(215). Вып. 27. С. 140-144.
3. Лучинкина А.И. Троллинг в интернет-пространстве как результат девиантной интернет-социализации. Крым: Крымский инж. пед. ин-т // Научная электронная библиотека «КИБЕРЛЕНИНКА» // [Электронный ресурс] URL: https://cyberleninka.ru/article/n/trolling-v-internet-prostranstve-kak-rezultat-deviantnoy-internet-sotsializatsii/viewer (дата обращения 03.07.2020)
4. Фонталова Н.С., Турганова Г. Э. Социально-психологические особенности людей, занимающихся троллингом // Вопросы теории и практики журналистики. 2019. Т.8. №1. С. 179- 194
5. Черных А. Мир современных медиа. М.: Изд.дом «Территория будущего», 2007. 312 с.

УДК 32.019.51

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ВОЗДЕЙСТВИЯ ФЕЙКОВЫХ НОВОСТЕЙ НА АУДИТОРИЮ

Садчиков Даниил Игоревич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: sadchikovforwork@mail.ru

Аннотация. Статья посвящена изучению фейковых новостей как коммуникативного инструмента ведения сетевой пропаганды и новейшей формы пропагандистского воздействия, в основе которого лежат социально-психологические особенности взаимодействия с окружающей действительностью.

Ключевые слова: фейковые новости, пропаганда, PR-отдел, воздействие.

SOCIAL AND PSYCHOLOGICAL PECULIARITIES OF THE IMPACT OF FAKE NEWS ON THE AUDIENCE

Sadchikov Daniil
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: sadchikovforwork@mail.ru

Abstract. The article is devoted to the study of fake news as a communicative tool for conducting network propaganda and the latest form of propaganda influence, which is based on the social and psychological characteristics of interaction with the surrounding reality.

Keywords: fake news, пропаганда, PR-отдел, воздействие.

Сегодня информационные потоки бесчисленны, и контроль над ними является важнейшим средством достижения успеха. Пропаганда становится важнейшим инструментом, лоббирующим интересы самых разнообразных политических и экономических организаций. Каждая политическая партия имеет свои канал распространения информации в широкие массы людей, каждая коммерческая организация имеет свой PR-отдел, который продвигает интересы бренда в обществе, каждое важное политическое решение сопровождается подготовкой общества к переменам через СМИ.

Но далеко не всегда мотив распространения определенной идеологии прозрачен и бескорыстен. Огромное количество организаций не пренебрегают искажением информации или искажением фактов, использованием манипулятивных технологий при аргументации своей позиции в обществе. Как правило, целью негативной пропаганды является создание удобного фона в виде социальной вражды, эскалации социальных конфликтов,

обострения противоречий в обществе, пробуждения низменных инстинктов у людей. Негативная пропаганда основана на низкой критичности и внушаемости масс с целью манипулирования этими массами в интересах узкой группы лиц [2]. Сегодня человеку в процессе взаимодействия с информацией постоянно необходимо задумываться, актуальна ли полученная информация, заслуживает ли источник сообщения доверия, не представляют ли собой новость набор слухов и мистификаций, выдаваемых за истину?

К тому же фокус внимания потребителей новостей постепенно смещается в социальные сети. И, если каждый человек на протяжении всей своей жизни находится под воздействием пропаганды подконтрольной государству, которое чаще преследует благоприятные для общества цели, то социальные сети – чрезвычайно удобная площадка для распространения деструктивной пропаганды, направленной на разжигание социальной вражды, эскалации конфликтов, источником которой может быть лицо, которое никогда не вскроет о себе данные, которые дадут возможность его идентификации. В таких условиях человек и общество потенциально подвержены негативному воздействию.

При этом параллельно с ужесточением законодательства в области СМИ, пропагандисты разрабатывают все более ухищренные способы манипулятивного воздействия на аудиторию. Так, совсем недавно общество столкнулось с совершенно новым коммуникативным инструментом ведения пропаганды, которое в медиасфере получило название fake news или фейковые новости.

В связи с недавними событиями в мировой политике, фейковые новости находятся под пристальным вниманием политологов, журналистов, экспертов в области вычислительной техники во всем мире и вызывают серьезные опасения. Фейковые новости представляют собой настолько сильный по своему воздействию инструмент пропаганды, что из-за них ставят под сомнение легитимность выборов президента США в 2016 г. Проблема фейковых новостей представляют собой проблему на мировом уровне: «Решения на основе фейк ньюс принимаются моментально и могут быть фатальны, победить подобные «лженовости» невозможно, но их ущерб можно минимизировать» –заявила представитель МИДа Мария Захарова [1]. И если специалист в области связей с общественностью хорошо понимает принципы, цели и методы использования традиционных пропагандистских инструментов, таких как сенсационность, навешивание ярлыков, информационная блокада и т.д., то фейковые новости – гораздо более сложный инструмент ведения негативной пропаганды, который представляет собой нерегулируемый процесс, несущей в себе угрозу обществу с точки зрения номенклатурных и социетальных свойств. Отсюда – огромный интерес к феномену фейковых новостей у специалистов самого разного профиля – политологов, лингвистов, социологов, и предметная область психологии выходит на один из первых планов в изучении нового явления.

СПИСОК ЛИТЕРАТУРЫ

1. РИА Новости – https://ria.ru/20190418/1552825431.html, дата обращения 10.04.20192
2. Цуладзе А.М. Большая манипулятивная игра. – М.: Алгоритм, 2000. – 336 с.

УДК 32.019.5

ОСОБЕННОСТИ РАБОТЫ ПРЕСС-СЛУЖБЫ В ЗОНЕ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ: ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Салтыков Виталий Владимирович
Управление Сибирского округа войск национальной гвардии Российский Федерации
Фрунзе ул., 10, Новосибирск, 630091, Россия
e-mail: 9129492212@mail.ru

Аннотация. В статье рассматривается особенность работы временного пресс-центра Сибирского округа войск национальной гвардии РФ, уделено внимание специфике сбора данных в зоне наводнения Иркутской области лета 2019 г. На конкретных примерах описана деятельность по получению и применению получаемых сведений в координации работы как самого пресс-центра, так и действий по ликвидации последствий чрезвычайной ситуации. Определены задачи, стоящие перед временным пресс-центром в зоне ЧС по сбору данных.

Ключевые слова: временный пресс-центр; чрезвычайная ситуация; сбор данных; наводнение в Иркутской области; Росгвардия.

SPECIFIC FEATURES OF THE PRESS SERVICE IN THE ZONE OF EMERGENCY SITUATION: PROBLEMS OF INFORMATION SECURITY

Saltykov Vitaliy
Federal National Guard Troops Service of the Siberian district, Russian Federation
10 Frunze St, Novosibirsk, 630091, Russia
e-mail: 9139492212@mail.ru

Abstract. The article discusses the peculiarity of the work of the temporary press center of the Siberian District of National Guard of the Russian Federation, attention is paid to the specifics of data collection in the flood zone of the Irkutsk region in the summer of 2019. Using specific examples, the activity on obtaining and using information in coordination the work of both press center and actions to eliminate the consequences of an emergency are described. A conclusion is made on the important tasks facing the temporary press center in the emergency zone to collect data.

Keywords: temporary press center; emergency; data collection; flooding in the Irkutsk region; Federal National Guard Troops Service.

Развитие информационного общества в России требует от различных ведомств и органов государственной власти придерживаться важнейших принципов работы, когда помимо выполнения непосредственных обязанностей и распоряжений руководителя, необходимо информировать общественность, взаимодействующую со средствами массовой информации. Благодаря работе СМИ, а также наличию мессенджеров по обмену информации, публикационной активности блоггеров, любая чрезвычайная ситуация становится темой для активного обсуждения, которая содержит в себе не только описание сложившейся ситуации, в том числе и мер по предотвращению последствий, но потребности и ожидания участников трагедии, в сообщениях демонстрируя их страхи и надежды. В итоге на сотрудников временной пресс-службы в зоне чрезвычайной ситуации накладывается задача не только освещать свои действия, но и осуществлять «своего рода психотерапию социальной сферы» [1].

Особенностью работы пресс-службы в зоне чрезвычайной ситуации в Иркутской области летом 2019 г. в том, что она является *резонансной*, а значит из-за ее особенностей (масштабность, экстремальность и критичность для органов государственной власти, а также разрушения, вызванные стихией) все общественное внимание приковано к происходящим событиям и вызывает ажиотаж при обсуждении проблемы. Главной задачей сотрудников временного пресс-центра Росгвардии был оперативный сбор данных для быстрого реагирования и снижения градуса напряженности, в первую очередь у местных жителей, та как они находились в стрессовой, кризисной ситуации [2, 3]. Для сбора данных при современном развитии информационного поля в первую очередь было важно проводить постоянный мониторинг социальных сетей, что позволяло быстро принимать меры для оказания помощи в конкретных случаях, в частности, проводился анализ публикаций граждан на страницах соцсетей, где была размещена информация о той или иной ситуации в конкретном районе, улице или доме. Важно отметить, что в пострадавших районах была ограничена работа Интернет, что вызывало необходимость работать и собирать данные непосредственно у местных жителей. В ситуации кризиса человеку свойственно при нехватке достоверной, а главное официальной информации по актуальным проблемам (особенно если это касается удовлетворения базовых потребностей), формировать слухи, в том числе и слухи-пугала. Такой темой для пострадавших была доставка чистой питьевой воды. Информация расходилась среди пострадавших от паводка исключительно при личном контакте или во время телефонных переговоров. Суть передаваемой информации заключалась в том, что в воде, поставляемой военнослужащими Росгвардии с помощью специальной техники АРС имеются опасные болезнетворные бактерии и частицы травы и ила. Для предотвращения распространения слухов в первую очередь необходимо предоставить официальную информацию. Был подготовлен сюжет, совместно с местным телеканалом ТВ-12 (г. Нижнеудинск), в котором привлекалась санитарно-эпидемиологической службы по проверке качества воды специалистами СЭС, как на водозаборнике, так и с машин АРС Росгвардии в пунктах выдачи воды, что позволило прекратить распространение слухов среди пострадавшего населения. Отдельно важно заменить, что задачей деятельность временного пресс-центра было не только освещать действия сотрудников Росгвардии по предотвращению последствий чрезвычайной ситуации, но и сбор сведений на местах, включая личную беседу с пострадавшими. Получаемые данные позволяли координировать работу военнослужащих для оказания помощи населению.

Необходимо отметить, что для оперативного реагирования временному пресс-центру на месте чрезвычайной ситуации, для корректной работы необходимо выполнить ряд задач:

1) составить список первоочередных вопросов/проблем местного населения, требующих действий от сотрудников Росгвардии, что позволит оперативно составить не только план работ для ликвидации последствий ЧС, но и взаимодействуя со СМИ, успокоить слухи и предотвратить распространение паники и страхов;

2) проводить мониторинг не только информационного пространства, но и обязательно лично взаимодействовать с пострадавшими гражданами, получая сведения, которые позволят корректировать действия собственного ведомства для снижения негативных настроений населения (желательно в личных беседах с пострадавшими для получения верных и наиболее полных данных выступать в роли гражданского населения, так как высока вероятность, что пострадавшие и находящиеся в зоне ЧС могут предоставить неверные сведения);

3) корректно, а главное своевременно предотвращать появившиеся слухи, используя официальные каналы, особенно местные и федеральные СМИ, для предоставления официальных данных.

Сложность сбора данных в зоне чрезвычайной ситуации обусловлена психологическим состоянием пострадавшего населения, а человеку свойственно в состоянии стресса воспринимать действительность в искаженном виде, а также транслировать свои страхи и ожидания всеми возможными способами.

В этих условиях важно суметь правильно собрать, проанализировать оперативную информацию и провести коррекцию действий для помощи пострадавшему населению.

СПИСОК ЛИТЕРАТУРЫ

1. Катарина И.В., Закирова С.В. Работа временных (выездных) пресс-центров территориальных подразделений МЧС России при возникновении чрезвычайных ситуаций // Новое слово в науке: перспективы развития. 2016. № 3 (9). С. 81-85. [Электронный ресурс]. URL: https://www.elibrary.ru/download/elibrary_26508282_36086709.pdf (дата обращения: 10.07.2020).

2. Рыклина М.В. Пресс-секретарь чрезвычайного ведомства. Советы начинающим. Уч. пособие. ВНИИ ГОЧС (ФЦ) МЧС России. Москва, 2014.
3. Елисеев А.П., Лебедев А.В. Катастрофический паводок в Краснодарском крае (2012 г.) // Стратегия гражданской защиты: проблемы и исследования. 2017. Т.7. № 1(12). С. 83-94

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ

УДК 004.8

ПЕРСПЕКТИВЫ РОБОТОТЕХНИКИ И СЕНСОРИКИ В СФЕРЕ ЭКОНОМИЧЕСКОГО ОБРАЗОВАНИЯ

Гуськова Екатерина Дмитриевна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: katya.guskova.2000@mail.ru

Аннотация. Рассмотрено влияние сквозных информационных технологий на сферу образования. Проанализированы возможности и примеры внедрения компонентов робототехники и сенсорики в процесс обучения студентов.

Ключевые слова: сквозные технологии; робототехника и сенсорика; образование; моделирование; компьютерные симуляторы.

THE PERSPECTIVES OF THE COMPONENTS OF ROBOTICS AND SENSORICS IN THE ECONOMIC EDUCATION SPHERE

Guskova Ekaterina
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: katya.guskova.2000@mail.ru

Abstract. This article examines the influence of the end-to-end information technologies on the education sphere. Possibilities and examples of implementation of the components of Robotics and Sensorics technology in the learning process are analyzed.

Keywords: end-to-end technology; robotics and sensorics; education; modeling; computer simulators.

Образование – одна из тех областей, которая способна внедрять технологические нововведения и готовить высококвалифицированные кадры, которые будут востребованы в будущем. В ближайшее время в сфере образования одной из востребованных сквозных информационных технологий может стать цифровая технология «компоненты робототехники и сенсорика» [1].

Если не рассматривать человеческий и психологический факторы, то становится ясно, что технологии позволят в ближайшем будущем полностью исключить человека из рутинного процесса образования, но этот подход не является правильным. На сегодня задача – создать инструменты, которые помогут преподавателям обучать студентов и которые улучшат качество образования. Компоненты робототехники и сенсорика (КРиС) могут стать вспомогательными инструментами в процессе обучения и значительно увеличат интерес обучаемых благодаря инновационному подходу, моделированию реальных ситуаций и возможности обучаться из любой точки мира.

Робототехника – наука, связанная с созданием и использованием роботов и компьютерных систем управления различного назначении [2].

Цифровые системы имеют свои «органы чувств», за их развитие отвечает сенсорика. Эксперты прогнозируют непосредственное влияние сенсорики на развитие экономики в ближайшие десятилетия. Сегодня сенсорика помогает роботам как измерять физические величины, так и обрабатывать сенсорную информацию.

Цифровая технология КРиС предусматривает как создание автоматизированных и сенсорных систем, так и разработку методов управления ими. Помимо этого, еще одна важная задача КРиС – создание отлаженного взаимодействия между человеком и техническими системами [3].

При рассмотрении возможности внедрения КРиС необходимо учитывать последствия и рассматривать уже существующие примеры. В сегодняшней ситуации очень остро встает вопрос дистанционного образования, но робототехника и сенсорика это следующие шаги в развитии и информатизации данной сферы.

Образование – одна из приоритетных областей применения КРиС. В ней выделяются два главных аспекта развития: образовательные программы и обучение на физических симуляторах/конструкторах. Такие технологии можно применять как в высшем, так и в школьном образовании.

Основными задачами внедрения являются: улучшение качества образования; обучение современным технологиям с ориентацией на высокотехнологичное будущее; получение самых актуальных знаний о современном мире. Но в процессе внедрения можно столкнуться с некоторыми трудностями, такими как: технические сложности в создании программ и роботов-учителей: производство дорогостоящего оборудования; наполнение технических инструментов качественным контентом и понятным интерфейсом; изменение нынешней программы; переквалификация педагогического состава.

Нужны сильные кадры для разработки новейших инструментов, а также для дальнейшего понимания работы таких систем и активного использования в повседневной жизни. Поэтому высшее образование должно быть нацелено на подготовку высококвалифицированных специалистов в разных сферах, которые в будущем будут иметь непосредственный контакт со «сквозными» технологиями.

КРиС могут быть введены в качестве дополнительных дисциплин для изучения непосредственно для технических специалистов, а также и для всех других специальностей в новом формате обучения на симуляторах и конструкторах. Сегодня симуляторы используют в тех сферах подготовки кадров, где затраты на создание робота меньше, чем на любое другое моделирование реальной ситуации, например, подготовка пилотов. Явным преимуществом таких симуляторов являются низкие экономические затраты, не требующие постоянного вложения денежных средств для пополнения материалов, ведь их можно использовать многократно. Другим преимуществом будет безопасность использования и наглядность. Учащиеся смогут проводить эксперименты в рамках изучения естественных наук без вреда для жизни и здоровья.

На данный момент у каждого человека есть возможность воспользоваться открытым интернет-источником «Physics Education Technology» [4], созданным доктором естественных наук К. Виманом. Этот источник представляет пользователям возможность виртуального моделирования различных ситуаций, проведение опытов, относящихся к естественным наукам: химия и физика. Такой инструмент дает наглядное, детальное и максимально приближенное к реальности представление о протекании разнообразных физических и химических процессов.

Процесс внедрения компонентов робототехники и сенсорики требует финансирования, разработки технических инструментов, приложений и конструирования роботов-учителей, а также переквалификацию педагогов. Применение компьютерных симуляций и моделирование естественнонаучных процессов повышает активность и интерес учащихся к заданной предметной области. Сейчас симуляторы широко используются в играх, но их можно и нужно внедрять в образование для того, чтобы повысить интерес обучающихся, восполнить недостаток высококвалифицированных преподавателей, стандартизировать образование и повысить шансы людей из разных регионов получать одинаково качественную образовательную услугу.

За рубежом уже был опыт единичных внедрений роботов-учителей. Так, например, во Франции был разработан робот-математик Nao [5], который может давать подсказки учащимся для решения разных математических задач. Еще одним интересным изобретением является VGo [5], оборудованный веб-камерой и позволяющий не пропускать занятий студентам и школьникам с различными заболеваниями или травмами, он в реальном времени транслирует образовательный процесс в двустороннем порядке, что позволяет имитировать живое взаимодействие. Но сегодня каждый компьютер и смартфон оборудован такими же возможностями, поэтому необходимость замены учителей роботами пока что не является актуальной, а вот вопрос об изменении образовательной программы студентов является важным.

Как возможно модернизировать учебную программу студентов для того, чтобы они были востребованными специалистами с актуальными знаниями? Самая ценная возможность, которую могут дать роботы студентам – моделирование реальных ситуаций без финансовых затрат. Это значит, что для обучения студентов экономических специальностей могут быть разработаны специальные программы для имеющихся устройств, которые могли бы давать студенту кейсы для решения с разными вариантами ответов на каждом этапе. От выбора действия в той или иной ситуации зависит дальнейших ход событий и так шаг за шагом студент приходит к результату, по факту, видя все ошибки и эффективные методы на различных этапах, которые максимально приближены к реальным ситуациям в компаниях.

Такой инструмент похож на квест-игру и точно придется по вкусу людям с аналитическим мышлением. Также подобное внедрение поможет рассматривать сложные задачи самостоятельно, но с пояснениями на каждом шаге, что в совокупности с изученными материалами на лекциях даст хороший результат и поможет материалу лучше усвоиться.

Сегодня на различных сайтах можно найти кейсы от компаний, но процесс их решения очень часто кажется сложным и несистематизированным, и студенты, прочитав задание, сомневаются в своих способностях.

Принципиальное отличие программы состоит в том, что каждый шаг будет детализирован и иметь несколько вариантов, каждый из которых приводит к определенному исходу событий. Возможности ошибиться как таковой нет, ведь, как и в жизни, каждое неправильное действие можно будет компенсировать дальше.

Чем данное внедрение таких программ в образование лучше, чем решение таких же кейсов с преподавателем? Во-первых, время на проверку преподавателем сложных задач уменьшится, что поможет педагогу концентрироваться и давать больше полезной информации студентам, так как робот сам будет проверять решения кейса. Во-вторых, интерес студентов и новизна системы. Если добавить в программу понятный и привлекательный интерфейс, то каждому студенту захочется попробовать себя в решении интересных заданий с помощью новых инструментов. Также к плюсам для студентов: такая программа-симулятор даст им возможность попробовать себя в роли желаемых профессий: банкиров, брокеров, аналитиков, менеджеров или даже владельцев больших корпораций.

Сегодня массовое внедрение роботов в сферу образования не представляет большой необходимости, так как затраты на создание инструментов и повсеместное распространение слишком высоки. Однако в будущем это будет хорошая альтернатива «живому» процессу обучения. На данный момент, верная стратегия – подготовка высококвалифицированных специалистов, которые будут готовы к работе со «сквозными» технологиями, в том числе и с «компонентами робототехники и сенсорики» в различных сферах деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровые технологии [Электронный ресурс] // Минкомсвязь России. – Режим доступа: https://digital.gov.ru/ru/activity/directions/878/ (дата обращения: 05.06.2020 г.).
2. Компоненты робототехники и сенсорика [Электронный ресурс] // Минкомсвязь России. – Режим доступа: https://digitech.ac.gov.ru/technologies/robotics_and_sensorics/ (дата обращения: 05.06.2020 г.).
3. Дорожная карта развития «сквозной» цифровой технологии «Компоненты робототехники и сенсорика» [Электронный ресурс] // Минкомсвязь России. – Режим доступа: https://digital.gov.ru/ru/documents/6666/ (дата обращения: 05.06.2020 г.).
4. Physics Education Technology [Электронный ресурс]. – Режим доступа: https://phet.colorado.edu/ (дата обращения: 05.06.2020 г.).
5. Роботы в школах – реальность [Электронный ресурс]. – Режим доступа: https://womo.ua/robotyi-v-shkolah-realnost/ (дата обращения: 05.06.2020 г.).

УДК 007.2

ИСПОЛЬЗОВАНИЕ МЕТОДОВ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ

Емельянов Александр Александрович
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: S1_Alex2000@mail.ru

Аннотация. Описываются методы автоматизированного анализа фото- и видеоизображений. Рассмотрено применение концепций компьютерного зрения для повышения уровня безопасности работы на предприятиях.

Ключевые слова: компьютерное зрение; распознавание изображений; безопасность.

USING COMPUTER VISION FOR INCREASE THE SAFETY OF PRODUCTION PROCESSES

Emelyanov Alexandr
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: S1_Alex2000@mail.ru

Abstract. Describes automated analysis of photo and video images. Considering application the concepts of computer vision to improve enterprises safety work.

Keywords: computer vision; image recognition; security.

При работе сотрудников в рамках вариативных направлений, связанных с производственной сферой деятельности, регулярно возникают ситуации, которые могут явно или опосредованно создавать различные угрозы безопасности. Спектр угроз чрезвычайно велик: от прямой опасности для жизни и здоровья сотрудников до некорректного функционирования бизнес-процессов организации. Общим для всех этих угроз является одно: негативное влияние на финансовые, репутационные и правовые аспекты работы предприятия [1].

Частично подобные ситуации можно предотвратить, используя механизмы так называемого «компьютерного зрения», реализуемые в виде аппаратно-программных комплексов, осуществляющих автоматический анализ фото- и видеоизображений.

Спектр применения таких механизмов весьма широк: от управления конвейерами в цехах обработки и сборки металлоконструкций до распознавания лиц криминальных элементов в видеопотоке камер уличного наблюдения [2]. В целом, все алгоритмы данного класса методик можно свести к следующим задачам:

1. Преобразование формата цветового пространства и выбор способа его отображения. В большинстве случаев перед выполнением следующих шагов требуется привести изображение к более удобному для обработки виду. Например, реализовать повышение уровня резкости, контрастности, свести к черно-белому или полутоновому отображению и т.п.

2. Сегментирование/классификация. Под этим действием подразумевается выделение тех объектов, которые так или иначе можно отделить от остальных по вариативным характеристическим признакам. Данный подход тесно связан с задачами кластеризации. Проблема может быть описана следующим образом: существует некоторое изображение, в рамках которого необходимо предсказать: к какой из категорий относится тот или иной объект, параллельно оценивая точность осуществляемых предсказаний. Решаются задачи определения угла наклона, размера, деформации изображения (аффинных преобразований), освещения поверхностей и т.д.

3. Распознавание (идентификация). В рамках данного этапа определяется: какие объекты из заранее предопределённого набора присутствуют в кадре.

Для эффективной реализации вышеописанных этапов используются различные алгоритмы – многоуровневые каскады Хаара, ИНС, Марковские модели, метод Виолы-Джонса и так далее. Одна из популярных архитектур – свёрточные нейросети, перестраивающие входящий поток данных. Данный подход

позволяет при размере изображения 1000x1000 пикселей не анализировать миллион блоков; вместо этого исходный массив разбивается на части 10x10 и рассматривается определённое количество точек внутри каждого блока. Затем осуществляется смещение на следующий блок. В результате алгоритм осуществляет проход через всё изображение. Это существенно ускоряет классификацию и сокращает вычисления. На следующем шаге преобразованные изображения передаются свёрточному слою классификатора. Каждый слой работает с близлежащими блоками. Затем применяются объединяющие слои. Свёрточный слой 2x2 пикселя сжимается до размеров одного пикселя, который имеет наиболее высокий «вес».

Идентификация отличается от классификации тем, что заключается в обнаружении нескольких объектов в рамках одного изображения. Использование сетей предсказания регионов (RPN) позволяет определить: какую часть изображения следует извлечь, чтобы уменьшить вычислительные затраты.

Немаловажной задачей является отслеживание, то есть процесс определения перемещения одного или нескольких объектов в пространстве. Данная технология активно используется в анализе видеопотока. Применяется такими крупными брендами, как Uber, Tesla и др. Существуют генеративные и дискриминативные методы отслеживания объектов. Первый вариант применяет генеративную модель для описания текущих характеристик объекта и уменьшает вероятность возникновения ошибки в его поисках. Дискриминативный метод применяется для того, чтобы выделить объект и его окружение.

При реализации производственных процессов необходимо решать ряд задач – например, разграничивать доступ в определённые зоны, регистрировать перемещения сотрудников с привязкой ко времени и месту, своевременно обнаруживать брошенные предметы, контролировать ношение средств индивидуальной защиты при работе с потенциально опасной средой и так далее [3]. Для выполнения данных процессов рациональна разработка вариантов программного обеспечения, способного принимать на вход данные о сотрудниках – фотографии, ФИО, личностные характеристики, принадлежность к отделу предприятия и т.д. Далее, на основании анализа видеопотока с камер наблюдения и микрофонов осуществлять ряд действий, базирующихся на прогностических моделях с целью снижения вероятности возникновения потенциально опасных ситуаций. В качестве таковых, например, могут выступать: несоблюдение сотрудниками техники безопасности; пребывание в зоне повышенного риска без соответствующего защитного оборудования; алкогольное или наркотическое опьянение и так далее. В случае возникновения ситуации, подпадающей под критерии потенциально опасной, формируется соответствующее воздействие – информирование службы безопасности, активация аварийной аудиовизуальной сигнализации и т.д.

Также подобное решение может применяться для оперативной оценки в масштабе реального времени некоторых наблюдаемых показателей состояния здоровья сотрудников. Например, при ряде заболеваний имеются внешние манифестации таковых: изменение цвета кожных покровов, характера телодвижений, динамики речи. Подобные показатели достаточно легко отслеживаются при помощи системы видеокамер и микрофонов. Так как данные технические решения используются повсеместно в большинстве устройств, необходима лишь разработка программных модулей для анализа видео- и аудиопотока.

Подобные решения позволят не только повысить уровень безопасности сотрудников (в том числе, и с учётом эпидемиологической ситуации), но и позволит предприятиям сократить расходы на финансовые компенсации и реорганизацию бизнес-процессов в случаях возникновения ситуаций, которые могут привести к значимым потерям как финансового, так и организационного плана.

СПИСОК ЛИТЕРАТУРЫ

1. Аминов Х.И. Модели цифровизации экономической деятельности: монография / Аминов Х.И., Андреевский И.Л., Безрук Г.Г., Верзун Н.А., Воробьева Д.М., Головкин Ю.Б., Горулев Д.А., Емельянов А.А., Карташов П.Н., Касаткин В.В., Кефели И.Ф., Колбанев М.О., Коршунов И.Л., Кунтуров А.Л., Кунтурова Н.Б., Левкин И.М., Левкин О.М., Микадзе С.Ю., Омельян А.В., Пойманова Е.Д., Пуха Г.П., Савченко В.А., Соколов Р.В., Татарникова Т.М., Цихлер А.О., Шахова Е.Ю. – СПб: изд-во СПбГЭУ, 2019. – 179 с.
2. Коршунов И.Л. Проблемы информационно-технологической деятельности / И.Л. Коршунов, М.О. Колбанёв, И.М. Лёвкин // Изв. вузов. Приборостроение. 2017. Т. 60. № 2. С. 105–109
3. Левкин И.М. Комплексная оценка эффективности робототехнических систем добывания и обработки информации // Изв. вузов. Приборостроение. 2017. Т. 60, № 2. С. 110–116.

УДК 621.391

АЛГОРИТМ ВЫБОРА МАРШРУТА ПЕРЕДАЧИ ПАКЕТА ДАННЫХ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Кирилова Дарья Александровна[1], Колбанёв Михаил Олегович[2]

[1] Нижегородский государственный инженерно-экономический университет

Октябрьская ул., 22а, Княгинино, 606340, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

e-mails: dasha.kirilova.96@bk.ru, mokolbanev@mail.ru

Аннотация. В работе предложен алгоритм выбора маршрута передачи пакета данных в беспроводных сенсорных сетях, учитывающий физические характеристики сенсорных устройств в сельскохозяйственных приложениях, основанных на технологии беспроводной связи.

Ключевые слова: беспроводная сенсорная сеть, алгоритм маршрутизации, оптимальный маршрут, сельское хозяйство, энергопотребление.

ALGORITHM FOR CHOOSING THE DATA PACKAGE TRANSFER ROUTE IN WIRELESS SENSOR NETWORKS

Kirillova Daria[1], Kolbanev Mikhail[2]
[1] Nizhny Novgorod state University of engineering and Economics
Oktyabrskaya St., 22A, Knyaginino, 606340, Russia
[2] Saint Petersburg Electrotechnical University "LETI"
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: dasha.kirilova.96@bk.ru, mokolbanev@mail.ru

Abstract. The paper proposes an algorithm for selecting a data packet transmission route in wireless sensor networks, taking into account the physical characteristics of sensor devices in agricultural applications based on wireless technology.

Keywords: wireless sensor network, routing algorithm, optimal route, agriculture, energy consumption.

Цифровая трансформация многих сфер человеческой деятельности не может обойти стороной и сельское хозяйство. Наряду с цифровизацией финансовой [1], образовательной [2] и других деятельностей, цифровизируется и производственная деятельность. Как показывают данные [3], это приносит значительный эффект и в земледелии, и в животноводстве. Внедрение IoT позволило снизить более чем на 20% затраты на воду, благодаря системам орошения, от 5 до 15% снизились затраты на посевной материал, за счет точного земледелия, в результате чего, урожайность повысилась более чем на 10%. Внедрение технологий «Цифровой фермы» позволяет снизить затраты предприятия примерно на 15% за счет эффективного использования кормов и снижения производственного цикла, затраты на оплату труда уменьшаются благодаря сокращению обслуживающего персонала, кроме этого уменьшаются расходы на ветеринарное обслуживание за счет своевременного выявления заболеваний, в целом средняя экономия затрат в животноводстве составляет 15-20%. К числу информационных систем, которые позволяют достигнуть таких результатов, относится интернет вещей, объединяющий технологии идентификации объектов, беспроводных сетей связи, автономного электропитания, сенсорики и др. Сенсорные устройства в сельском хозяйстве необходимы для создания умной фермы. С помощью них, производится постоянный мониторинг всего производства, отслеживают показатели температуры, влажности и т.д. Сенсорные устройства в совокупности представляют собой сенсорную сеть. К числу информационных систем, которые позволяют достигнуть таких результатов, относится интернет вещей, объединяющий технологии идентификации объектов, беспроводных сетей связи, автономного электропитания, сенсорики и др. Сенсорные устройства в сельском хозяйстве необходимы для создания умной фермы. С помощью них, производится постоянный мониторинг всего производства, отслеживают показатели температуры, влажности и т.д.

Эффект от использования сенсорных устройств для контроля за состоянием сельскохозяйственных угодий возникает при их массовом внедрении и использовании для сбора формируемых ими данных при помощи беспроводных сенсорных сетей [4]. При этом существуют проблемы электропитания устройств, которые в подавляющем количестве приложений не могут быть обеспечены централизованным питанием и получают энергию для реализации своих функций от автономной батареи. Продолжительность жизни устройства в основном определяется емкостью батареи и объемом ее энергопотребления [5].

При передаче сообщения сенсорное устройство затрачивает определенное количество энергии, для увеличения жизненного цикла функционирования сети необходимо минимизировать энергопотребление сенсорных устройств, сделать это возможно при выборе правильного алгоритма маршрутизации.

В работе [6] показано, что основным параметром, при помощи которого можно управлять энергозатратами радиопередатчика, является расстояние между антеннами взаимодействующих сенсорных устройств. Требуемая мощность сигнала на передающей антенне прямо пропорциональна квадрату этого расстояния, поэтому в целом ряде случаев использование сенсорных устройств, которые расположены «на пути» передачи сигнала, в качестве ретрансляторов снижает общее энергопотребление пары «источник-ретранслятор».

Расстояние, которое в процессе функционирования беспроводных сенсорных устройств придется преодолевать сигналу, излучаемому передающей антенной, зависит от протоколов маршрутизации. При этом под маршрутизацией понимается процесс определения пути передачи пакета данных от одного узла к другому в сетях связи.

Для нахождения наилучшего пути передачи пакета данных применяется алгоритм маршрутизации данных, который в общем случае состоит из 3 этапов:

1. Выделение из заголовков пакета адреса назначения;
2. Поиск в таблице маршрутизации строки, соответствующей этому адресу;
3. Обновление заголовка пакета, и передача его на блок коммутации [7].

В статье рассмотрена классификация алгоритмов и протоколов маршрутизации. Все изученные протоколы имеют общую идею – выбор наиболее оптимального маршрута внутри беспроводной сенсорной сети, для повышения надежности и производительности сети. В работе предлагается развитие этой общей идеи.

Сенсорное устройство-источник по заданному алгоритму маршрутизации решает проблему выбора маршрута передачи сообщения на базовую станцию. Внутри этого сенсорного устройства заложена программа, которая получает данные со спутника и на основе этих данных, определяет координаты других точек и соответственно решает, как лучше передать сообщение.

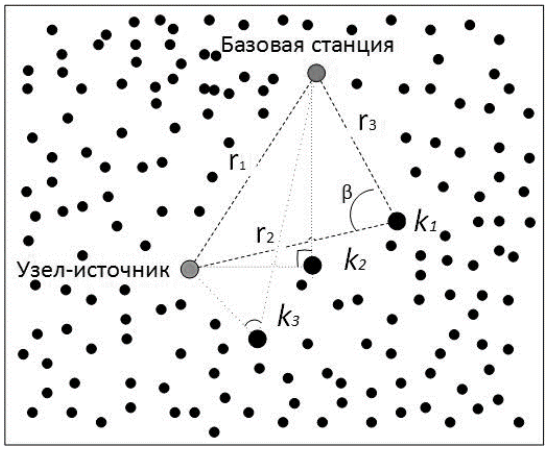

Рис. 1. Пример процесса передачи сообщения от узла-источника к базовой станции

Следствие из теоремы косинусов. Мощность передачи через ретранслятор k (рис.1) меньше затрачиваемой мощности передачи сообщения напрямую от узла-источника к базовой станции, при условии, что угол $\beta \in (\pi/2;\pi]$; мощность передачи через ретранслятор равна мощности передачи сообщения напрямую от узла-источника к базовой станции, при условии, что угол $\beta = \pi/2$, в ином случае наименьшая мощность будет затрачена при передаче напрямую от узла-источника к базовой станции.

В работе определены критерии для выбора оптимального маршрута передачи сообщения в беспроводных сенсорных сетях, учитывающие физические характеристики сенсорных устройств в сельскохозяйственных приложениях, основанных на технологии беспроводной связи. Получено следствие из теоремы косинусов, позволяющее определить маршрут передачи сообщения от узла-источника к базовой станции, при котором затрачивается минимальная мощность. Выявлено, что если угол, образующийся между расстояниями передачи сообщения через ретранслятор, больше 90°, то выгоднее осуществлять передачу при помощи ретранслятора, а не напрямую от узла-источника к базовой станции. Методика эксперимента подтверждена численными результатами.

СПИСОК ЛИТЕРАТУРЫ

1. Якунин С.В., Якунина А.В., Семернина Ю.В. Финансовое посредничество банков в цифровую эпоху // Вестник Саратовского государственного социально-экономического университета. 2019. №2 (76). URL: https://cyberleninka.ru/article/n/finansovoe-posrednichestvo-bankov-v-tsifrovuyu-epohu (дата обращения: 07.01.2020)
2. Н. П. Петрова, Г. А. Бондарева Цифровизация и цифровые технологии в образовании // МНКО. 2019. №5 (78) – С. 353-355.
3. рименение цифровых технологий для повышения эффективности сельского хозяйства // URL: https://files.data-economy.ru/cipr/mts_astashov.pdf (дата обращения: 20.12.2019).
4. Bogatyrev,V., Bogatyrev,S., Bogatyrev,A.: ”Model and Interaction Efficiency of Computer Nodes Based on Transfer Reservation at Multipath Routing”. 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2019, pp. 1-4. doi: 10.1109/WECONF.2019.8840647
5. Bogatyrev, A., Bogatyrev, S., Bogatyrev, V.: Analysis of the Timeliness of Redundant Service in the System of the Parallel-Series Connection of Nodes with Unlimited Queues. 2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). 2018, pp. 1-4
6. Астахова, Т. Н., Верзун, Н. А., Касаткин, В. В., Колбанев, М. О., Шамин, А. А. (2019). Исследование моделей связности сенсорных сетей. Информационно-управляющие системы, (5) – С. 38-50.
7. Грищенко В. И., Ладыженский Ю. В. Использование сетевых процессоров для решения задачи маршрутизации в компьютерных сетях. – 2007

УДК 004.9, 658.512

АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ УПРАВЛЕНИЯ ПРОЦЕССАМИ РАЗВИТИЯ ПЕРСОНАЛА ОПЕРАТИВНО-ДИСПЕТЧЕРСКИХ СЛУЖБ ГАЗОТРАНСПОРТНОЙ СИСТЕМЫ

Колбанев Михаил Олегович, Коршунов Игорь Львович
Санкт-Петербургский государственный экономический университет
ул.Садовая, 21, Санкт-Петербург, 191023, Россия
e-mail: kil53@mail.ru

Аннотация. Цифровизация активно внедряется во все сферы экономики. Возможности современных информационных технологий позволяют разрабатывать и применять высокотехнологичные тренажеры в процессе профессиональной подготовки оперативно-диспетчерского персонала управления сложными автоматизированными системами, в частности газотранспортными системами. В свою очередь, это ведет к изменению требований к составу и методикам формирования профессиональных компетенций, их учету и построению индивидуальной траектории развития для каждого сотрудника. Предлагается создать программный комплекс для управления процессами развития персонала оперативно-диспетчерских служб газотранспортной

системы, который позволит оценить способности каждого сотрудника в полном объеме выполнять свои функциональные обязанности, выявить слабые места в компетенциях каждого сотрудника и построить траекторию его обучения с целью ликвидации выявленных пробелов.

Ключевые слова: Газотранспортная система, специалист по оперативно-диспетчерскому управлению нефтегазовой отрасли, профессиональные компетенции, программный комплекс.

ARCHITECTURE OF THE SOFTWARE COMPLEX FOR MANAGING THE PROCESSES OF PERSONNEL DEVELOPMENT OF OPERATIONAL DISPATCH SERVICES GAS TRANSPORTATION SYSTEM

Kolbanev Michail, Korshunov Igor
The St.Petersburg state university of economics
21 Sadovaya street, St.Petersburg,191023, Russian
e-mail: kil53@mail.ru

Abstract. Digitalization is being actively implemented in all areas of the economy. The capabilities of modern information technologies allow us to develop and apply high-tech simulators in the process of professional training of operational dispatcher personnel for managing complex automated systems, in particular gas transportation systems. In turn, this leads to changes in the requirements for the composition and methods of forming professional competencies, accounting for them, and building an individual development trajectory for each employee. It is proposed to create a software package for managing the development of personnel of operational dispatching services of the gas transportation system, which will allow assessing the ability of each employee to fully perform their functional duties, identify weaknesses in the competence of each employee and build a trajectory of their training in order to eliminate the identified gaps.

Keywords: Gas transportation system, specialist in operational and dispatching management of the oil and gas industry, professional competencies, software package

Проектирование комплексных сложных технических систем – гибких автоматизированных производств (ГАП) является поэтапным процессом, который включает подготовку технического задания, выбор технического предложения, создание эскизного и рабочего проектов, обобщенный экономический расчет эффективности проекта и практическое применение данного проекта в производстве [1]. Как известно, в настоящее время для обеспечения всех проектных работ конструкторского, функционального назначения и экономического обоснования выбранных проектов на этапах разработки ГАП используются технические, программные и информационные инструментарии [2]. Но, экономическое обоснование и определение экономической эффективности проектных работ требуются почти на каждом этапе, начиная от правильного выбора инструментарий САПР, прототипов проекта, их сравнительного конструкторского, функционального и качественного анализа, при инженерных расчетах, создании 2-х и 3-х мерных конструкторских проектах, проведении компьютерных экспериментов, лабораторных и производственных испытаниях.

Главной целью любой газотранспортной системы (ГТС), связывающей месторождения газа с потребителями, заключается в удовлетворении имеющегося спроса на газ. Эта цель должна достигаться в реальном масштабе времени в условиях:

- колебаний спроса на газ, вызванных природными, экономическими или другими причинами,
- изменения текущих условий функционирования ГТС из-за планового или аварийного вывода из эксплуатации газопроводов различного типа, газораспределительных станций, газорегуляторных пунктов и других технологических объектов;
- пересмотра моделей бизнеса поставок природного газа.

Выбор безопасных режимов работы ГТС, гарантирующих удовлетворение спроса и обеспечивающих достижение оптимальных значений экологических, экономических и энергетических критериев с учетом всего набора факторов, влияющих на процессы работы ГТС, является главной задачей персонала оперативно-диспетчерской служб.

Профессиональные компетенции соответствующих сотрудников определены профессиональным стандартом «Специалист по оперативно-диспетчерскому управлению нефтегазовой отрасли» [1], а также отраслевыми и корпоративными документами. В самом общем плане эти компетенции должны обеспечивать выбор таких режимов работы ГТС, которые соответствуют планам доставки газа до потребителей. Для этого необходимо управлять потоками углеводородного сырья в трубопроводном транспорте, контролировать баланс газа, передаваемого по ГТС, следить за качеством газа. Поскольку ГТС представляет собой систему, распределенную на больших пространствах, важной компетенцией является ведение нормативно-справочной информации, сопровождающей все решения, в привязке к картам различного назначения.

Вектор развития нефтегазовой отрасли характеризуется сегодня широкой цифровизацией всех процессов деятельности оперативно-диспетчерского персонала на базе технологий третьей платформы информатизации. В первую очередь, к таким технологиям относятся интернет вещей, мобильный широкополосный доступ к инфокоммуникационным услугам, большие данные, геоинформационные технологии и, построенные на их основе, предметно ориентированные технологии, такие как SCADA-системы, АРМы диспетчеров, информационно-измерительные технологии и другие.

В последнее время на многих ГТС внедряется программно-вычислительный комплекс нестационарного моделирования, оптимизации и мониторинга газотранспортных систем «ВОЛНА» [2], который предназначен для использования в газотранспортных обществах в целях поддержки принятия диспетчерских решений по управлению ГТС и позволяет:

– моделировать стационарные и нестационарные режимы работы ГТС и по заданному сценарию управляющих воздействий проводить расчеты в реальном времени;

– рассчитывать режимы работы компрессорных цехов и параметров потока газа в линейных частях магистрального газопровода с учетом схемы подключения и индивидуальных характеристик газоперекачивающих агрегатов;

– оптимизировать режимы газотранспортной системы на заданную производительность или максимальную пропускную способность с учетом технологических ограничений;

– рассчитывать потери газа при разрыве газопровода с учетом управляющих воздействий диспетчера по локализации аварии;

– рассчитывать размеры опасных зон поражения при авариях с разрывами газопровода и нанесение их на карту;

– рассчитывать движение очистных и диагностических снарядов по газопроводу с учетом рельефа местности и управляющих воздействий диспетчера, отображать на технологической схеме и географической карте текущее расчетное положение снаряда;

– осуществлять мониторинг показателей энергетической эффективности функционирования объектов ГТС;

– осуществлять мониторинг выбросов загрязняющих веществ и парниковых газов в атмосферу при работе ГТС.

В целом, при формировании компетенций персонала оперативно-диспетчерских служб ГТС [3-5] необходимо учитывать следующие обстоятельства:

– высокая ответственность при принятии управленческих решений;

– чрезвычайно сложный объект управления, который включает большое количество разнородных технологических элементов, распределенных на больших пространствах;

– цифровизация системы управления, которая использует новые самые современные информационные технологии;

– трансформация моделей деятельности газотранспортных предприятий в целом и оперативно-диспетчерских служб, в частности, и др.

Все эти обстоятельства оказывают определяющее влияние на изменение требований к составу и методикам формирования профессиональных компетенций, которые должны теперь охватывать не только знания и умения, связные с взаимодействием с потребителями, функционированием трубопроводного транспорта, контролем за всеми процессами и отображением достигнутых результатов в информационных и геоинформационных системах, но и цифровые компетенции, позволяющие эффективно использовать новый цифровой инструментарий управления физическими оборудованием и процессами.

Достигнуть нужных качественных показателей работы персонала можно путем создания программного комплекса для управления процессами развития персонала оперативно-диспетчерских служб газотранспортной системы. Архитектура программного комплекса должна содержать три взаимосвязанных уровня:

– уровень данных;

– логический уровень, на котором реализуется логика моделей деятельности;

– уровень представления, отвечает за пользовательский интерфейс.

Такое разделение обеспечит программному комплексу безопасность, масштабируемость и высокую производительность, позволит обслуживать и модернизировать программные уровни независимо друг от друга, упростит внедрение комплекса в более общие системы, такие как роботизированные тренажеры.

Определяющее значение имеет уровнь данных, где обеспечивается сохранение информации, необходимой для реализации процессов деятельности на логическом и процессов взаимодействия с пользователями на представительском уровне. Для систематизации информации здесь необходимо организовать следующие базы данных:

– о компетенциях персонала оперативно-диспетчерских служб ГТС;

– об индикаторах компетенций;

– о профилях компетенций;

– о тестах для оценки компетенций сотрудников;

– о результатах тестирования по компетенциям;

– о сценариях проведения интервью по компетенциям;

– о сценариях решения задач по управлению режимами транспорта газа в штатных и нештатных ситуациях;

– о результаты интервью по компетенциям;

– о документах для самоподготовки;

– о программах обучения (подготовки) по всем уровням и видам компетенций

– об индивидуальных планах подготовки и маршрутах развития компетенций.

Создаваемый программный комплекс позволит оценить способности каждого сотрудника в полном объеме выполнять свои функциональные обязанности, выявить слабые места в компетенциях каждого сотрудника и построить траекторию его обучения с целью ликвидации выявленных пробелов. Проектный подход, реализуемый в рамках выполнения этих работ, позволяет учесть особенности газотранспортной отрасли, научные достижения в области управления качеством, а также возможности современных информационных технологий, которые являются основой цифровизации экономической деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Министерства труда и социальной защиты РФ от 26 декабря 2014 г. N 1177н.
2. https://reestr.minsvyaz.ru/reestr/112248/
3. Багдасарова Ю.А. Использование виртуальных тренажерных комплексов при формировании профессионально-экологической компетентности у будущих специалистов трубопроводного транспорта // Вестник Самар. гос. техн. ун-та. Сер. Психолого-педагогические науки. – 2013. – № 1 (19). – С. 11-19.
4. Технологии управления развитием персонала: Учебник/ под ред. Карпова А.В. – М.: Проспект, 2018 – 408 с.
5. Маслова В.М. Управление персоналом: учебник и практикум для академического бакалавра / В.М.Маслова. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2016. – 492 с.

УДК 681.3

О СКОРИНГОВОЙ СИСТЕМЕ ОЦЕНКИ КРЕДИТОСПОСОБНОСТИ

Лемешев Михаил Сергеевич, Головкин Юрий Борисович
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: lm1998@bk.ru, comparif@rambler.ru

Аннотация. Рассматриваются особенности реализации скоринговой системы оценки кредитоспособности для оптимизации процесса кредитования в банковской организации. Описывается формирование скоринговой модели для кредитного скоринга. Обсуждается алгоритм формирования скоринговой модели.

Ключевые слова: кредитный скоринг; скоринговая модель; скоринговая система; оценка кредитоспособности.

DESCRIPTION OF THE SCORING SYSTEM FOR ASSESSING CREDIT CAPABILITY

Lemeshev Mikhail, Golovkin Yury
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mails: lm1998@bk.ru, comparif@rambler.ru

Abstract. In article are reviewed features of the implementation of a scoring system for assessing creditworthiness to optimize the lending process in a banking organization. Describes the formation of a scoring model for credit scoring. Algorithm for the creating of a scoring model is discussed.

Keywords: credit scoring; scoring model; scoring system; credit rating.

Введение. Банковская сфера деятельности на данный момент контактирует с каждым живущим в условиях глобализации человеком. Таким образом, масштабы данной сферы растут, а кредитное дело, как часть сферы, также является областью, актуальность которой в настоящее время весьма велика. Продолжающийся рост рынка кредитования физических лиц неизбежно влечет за собой принятие дополнительных кредитных рисков как на отдельное кредитное учреждение, так и на банковскую систему в целом.

Одним из основных рисков является не возврат заемщиком суммы кредита в полном объеме или в указанный срок, т.е. нарушение обязательств. Оценка кредитных рисков потенциального заемщика называется кредитным скорингом (от англ. creditscoring). Говоря о кредитном скоринге, как правило, имеют в виду анализ рисков по кредитованию физических лиц, хотя методы оценки надежности организаций также существуют [2, с.22].

Система скоринга представляет собой методику, главной целью которой является изучение и применение на практике данных, полученных в области кредитных взаимодействий между банковской организацией и её пользователями в течение определенного времени. На современном этапе развития банковской системы оценка кредитоспособности заёмщика является одним из важнейших этапов процесса кредитования для банка. Оценка кредитоспособности для физического лица помогает определить его платёжеспособность [1, с. 14]. Эта информация необходима для того, чтобы оценить кредитоспособность клиента и взвесить возможные риски, связанные с его кредитованием. Полученные результаты представляются в виде балльного показателя, позволяющего определить целевую группу заемщиков, к которой можно отнести рассматриваемого клиента. В самой простой и наиболее важной с практической точки зрения ситуации данный показатель выдает в итоге два варианта: «клиент кредитоспособен» (одобрить займ) или «клиент некредитоспособен» (отказ в выдаче займа). При этом, и потребительский опыт, и потребительские ожидания, и, как следствие, потребительское поведение, несут в себе значительный запрос на инновации именно в финансовом рынке, с которым в ежедневном режиме

прямо или косвенно сталкивается каждый человек (потребитель) и хозяйствующий субъект, что, на самом деле является в т.ч. отражением уровня финансовой грамотности населения [3, с. 33].

Основой скоринга выступает так называемая скоринговая модель, это статистическая или математическая модель, сопоставляющая данные о клиенте со степенью риска в сфере кредитования, полученная в результате работы с предыдущими заемщиками. Таким образом, скоринговые системы дают возможность банковским организациям на основе сведений о возвращении заемных средств предыдущими заемщиками установить размер вероятности, с которой нынешний клиент, желающий получить займ, вернет его в назначенное время. Эта модель первоначально формируется за счет описания некоторых критериев заемщика. На самом деле, при создании скоринговых моделей характеристики клиента в области кредитоспособности определяются методом вычленения из их состава реальных случаев, которые, согласно мнению банковской организации, оказывают влияние на процесс оценки кредитоспособности. К примеру, свойство платежеспособности заемщика может быть оценено путем аналитических действий в отношении его настоящего дохода, активов, должности, места постоянной работы и прочих показателей. К тому же, деятельность показателей платежеспособности в течение определенного срока обладает постоянным характером, а итоги кредитных операций не зависят друг от друга, благодаря чему появляется возможность оценки вероятных событий в будущем, которые имеют отношение к кредитоспособности. Чтобы оценить показатели платежеспособности своего потенциального клиента, банковские организации применяют различные источники данных, главными из которых считаются следующие:

– личные статистические сведения об одобрении кредитов и о возврате заемных средств прошлыми клиентами;
– информация о кредитной истории;
– информация от службы безопасности;
– сведения, передаваемые потенциальным заемщиком, на получение кредитных средств.

На сегодняшний день наряду с данными о потенциальных заемщиках, которые банк может получить самостоятельно из кредитной заявки, активно используются сведения, которые направляют кредитные организации. Эти организации помогают всем кредитующим органам устранить асимметрию информации относительно настоящих и будущих клиентов, обеспечивая тем самым более эффективный кредитный скоринг, что улучшает уровень безопасности в финансовом отношении, снижает операционные расходы в сфере предоставления кредитов для малого и среднего бизнеса.

Скоринг подбирает факторы, которые максимально отображают кредитоспособность, следовательно, необходимо удостовериться в верном выборе данных характеристик и выявить определяющие их удельные значения. К тому же, главное свойство скоринга это индивидуальность, следовательно, его методы должны разрабатываться исходя из особенностей, таких как демографические показатели, социальные условия, экономические показатели и т. п. Внедряя скоринговую систему, банку необходимо выполнить аудит существующей модели и при потребности усовершенствовать систему факторов и их удельный вес в балльном отображении.

Реализация алгоритма скоринговой модели состоит из применения различных математических и статистических методов, каждый из которых имеет свои преимущества и недостатки. В основном, при построении именно кредитных скоринговых моделей используют линейную или логистическую регрессию, дискриминантный анализ, нейронные сети, а также деревья решений. Регрессии, как линейные, так и логистические, достаточно распространены в кредитном скоринге. Поскольку перед банком стоит задача отобрать лучших заемщиков, не обязательно действовать в рамках задачи классификации: вместо нее может быть реализована задача ранжирования, для которой подходят и линейная, и логистическая регрессии (так как могут предсказывать вероятность принадлежности к одному из бинарных классов, по которой и будут упорядочены потенциальные заемщики) [2, с. 23].

Для формирования скоринговой модели необходимо иметь репрезентативную выборку данных, основанную на данных заемщиков. Объём выборки может разниться в зависимости от модели и методах ее построения, но для реализации статистически правильной модели потребуется несколько тысяч записей. К тому же, для составления точной скоринговой модели необходимо учитывать качество данных и их соответствие к сопоставляемой модели. Иначе говоря, выборка должна быть актуальной по временным рамкам и характеру данных.

За счет проведения аналитических мероприятий в отношении прошлых сведений происходит формирование средних показателей по предварительно установленным категориям факторов, которые могут описывать, к примеру: семейное положение, возраст, образование, профессию, место работы, степень доходов возможного клиента и т.д.

Доработав эти показатели, банковская организация выводит интегрированный коэффициент в любой единице измерения, который участвует в сравнении с заранее определенными пороговыми показателями и позволяет отнести заемщика к той или иной целевой группе. А также появляется возможность внести изменения аналогичным способом на основании внутренних норм банковской организации в такие критерии, как: срок, объем займа, процентная ставка.

Таким образом, полученная скоринговая система на основе разработанной модели позволяет оценить определенного заемщика с помощью системы отбора ключевых финансовых показателей, основанной на подсчете конечной переменной, необходимой для оценки кредитоспособности лица и перевода решения в бинарную систему – кредитоспособен или некредитоспособен.

Заключение. Хотелось бы отметить, что в настоящее время эта практика стала неотъемлемой, и почти каждый банк имеет собственную методику оценки кредитоспособности, благодаря которой принимается решение о предоставлении услуг кредитования. Данное решение позволяет автоматизировать процесс кредитования, а также решает проблему предвзятости, тем самым оптимизируя банковские операции, а также сокращает время обработки заявок на предоставление кредита и дает возможность банкам проводить свою кредитную политику централизованно, обеспечивая дополнительную защиту финансовых организаций от мошенничества. Как правило, внедрение скоринговой системы в банковские процессы может гарантировать банку весомую выгоду, а именно, снижение издержек и увеличение доходности, снизив при этом операционные риски.

СПИСОК ЛИТЕРАТУРЫ

1. Голубенко Н. А. Оценка кредитоспособности клиентов банка / Н. А. Голубенко, Е. А. Маякова // Скиф. – 2019. – № 1 (29). – С. 12-17.
2. Кочеткова В.В. Обзор методов кредитного скоринга / К.Д. Ефремова, В.В. Кочеткова // Juvenis scientia. – 2017. – №6. – С. 22-26.
3. Модели цифровизации экономической деятельности. – СПб.: Изд-во СПбГЭУ, 2019. – 179 с.

УДК 004.9, 338.2

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДИК ОЦЕНКИ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ СОЗДАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Микадзе Сергей Юрьевич, Митенков Антон Валентинович
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: mitenkov.anton@bk.ru

Аннотация. Рассматриваются существующие методики оценки экономического эффекта для анализа проектов создания ИТ-проектов (информационных систем).

Ключевые слова: методы оценки, экономическая эффективность; информационные системы; оценка эффективности.

COMPARATIVE ANALYSIS OF THE EXISTING METHODS OF ASSESSING THE ECONOMIC EFFECTIVENESS OF CREATING AN INFORMATION DATA SYSTEM

Mikadze Sergei, Mitenkov Anton
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: mitenkov.anton@bk.ru

Abstract. The existing methods of assessing the economic effect used for analyzing projects for creating IT-projects (information systems).

Keywords: methods of assessing, economic effectiveness, information data systems, evaluating effectiveness.

Информационные технологии-неотъемлемая часть современного бизнеса. Информационные технологии, в частности информационные системы, увеличивают конкурентоспособность предприятий через оптимизацию принятия решений управленческих задач с помощью интеллектуальных систем, снижение затрат на производство, улучшение работы с клиентами, составление аналитической документации [1]. С другой стороны, внедрение современных ИТ-решений процесс дорогостоящий и длительный, вынуждающий предприятие мобилизовать финансовые, кадровые и материальные ресурсы. При этом капитальные инвестиции не гарант, что внедрения будут удачными. Большая стоимость и высокий риск являются главными проблемами проектирования и внедрения ИТ-решений. Для этого и применяются методы оценки экономического эффекта информационных систем для рационального выбора предлагаемых проектов [2].

Экономическая эффективность оценивается сопоставлением показателей экономической результативности информационной системы (подсистемы или проекта) со стоимостными затратами на реализацию этой системы (подсистемы или проекта). Для корректного оценивания необходимо правильно сопоставлять временные промежутки оценивания экономического результата и промежутка, в течение которого оценивались затраты на проектирование и развитие системы [3].

Методики оценки экономической эффективности можно разделить на группы: традиционные, контроля затрат, управления рисками, современные.

Традиционные методики основываются на инвестиционном анализе. Внедрение ИТ-решения оценивается с точки зрения рентабельности инвестиционного проекта, рассчитывая дисконтируемые денежные потоки, которые будут образоваться в ходе реализации проекта. Методы базируются на традиционных подходах к финансовому расчету экономической эффективности и к оценке риска. Основное преимущество традиционных методов — это доступность в понимании руководящих должностей критериев оценки, т. к. они повсеместно используются в оценке различных инвестиционных проектов. Недостатком является то, что критерии подразумевают конкретику и точность в расчете денежных потоков, что для инновационных ИТ-проектов проблематично.

Основные показателями этой группы являются: простой срок окупаемости-PP (Payback Period), чистая приведенная стоимость- NVP (Net Present Value), индекс прибыльности -PI (Profitability Index), внутренняя норма

рентабельности – IRR (Internal Rate of Return), экономическая добавленная стоимость- EVA (Economic Value Added) [4].

Простой срок окупаемости подразумевает расчет срока окупаемости инвестиций. Метод расчета чистой приведенной стоимости проекта позволяет оценить его дисконтированную стоимость, определяемую как разность между дисконтированными ожидаемыми поступлениями от реализации проекта и дисконтированными затратами на его осуществление. Индекс прибыльности показывает дисконтируемую стоимость денежных поступлений от проекта в расчете на единицу вложения. Метод определения внутренней нормы доходности предназначен для установления нормы рентабельности, т. е. нахождение максимальной ставки дисконтирования, при которой прибыль будет равна нулю. Метод расчета экономической добавленной стоимости рассчитывается как разность между операционной прибылью за вычетом налогов, но до вычета процентов, и произведением средневзвешенной стоимости капитала на величину инвестиций, осуществленных к началу периода.

Следующая группа методик — это методы контроля затрат. Методы основаны на оценивании функционирования и процесса внедрения информационных систем. Методы контроля затрат используют как замену традиционным методам. Они учитывают затраты на проект и выгоды от реализации проекта, которые представляются как экономия средств. Преимуществом методов является базирование на затратах что позволяет иметь более достоверную и понятную информацию о проекте. При внедрении информационных систем проблематично установить связь с полученным результатом. Недостатком является то, затраты не отражают в полной мере эффективность ИТ-решения на начальных этапах.

Примерами данной группы методов являются метод функционально-стоимостного анализа и метод исследования затратно-временных показателей работы систем.

Метод функционально-стоимостного анализа (ФСА) предусматривается выполнение дифференцированной калькуляция и распределения проектных затрат по видам деятельности, продукции и функции предприятия. Такой подход позволяет установить связь между элементами себестоимости производимых предприятием товаров и услуг, используемыми производственными процессами и применяемыми технологическими решениями. Применительно к оценке эффективности информационных систем, метод ФСА опирается на построение бизнес-модели предприятия «как есть» и «как надо», и последующую оценку того, к каким изменениям основных бизнес-процессов приведет внедрение проектируемой системы [4].

Метод исследования затратно-временных показателей работы систем основан на широко известных сетевых моделях планирования и управления проектами (PERT/Cost-анализе, принципах декомпозиции работ), а также разработке различных сценариев развития проектов, что позволяет оценить эффективность внедрения информационной системы на уровне отдельных операций или групп операций уже на начальных стадиях реализации проекта. В рамках концепции затратно-временных показателей эффективность может быть оценена как на уровне различных стадий, так и на уровне отдельных операций проекта внедрения информационной системы на основе двух ключевых показателей: соотношение объема запланированных и выполненных работ, а также запланированных и фактических затратах на проведение проекта.

Методики, основанные на управления риска, оценивают вероятность возникновения рисков при реализации ИТ-проектов. Методики используют статистические и математические модели, позволяющие оценить будущий эффект ИТ-решения, на базе которого сравнивается эффективность альтернативные проектов, схожих по показателям. Метод пока не распространён в практике.

Современные методы основываются на совокупном подходе анализа финансовых и не финансовых факторов. Методики представляют собой системы элементов, которые рассматривают различные аспекты, такие как влияние на бизнес-процессы, риски, адаптивность, привязка к целям предприятия, архитектура. Преимущество этих методик заключается в том, что они адаптируются в пределах своих специализаций и охватывают все стороны влияния ИТ-проекта на предприятие, начиная от уменьшения затрат или повышения сервиса, до влияние информационной системы на текущую архитектуру. Недостатком является необходимость в большом количестве информации для рассмотрения заданных аспектов. Также необходимо интегрировать разрозненную информацию в общую систему в виде, котором она будет доступна не только для людей, вовлеченные в сферы деятельности, связанные с ней. Примерами современных методов являются TEI, REJ, TVO.

Методика расчета совокупного экономического эффекта-TEI (Total Economic Impact) предназначена для поддержки принятия решений, снижения рисков и обеспечения «гибкости». Методику используют для анализа вариантов внедрения какого-то определенного компонента, при анализе двух различных сценариев, если они сопряжены с построением инфраструктуры или реализацией корпоративных проектов, чьи положительные и отрицательные стороны оценить сложно.

Метод быстрого экономического обоснования- REJ (Rapid Economic Justification) предусматривает конкретизацию модели общей стоимости владения за счет установления соответствия между расходами на ИТ и приоритетами бизнеса. Методика REJ является наиболее сложным и комплексным инструментом оценки проекта внедрения ИТ-решения. Но она не может эффективно оценить проекты преобразования всей инфраструктуры.

Расчет совокупной ценности возможностей- TVO (Total Value of Opportunities) отражает большое количество экономических показателей и способна адаптироваться к различным уровням управления. Модель позволяет собрать большой объем информации, т. к. является интегрирующей платформой, которая способна объединить результаты разных методик в одну систему [4].

Таким образом, рассмотрев различные методики можно сделать вывод, что не существует универсального метода оценки. Каждый метод обладает своими преимуществами и недостатками. ИТ-решения, в частности информационные

системы, требуют инвестиций для реализации и сопутствующее обслуживание, влияя на бизнес-процессы компании на разных уровнях управления. Поэтому, для более детального и рационального анализа ИТ-проекта необходимо применять совокупность методов, критериев, показателей, которые будут определяться спецификой внедряемого компонента или решения и спецификой предприятием, в которое и будет внедряться решение.

СПИСОК ЛИТЕРАТУРЫ

1. Информационный менеджмент: учебное пособие / И.Л. Андреевский, Р.В. Соколов. – СПб.: Издательство СПБбГЭУ, 2016.-127 с.
2. Проектирование и эксплуатация информационных систем: учебник/ Р.В. Соколов, И.Л. Андреевский. – СПб.: Издательство СПбГЭУ, 2017.-382 с.
3. Экономика информационных систем: учебник пособие для вузов / А.Л. Рыжко, Н.А. Рыжко, Н.М. Лобанова, Е.О. Кучинская.- 2-е изд.,испр.и доп..-Москва: Издательство Юрайт, 2020.- 176 с. – (Высшее образование).- Текст: непосредственный.
4. Методики оценки эффективности информационных систем и информационных технологий в бизнесе: учебное пособие/А.Б. Анисифов, Л.О.Анисифорова.-СПб.: Издательсво СПбГПУ,2014.-97 с.

УДК 004

ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ЭКОНОМИЧЕСКУЮ ДЕЯТЕЛЬНОСТЬ

Нестеренко Евгения Сергеевна[1], Верзун Наталья Аркадьевна[2], Колбанёв Михаил Олегович[2]
[1] Крымский федеральный университет им. В.И. Вернадского
Академика Вернадского пр., 4, Симферополь, Республика Крым, 295007, Россия
[2] Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: nesterenko.e.s@yandex.ru, verzun.n@unecon.ru, mokolbanev@mail.ru

Аннотация. Рассматривается влияние цифровых технологий на человеческую деятельность. Отмечается, что понятие «цифровая технология» относится не только к информационной по Винеру, то есть управленческой стороне информационных процессов, но и к их материальной природе. Поэтому, цифровая экономика предусматривает информатизацию не только управления, но и других компонент, составляющих экономическую деятельность: производство, распределение, обмен, потребление. Внедрение цифровых технологий в отрасли экономики разрушает существующие способы создания, потребления продукции и услуг, и создает новые. Цифровые технологии влияют на развитие многих отраслей и существенно меняют их облик. В докладе рассматриваются примеры подобного влияния.

Ключевые слова: цифровые технологии; цифровая экономика; цифровая трансформация экономики.

IMPACT OF DIGITAL TECHNOLOGIES ON ECONOMIC ACTIVITY

Nesterenko Evgeny[1], Verzun Natalya[2], Kolbanev Mikhail[2]
[1] V.I. Vernadsky Crimean Federal University
4 Vernadskogo Av, Simferopol, Republic of Crimea, 295007, Russia
[2] Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mails: nesterenko.e.s@yandex.ru, verzun.n@unecon.ru, mokolbanev@mail.ru

Abstract. The influence of digital technologies on human activity is considered. It is noted that the concept of "digital technology" refers not only to information on Wiener, that is, the management side of information processes, but also to their material nature. Therefore, the digital economy provides Informatization not only of management, but also of other components of economic activity: production, distribution, exchange, and consumption. The introduction of digital technologies in the economy destroys the existing ways of creating and consuming products and services, and creates new ones. Digital technologies affect the development of many industries and significantly change their appearance. The report examines examples of such influence.

Keywords: digital technologies; digital economy; digital transformation of the economy.

Мир сегодня переживает глобальную цифровую трансформацию. Развивающиеся «цифровой мир», «цифровое общество», «цифровая экономика», «цифровая безопасность», «цифровая деятельность» – становятся уже не только предметом научного исследования и философского осмысления, но и политическими целями правительств, и практическими программами, финансируемыми государствами и бизнесом.

Мы живем в эпоху компьютерных технологий, используемых нами повсеместно. Поэтому экономистам нужно знать цифровые технологии и уметь правильно их применять. Исследование, проведенное глобальной экспертной группой, объединяющей специалистов McKinsey [1], доказывает, те компании, которые активно используют цифровые технологии, развиваются в два раза быстрее, экспортируют вдвое больше продуктов и услуг, а также создают более чем в два раза больше рабочих мест.

Отечественные эксперты сходятся во мнении [2], что для достижения более высокого уровня развития экономики, государству необходимо стимулировать те компании, которые используют цифровые технологии и принимают участие в их разработке, а также мотивировать другие компании на внедрение в свою деятельность мобильных технологий, бизнес-аналитику, цифровые платежные системы и др.

Понятие «цифровая технология» относится не только к информационной по Винеру, то есть управленческой стороне информационных процессов, но и к их материальной (т.е. энергетической) природе. Поэтому, цифровая экономика предусматривает информатизацию не только управления, но и всех других компонентов, составляющих экономическую деятельность: производство, распределение, обмен, потребление [3].

Методология кибернетики нацелена на автоматизацию процессов управления на основе субъект-объектного подхода, а методология цифровой экономики ориентирована на автоматизацию любых экономических процессов на основе сетевого подхода. Главный признак цифровой экономики – это «глубокое проникновение компьютера» – т. е. цифровизация не только управления, но и самого процесса материальной деятельности во всех областях жизни, включая экономическую.

Внедрение цифровых технологий в отрасли экономики разрушает существующие способы создания, потребления продукции и услуг, и создает новые. Можно привести следующие примеры дестабилизации традиционных отраслей экономики под влиянием цифровых технологий:

- услуги туристических агентств заменяются online-бронированием и электронными билетами,
- работа отделений банков переходит в цифровой (мобильный) банкинг,
- розничные магазины вытесняются интернет-магазинами, виртуальными складами и е-доставкой,
- офисы оказания государственных услуг замещаются единым online-порталом госуслуг,
- традиционная медицина заменяется на телемедицину с применением электронных карт истории болезни,
- система охраны – на системы видеонаблюдения.

Внедрение цифровых технологий влияет на развитие многих отраслей и существенно меняет их облик [4]. В докладе рассматриваются примеры подобного влияния, в частности:

В промышленности: внедрение цифровых технологий позволяет увеличить эффективность загрузки производственных мощностей, повышает конкурентоспособность продукции.

В сельском хозяйстве: автоматизация сельскохозяйственных процессов с помощью создания виртуальной (цифровой) модели всего цикла производства и взаимосвязанных звеньев цепочки создания стоимости, и с математической точностью планирования графика работ, принятия экстренных мер для предотвращения потерь в случае зафиксированной угрозы, прогнозирование возможной урожайности, себестоимости производства и прибыли.

В логистике и транспорте: повышение эффективности, производительности и безопасности транспорта. Уменьшение его негативного воздействия на окружающую среду.

В торговле: развитие прямой модели B2C-торговли через онлайн-канал (например, P&G). Упрощение координации и управления цепочкой поставок.

В строительстве: создание виртуальной модели зданий и сооружений. Возможность задания индивидуальных параметров объекта. Получение качественной проектной документации. Быстрое выявление и исправление ошибок и неточностей изменением параметров. Экспериментальное обследование модели при тех или иных условиях. Управление и контроль возведения объекта на всех этапах строительства. Контроль эксплуатации объекта непрерывно с его исходной проектной документацией. Пользование информационной моделью разными подрядными организациями (для создания водопроводных систем, вентиляционных систем, расчетно-экономических изысканий и др.).

В жилищно-коммунальном хозяйстве: формирование единого информационного пространство отрасли, создание ИТ-системы информирования клиентов и обработки их данных, внедрение мобильных и облачных решений, включая средства аналитики больших данных.

Следует отметить, что внедрение цифровых технологий приведет к существенному росту развития отраслей экономики и главная причина этого роста – повышение уровня эффективности производства. Автоматизация и роботизация производств сопровождаются кардинальным обновлением основных средств, приводят к уменьшению вклада такого фактора производства как труд в экономический рост, при последовательном росте вклада капитала практически по всем отраслям экономики.

Формирование цифровой инфраструктуры прежде всего может повлиять на увеличение темпов роста финансового, транспортного и строительного секторов. Также цифровые технологии позволят повысить качество услуг и доступность в социальной сфере, в образовании, здравоохранении, финансовой сфере, жилищно-коммунальном хозяйстве. Следовательно, внедрение цифровых технологий кардинальным образом меняют устройство глобальной экономической системы, саму операционную модель компаний, возможности потребителей, структуру отраслей, роль государства, уменьшает производственные затраты и выявляет новые потенциалы на рынке [5].

СПИСОК ЛИТЕРАТУРЫ

1. Цифровая Россия: новая реальность // McKinsey. – 2017 [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/images/c/c2/Digital-Russia-report.pdf (дата обращения: 02.05.2020).
2. Субботина Т.А. Роль цифровых технологий в экономике современной России // Beneficium. – 2018. – №3 (28). – С. 74–79.
3. Воробьев А.И., Колбанёв М.О. Инфокоммуникация и цифровая экономика // Аллея науки. – 2017. – Т 1. – № 1. – С. 791–799.
4. Нестеренко Е. С. К вопросу о значении цифровизации в трансформации экономики государства // Актуальные проблемы экономики и менеджмента. – 2020. – № 6 (26).
5. Программа «Цифровая экономика Российской Федерации», 2017. 87 с.

УДК 004.89

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОГНОЗИРОВАНИЯ ЭФФЕКТИВНОСТИ ИНВЕСТИЦИОННЫХ ПРОЕКТОВ

Пономарев Иван Глебович, Верзун Наталья Аркадьевна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: nokojoy@yandex.ru, verzun.n@unecon.ru

Аннотация. Рассматриваются возможности применения систем искусственного интеллекта для оценки и прогнозирования эффективности инвестиционных проектов. Описываются особенности задач, связанных с проведением подобной оценки. Проводится обзор решений, основанных на искусственном интеллекте и возможных для применения в целях прогнозирования эффективности инвестпроектов.

Ключевые слова: искусственный интеллект; инвестиционный проект; анализ данных; оценка эффективности проекта; нейронные сети.

PROSPECTS FOR USING ARTIFICIAL INTELLIGENCE TO PREDICT THE EFFECTIVENESS OF INVESTMENT PROJECTS

Ponomarev Ivan, Verzun Natalya
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mails: nokojoy@yandex.ru, verzun.n@unecon.ru

Abstract. The possibilities of using artificial intelligence systems for evaluating and predicting the effectiveness of investment projects are considered. The features of the tasks associated with such an assessment are described. An overview of solutions based on artificial intelligence and possible applications for predicting the effectiveness of investment projects is given.

Keywords: artificial intelligence; investment project; data analysis; assessment of the effectiveness of the project; neural networks.

Искусственный интеллект – область науки, сформировавшаяся в середине прошлого века, и занимающаяся моделированием мыслительной деятельности человека, разработкой систем, способных решать задачи, принимать решения, мыслить также как человек. Благодаря бурному развитию систем искусственного интеллекта, машины сегодня способны заменять людей на многих рабочих местах и к ним все чаще прибегают при решении различных задач в экономике. Машинный разум по своей эффективности оказывается равным или превосходит человеческий, а также зачастую обходится дешевле [1]. Охватывая все больше сфер деятельности, искусственный интеллект ускоряет принятие решений, позволяет исключить негативное влияние человеческого фактора (ошибки, субъективный взгляд и пр.). К нему обращаются при выполнении нетривиальных задач, требующих учета множества разнообразных факторов, в условиях неопределенности, неполноты исходных данных. К подобным задачам можно отнести задачу оценки эффективности инвестиционных проектов.

Инвестиционный проект – это совокупность мероприятий с известной конечной целью, требующих вложения некоторых инвестиций (финансовых, материальных средств) в определенную деятельность. Под эффективностью инвестиционного проекта понимают степень его соответствия целям, интересам участников инвестирования. В целом она оценивается для того, чтобы определить потенциальную привлекательность проекта для возможных участников и поисков источников его финансирования [2].

Традиционно для оценки эффективности инвестпроекта применяются методы, основанные на расчете и анализе множества количественных показателей, например: чистый дисконтированный доход (NPV – Net Present Value), окупаемость инвестиций (ROI – Return on Investment), индекс рентабельности (PI – Profitability Index) и других. Кроме количественных, используют также и качественные подходы к оценке эффективности проектов. К ним следует отнести различные методики, как правило, определяемые экспертами, по определению возможности и фактического достижения результатов, а также методы оценки рисков, среди которых различают финансово-инвестиционные, организационные, криминогенные, социальные, экологические, политические и др. виды рисков.

Представленные на рынке программные продукты, ориентированные на автоматизацию процессов, связанных с оценкой эффективности проекта (например: программные продукты от российских производителей: Альт-Инвест, ТЭО-Инвест, или зарубежных производителей: COMFAR, Project Expert), предоставляют пользователю возможность провести комплексный анализ проекта на стадии его планирования и обоснования эффективности инвестиций. Используемые в российских продуктах подходы к расчету показателей эффективности инвестиций соответствуют «Методическим рекомендациям по оценке эффективности инвестиционных проектов», утвержденным Госстроем, Минэкономики, Минфином и Госкомпромом России, а также учитывают требования международных стандартов (например методики ЮНИДО и Всемирного банка).

Подобное ПО можно рассматривать как систему поддержки принятия решений, применяемую на этапе «прединвестиционной подготовки» [3], как средство агрегации существующих знаний по проекту и генерации новых. Но, даже с учётом уровня развития современных технологий, окончательное решение об инвестировании в проект и начале его реализации принимает человек. Поэтому основной целью программного продукта в данной области является предоставление инструментов анализа текущей конфигурации проекта, формирование альтернативной конфигурации, а также их сравнения.

К особенностям задачи оценки и прогнозирования эффективности инвестиционных проектов можно отнести следующее:

– необходимость учета, сопоставления множества разнообразных внешних и внутренних факторов проекта;

– зачастую неполнота (и/или) противоречивость входных данных;

– междисциплинарный характер оценки инвестиционных проектов – в данном процессе применяются методы риск-менеджмента, финансовой и экономической науки, маркетинга и экономической психологии [2];

– отсутствие определенности, например по причине действия глобальных рисков – геополитических, макроэкономических.

В данном случае, применение методов, основанных только на стандартных расчетах экономических показателей, может привести к неверным результатам и, как следствие, возможному принятию ошибочных решений [3]. Поэтому, программные продукты предусматривают использование и других, альтернативных числовым расчетам, методов анализа и оценки. Так, например, ТЭО-Инвест, позволяет создать имитационную модель денежных потоков, что дает пользователю возможность построить финансовую модель предприятия, реализующего инвестиционный проект, проанализировать варианты его осуществления в соответствии с различными сценариями.

Также, целесообразно в подобных условиях прибегать к вспомогательным инструментам, разработанным на базе искусственного интеллекта. Способность к обучению, к работе с неполными, противоречивыми, многочисленными и разнородными данными, быстрое принятие решений и отсутствие эмоций – все это преимущества средств искусственного интеллекта, которые могут способствовать повышению эффективности оценки привлекательности проектов для инвесторов. Например, нейронные сети и использование нечёткой логики может значительно расширить как возможности анализа количественных и качественных показателей, так и отслеживать закономерности в реализации проектов, проводить более глубокий анализ чувствительности [3].

В докладе проводится обзор решений, основанных на применении систем искусственного интеллекта и возможных для применения в целях прогнозирования и принятия решений об эффективности инвестпроектов.

Так, в [3] предлагается построение нейронной сети из пяти слоёв для анализа эффективности инвестиционного проекта. В качестве параметров автор предлагает использовать выручку от продаж, себестоимость производства, затраты на рекламу, текущие расходы и затраты на выплату кредитов, а в качестве выходного параметра – прибыль. Оценка происходит по значению выходного параметра, где его минимальное значение приравнивается к «0», а максимальное – к «100». Применение подобного алгоритма, подстроенного под запросы программы, в сочетании с базой данных завершённых проектов позволит повысить точность расчёта ожидаемой эффективности инвестиционного проекта, а также предоставит аналитику дополнительную информацию, которую он сможет сопоставить с полученными им данными.

Другим вариантом применения технологий нейронных сетей при анализе и прогнозировании инвестпроектов могут стать инструменты data mining, которые, в частности, могут позволили бы аналитику находить скрытые корреляции в разрозненных данных [4]. В первую очередь это касается интеллектуального исследования литературных источников, в том числе архивных данных, новостей и научных публикаций, которое бы мог производить сам аналитик, не опираясь на чужую выборку данных. Применение data mining для исследования текстовых источников в значительной степени позволит сократить время, затрачиваемое на формирование видения внешней среды проекта, а также значительно расширит создаваемую в рамках проекта выборку факторов, влияющих на перспективность проекта.

Кроме того, средства искусственного интеллекта позволят анализировать план проекта и находить в нём недостатки, к примеру, в виде оптимизации объёмов закупаемого материала [5], что в свою очередь позволит как вводить более точные данные по анализируемому проекту, так и оптимизировать затраты, связанные с его реализацией.

СПИСОК ЛИТЕРАТУРЫ

1. Верзун Н.А. Колбанёв М.О., Омельян А.В. Сетевая архитектура цифровой экономики: монография. – СПб.: Изд-во СПбГЭУ, 2018. – 157 с.
2. Андрианова Ю.В. Оценка эффективности инвестиционных проектов в современных условиях [Электронный ресурс] // Российский экономический интернет-журнал, 2019. – № 1. URL: http://elib.fa.ru/art2019/bv261.pdf.
3. Кричевский М.Л., Мартынова Ю.А. Инструменты искусственного интеллекта при оценке эффективности инвестиционного проекта // КЭ. 2018. №8. – С.1105–1118.
4. Тришечкин С.Н. Data Mining и метод нейронных сетей // Вестник науки и образования. 2019. №8-1 (62) – С.37–40.
5. Иманов Р.А., Пономарева С.В., Серебрянский Д.И. Развитие цифровой экономики: искусственный интеллект в отечественном промышленном производстве // РППЭ. 2018. №6 (92). DOI: https://doi.org/10.26726/1812-7096-2018-6-5-11.

УДК 004.9

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ РОБОТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ РАЗЛИЧНЫХ СФЕРАХ БИЗНЕСА

Соловей Полина Сергеевна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: polina_solovyshka@mail.ru

Аннотация. Данная работа посвящена возможностям применения инновационной технологии роботизации бизнес-процессов (RPA) в различных сферах бизнеса. Рассматриваются особенности внедрения технологии RPA в различные сферы бизнеса и перспективы ее развития.

Ключевые слова: RPA; роботизация; бизнес; бизнес-процессы; программные роботы; роботизация бизнес-процессов.

OPPORTUNITIES OF ROBOTIZATION OF BUSINESS PROCESSES APPLICATION IN VARIOUS BUSINESS FIELDS

Solovey Polina
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: polina_solovyshka@mail.ru

Abstract. This work is devoted to the possibilities of applying innovative technologies for the robotization of business processes (RPA) in various fields of business. The features of the introduction of RPA technologies in various business areas and the prospects for its development are considered.

Keywords: RPA; robotization; business; business processes; software robots; robotization of business processes.

В существующих условиях высокой конкурентной среды в различных сферах бизнеса задача автоматизации бизнес-процессов является актуальной. Одним из способов автоматизации бизнес-процессов, позволяющий повысить эффективность ведения бизнеса, является роботизация бизнес-процессов.

Роботизация бизнес-процессов (Robotic Process Automation, RPA) – современная технология, позволяющая автоматизировать задачи и процессы, которые ранее выполнялись человеком, путем программирования роботов на выполнение повторяющихся действий. RPA используется для автоматизации деятельности работника, имеющей четкий алгоритм действий.

Машинное обучение (Machine Learning, ML), искусственный интеллект (Artificial Intelligence, AI) и бизнес-аналитика (Business Intelligence, BI) в ближайшем будущем могут стать составными частями технологии RPA, что позволит бизнесу в разных сферах достичь еще большей операционной эффективности. Кроме того, технологии ML, AI и BI могут позволить автоматизировать множество процессов при помощи роботизации, включая процессы, требующие принятия решений, суждений и обработки нетривиальных сценариев и неструктурированных данных [1].

В качестве инструментальных средств создания программных роботов существуют как зарубежные, так и российские решения. Среди зарубежных решений можно отметить четыре мировых вендора – это UiPath, Automation Anywhere, Blue Prism и NICE. Также существует несколько российских платформ – Robin, electroNeek и PIX. Данные российские платформы начали появляться с середины 2018 года, но уже имеют некоторые преимущества перед зарубежными: конкурентная цена и лучшая адаптация к документам на русском языке [2]. Следует отметить, что российский рынок RPA активно растет, и разработчики данной технологии сейчас пользуются огромным спросом, множество известных компаний нуждаются в RPA-профессионалах.

Важной особенностью RPA является способность технологии работать поверх текущей инфраструктуры, не изменяя ее, что обеспечивает гибкость процессов при их трансформации. Принцип работы технологии роботизации «заключается на создании списка действий для автоматизации задачи с использованием программных интерфейсов (API) или языка сценариев» [2]. Для успешного внедрения RPA в бизнес-процесс любой сферы необходимо построить четкую стратегию внедрения и детально продумать дорожную карту развития, которая в основном составляется бизнес-аналитиками организации.

Роботизация процессов в бизнесе является кросс-культурной технологией и может использоваться практически во всех сферах, например, в бухгалтерском учете, логистике, сфере HR, страховании, управлении цепочками поставок, деятельности органов государственного управления и банковской сфере. В различных областях бизнеса существует много ручных, часто повторяемых и основанных на четких правилах процессов, где роботизация проявляет себя наилучшим образом.

Многие крупные компании как зарубежные, так и российские, уже имеют успешный опыт внедрения технологии RPA. Например, сеть розничной торговли «Лента», сеть универсамов «Бегемаг», в сфере финансов – Альфа-Банк, Банк России и Экспобанк. Также свои бизнес-процессы роботизировали организации из сферы страхования, логистики и медицины – Росгосстрах, Почта России и Teva Pharmaceutical Industries (Тева Фармацевтические предприятия) [3].

В банковском секторе данная технология может позволит существенно улучшить скорость обработки банковских операций, повысить производительность бизнес-процессов, устранить ошибки, связанные с

«человеческим фактором», а также освободить работников от рутинных задач, вследствие чего у них появится время, необходимое для улучшения обслуживания клиентов и решения более сложных и нестандартных задач.

В банках может быть роботизировано большое количество внутренних функций и процессов: обработка счетов и платежей, ввод и сверка данных, кредитование, аудиторская отчетность, открытие и закрытие счетов, администрирование клиентской базы, начисление комиссий, зарплат и т. д.

В дальнейшей перспективе в банковской сфере по мере развития направления ускорится роботизация сложных бизнес-процессов ввиду применения технологий, обладающих адаптивностью и интерактивностью. Это поможет создавать продвинутые когнитивные системы для предоставления услуг по управлению капиталом (консультирование, инвестиционные рекомендации и т.д.) в банковской системе.

Данная технология также очень эффективна в бухгалтерском учете. RPA перспективно использовать в таких областях бухгалтерского учета как общий и оперативный учет, составление внутренней и внешней отчетности, планирование, бюджетирование и прогнозирование [4]. Избавляя работников от рутинных задач и высвобождая время, роботизация может привести к переориентации и расширению функций бухгалтера. Бухгалтеры смогут уделять больше времени анализу и интерпретации полученных данных, а также принятию решений. Для эффективного использования результатов применения программных роботов бухгалтерам необходимы будут технические знания.

Еще одним перспективным направлением для внедрения технологии роботизации является сфера розничной торговли. В сфере ритейла технология RPA может применяться для управления складскими запасами, для сбора и обработки данных, для категоризации продуктов и клиентской поддержки. Роботизация данных бизнес-процессов позволит быстро обмениваться данными между несколькими системами, извлекать, сортировать и сохранять необходимые данные, отслеживать наполнение витрин и решать другие трудоемкие ручные процессы.

Обслуживание клиентов – еще одна сфера для эффективного использования технологии роботизации. В процессах обслуживания клиентов выделяют две формы RPA: боты, нацеленные на фронт-офис и бэк-офис. Высвобождение времени операторов позволит им фокусироваться на задачах, которые непосредственно влияют на отношения с клиентами. Благодаря RPA компании выпускают продукты и услуги с более сложными функциями и по более высокой цене, когда программные роботы берут на себя повторяющиеся, рутинные задачи. В перспективе при правильном использовании данной технологии, контакт-центры смогут добиться ощутимых результатов в работе с клиентами.

Ожидается, что мировой рынок роботизации бизнес-процессов к 2027 году достигнет 10,7 миллиардов долларов США, увеличившись в среднем на 33,6% в период с 2020 по 2027 год, согласно новому отчету Grand View Research [5].

Говоря о краткосрочных и долгосрочных прогнозах внедрения технологии RPA – здесь существуют самые разные применения. Организации будут все чаще применять технологию RPA во многих отраслях и секторах, таких как нефть и газ, розничная торговля, производство, аналитика и юридические услуги. Большинство всех управляемых компьютером процессов с платформами и протоколами будут управляться с помощью программных роботов.

Таким образом, в перспективе роботизация в различных отраслях может привести к большим изменениям в существующих моделях бизнеса. В перспективе линейный персонал организаций может потерять работу, но необходимо отметить, что технология RPA не направлена на сокращение мест, а наоборот, благодаря роботизации работникам открываются новые вакансии, так как программным роботам нужна техническая поддержка.

СПИСОК ЛИТЕРАТУРЫ

1. Лилия Каневская | Блоги | Компьютерное Обозрение [Электронный ресурс]. – Режим доступа: https://ko.com.ua/blogs/237286. – Заглавие с экрана. – (Дата обращения: 30.06.2020).
2. RPA - Актуальное решение для автоматизации рутинных задач [Электронный ресурс]. – Режим доступа: https://cloudnetworks.ru/analitika/rpa-avtomatizatsiya-processov/. – Заглавие с экрана. – (Дата обращения: 30.06.2020).
3. RPA - Роботизированная автоматизация процессов [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/RPA_-_Роботизированная_автоматизация_процессов. – Заглавие с экрана. – (Дата обращения: 30.06.2020).
4. Еременко Е. А. Роботизация и автоматизация бухгалтерского учета //Бухгалтерский учет, анализ и аудит: история, современность и перспективы развития. – 2017. – С. 72-77.
5. Robotic Process Automation Market Worth $25.56 Billion By 2027 [Электронный ресурс]. – Режим доступа: https://www.grandviewresearch.com/press-release/global-robotic-process-automation-rpa-market. – Заглавие с экрана. – (Дата обращения: 30.06.2020).

УДК 004.806

ВОПРОСЫ ФОРМИРОВАНИЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ

Цехановский Владислав Владимирович, Чертовской Владимир Дмитриевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vdchertows@mail.ru

Аннотация. Рассмотрена технология формирования и прикладных мультикомпьютерных распределенных систем. Выполнена их классификация и дано описание классов. Освещены вопросы реализации для одноранговых структур и структур клиент-сервер. Представлено описание и проведен сравнительный анализ методов обмена информацией. Определен программно-аппаратный состав систем.

Ключевые слова: технология; распределенная система; классификация; структура; методы прикладной реализации.

ISSUES OF FORMATION OF DISTRIBUTED SYSTEMS

Tsehanovsky Vladislav, Chertovskoy Vladimir
Saint Petersburg Electrotechnical University "LETI"
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vdchertows@mail.ru

Abstract. Technology of formation and application implementation of multicomputer distributed systems is considered. They are classified and classes are described. Implementation issues for peer-to-peer and client-server structures are covered. Information exchange methods are described and compared. Hardware and software composition of the systems is defined.

Keywords: technology; distributed system; classification; structure; methods of application implementation.

Распределенные системы получают все более широкое распространение [1-4]. Они применяются для систем получения информации для пользователя и для автоматизированных систем управления производством и предприятием, а в последнее время – в учебном процессе. Имеется множество методов построения распределенных систем. Для их выбора с учетом особенностей реализуемых систем требуется систематизация и классификация компьютерных методов с учетом их сфер применения и возможностей. Этим вопросам посвящена настоящая работа. Выявлены области использования и проведен анализ методов. Приведены рекомендации по их применению. Освещены вопросы прикладного построения и применения распределенных систем. Результаты данной работы могут быть полезны при проектировании распределенных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Радченко Г.И. Распределенные вычислительные системы / Г.И. Радченко. –Челябинск: Фотохудожник, 2012. – 184 с.
2. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/mehanizmy-integratsii-baz-dannyh-i-programm-analiza_– Заглавие с экрана. – (Дата обращения: 15.02.2020).
3. [Электронный ресурс]. – Режим доступа: https://stackoverrun.com/ru/q/169118_ – Заглавие с экрана. – (Дата обращения: 18.02.2019).
4. [Электронный ресурс]. – Режим доступа: http://qaru.site/questions/126239/how-to-insert-table-values-from-one-database-to-another-database – Заглавие с экрана. – (Дата обращения: 21.02.2019).

УДК 332.1; 338. 2

РАЗРАБОТКА ЦИФРОВОЙ МОДЕЛИ САМАРСКО-ТОЛЬЯТТИНСКОЙ АГЛОМЕРАЦИИ

Цыбатов Владимир Андреевич
Самарский государственный экономический университет «СГЭУ»
Советской Армии ул., 141, Самара, 443090, Россия
e-mail: tva82@yandex.ru

Аннотация. Рассматривается цифровая модель Самарско-Тольяттинской агломерации в составе прогнозно-аналитического комплекса, предназначенного для решения задач сценарного прогнозирования и стратегического планирования в рамках системы управления социально-экономическим развитием агломерации.

Ключевые слова: агломерация, сценарное прогнозирование, стратегическое планирование, цифровая модель, прогнозно-аналитический комплекс.

DEVELOPMENT OF THE DIGITAL MODEL OF SAMARA- TOGLIATTI AGRLOMERATION

Tsybatov Vladimir
Samara State University of Economics "SSEU"
141 Sovetskaya Armii St, Samara, 443090, Russia
e-mail: tva82@yandex.ru

Abstract. The article considers a digital model of the Samara-Tolyatti agglomeration as part of a forecast and analytical complex designed to solve the problems of scenario forecasting and strategic planning within the framework of the socio-economic development management system of the agglomeration.

Keywords: agglomeration, scenario forecasting, strategic planning, digital model, forecast and analytical complex.

Самарско-Тольяттинская агломерация представляет собой совокупность компактно расположенных городских и сельских населенных пунктов Самарской области, объединенных устойчивыми и интенсивными хозяйственными и социальными связями, характеризующихся возрастающей концентрацией населения, экономической активностью и доминированием двух центров-ядер – городских округов Самара и Тольятти. Самарско-Тольяттинская агломерация (СТА) является третьей по численности населения агломерацией в России. В состав СТА входят 17 муниципальных образований (МО) - 8 городов и 9 муниципальных районов. Для повышения эффектов от агломерационного развития была сформирована модель системы управления СТА, нацеленная на использование дополнительных механизмов для превращения агломерационных эффектов в конкретные социальные и экономические эффекты [1]. В рамках создания такой системы управления был разработан прогнозно-аналитический комплекс (далее – Комплекс) для поддержки задач прогнозирования и стратегического планирования. В состав Комплекса входят следующие компоненты:

– информационная база;
– база многовариантных сценариев развития МО;
– система частных цифровых (имитационных) моделей социально-экономической деятельности муниципальных образований (17 моделей);
– цифровая модель социально-экономической деятельности СТА;
– монитор Комплекса, реализующий информационные технологии долгосрочного сценарного прогнозирования.

Информационная база Комплекса предназначена для хранения и обработки собранных данных о деятельности 17 муниципальных образований, входящих в состав СТА, и Самарской области в целом. Проведена верификация отчетных данных, проверка их полноты, дополнение отсутствующих данных, устранение дисбалансов и противоречивости данных.

Сценарии развития МО (демографические и экономические) разработаны на основе сценарных материалов соответствующих муниципальных стратегий. При этом также учитывались:
– межмуниципальные миграционные потоки и инвестиционные проекты;
– дорожная карта стратегии развития Самарской области [2];
– целевые ориентиры национальных проектов.

Модель социально-экономической деятельности отдельного муниципального образования разработана в классе CGE-моделей, рассматривающих развитие экономики как результат деятельности экономических агентов - основных субъектов территории [3]. Эти модели хорошо себя зарекомендовали при региональных исследованиях [4]. В модели МО экономика разбита на совокупность экономических агентов согласно ОКВЭД2[5] с добавлением агентов: «домашние хозяйства», «органы государственной власти», «внешнее окружение» и агента «невидимая рука рынка», отвечающего за равновесие спроса и предложения на моделируемых рынках. Модельное описание экономического агента содержит описание его ресурсов (природных, трудовых, капитальных, финансовых) и поведения. Экономические агенты производят один или несколько условных продуктов из базового набора, которые продаются внутри региона или вывозятся. При этом агентами приобретаются необходимые продукты как внутри региона, так и за его пределами с учетом ресурсных и бюджетных ограничений. Модели экономических агентов реализованы как системы управления, работающие по отклонениям. Основой поведения каждого экономического агента являются целевые установки (траектории), которые ориентируют его действия в направлении, обеспечивающем достижение поставленных целей. Агент контролирует текущее отклонение значений целевых индикаторов от установленных целей и формирует управляющие воздействия на двунаправленную обобщенную производственную функцию (ОПФ) агента с учетом наблюдаемых параметров обстановки (рыночной конъюнктуры и состоянию ресурсов) и внешнего (сценарного) управления. Ресурсами экономического агента являются: основной капитал, трудовой потенциал, денежные средства (наличные и на счетах), запасы промежуточных и готовых продуктов. Экономические агенты объединены в единую систему через рынки условных продуктов. Целевые установки и сценарные условия для агентов задает Исследователь. Вычисления на модели МО проводятся с шагом 1 год. На каждом шаге по заданному сценарию развития на модели воспроизводственного процесса с учетом ресурсных ограничений последовательно рассчитываются валовой выпуск, отгрузка и элементы добавленной стоимости. В модели распределения добавленной стоимости рассчитываются: доходы и расходы бюджетов всех уровней и внебюджетных фондов, инвестиционные ресурсы, денежные доходы и расходы населения, показатели уровня жизни и прочие индикаторы социально-экономического развития. В модели конечного потребления и валового накопления формируется конечное потребление домашних хозяйств, государственных учреждений и некоммерческих организаций. В модели производственных факторов рассчитывается производственный потенциал экономики и формируются ограничения экономического роста по трудовым ресурсам и основному капиталу. Потенциал основного капитала рассчитывается на модели основного капитала, которая представляет собой совокупность моделей основных фондов (ОФ) отраслей муниципальной экономики. Динамика производственного потенциала моделируется на основе процессов ввода и выбытия капитала, связанных с инвестиционной активностью экономических агентов и загрузкой ОФ. При построении модели производственного потенциала также использованы рекомендации, приведенные в обзоре [6]. Потенциал трудовых ресурсов оценивается на основе демографических расчетов, в основе которых лежит классическая модель передвижки возрастов [7].

Монитор Комплекса реализует технологию сценарного прогнозирования социально-экономического развития СТА в виде последовательности следующих этапов:

1 – формирование сценариев развития МО с учетом межмуниципальных связей. Здесь важно, чтобы формируемые сценарии развития МО имели одинаковую «окраску» (консервативные, базовые или целевые) и согласовывались с соответствующим сценарием развития Самарской области. Также важно, чтобы эти сценарии были нацелены на достижение основных ориентиров национальных проектов;

2 – прогнозирование развития МО на горизонте 2020-2035 годов по сформированным сценариям. На этом этапе последовательно формируются прогнозные значения показателей социально-экономического развития для всех МО в виде динамических рядов в виде прогнозных матриц размером m*n, где m – количество показателей (m=800), n – глубина прогнозирования (n=16);

3 – формирование прогноза социально-экономического развития СТА в целом путем суммирования прогнозных матриц всех 17 муниципальных образований, входящих в состав СТА.

С помощью Комплекса проведен стратегический анализ направлений социально-экономического развития СТА путем отработки на цифровых моделях стратегий развития МО с учетом общих ресурсных ограничений (демографических, трудовых, финансовых, производственных). Сделана попытка сконструировать допустимые стратегии развития МО, позволяющие максимально близко подойти к целевым ориентирам национальных проектов. Полученные результаты анализа и прогнозирования позволили оценить потенциал СТА и перспективы ее развития. На их основе проведено стратегическое целеполагания развития СТА до 2035 года, сформировано дерево целей и установлены целевые ориентиры для разрабатываемой системы управления агломерацией.

СПИСОК ЛИТЕРАТУРЫ

1. Цыбатов В.А., Павлов Ю.В., Бортников С.П. Реформа модели управления Самарско-Тольяттинской агломерацией // Вестник Самарского государственного экономического университета. - Самара, 2019. - № 12 (182). - С. 38-45.
2. Стратегия социально-экономического развития Самарской области на период до 2030 года / Утверждена постановлением Правительства Самарской области от 12.07.2017 №441. [Электронный ресурс]. URL: http://economy.samregion.ru/upload/iblock/82a/strategiya-so_2030.pdf (дата обращения: 22.05.2019).
3. Handbook of Computable General Equilibrium Modeling, Volume 1B 1st Edition // Editors: Peter Dixon, Dale Jorgenson. - North Holland, Amsterdam. – 2013. – 1056 p.
4. Цыбатов В.А. Стратегическое планирование энергоэффективного развития субъекта Российской Федерации // Экономика региона. - 2018. - Т. 14, вып. 3. - С. 941-954.
5. Общероссийский классификатор видов экономической деятельности (ОКВЭД 2). ОК 029-2014 (КДЕС ред. 2). [Электронный ресурс]. URL: http://xn---2-dlci2ax1i.xn--p1ai/ (дата обращения: 15.01.2018).
6. Martínez-Costa, C., Mas-Machuca, M., Benedito, E., & Corominas, A. (2014). A review of mathematical programming models for strategic capacity planning in manufacturing. International Journal of Production Economics, 153, 66-85.
7. Методологические положения по статистике. Вып.1, Госкомстат России. – М.,1996 г. – 674 с.

УДК 004

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОБЛЕМЫ УПРАВЛЕНИЯ УМНЫМИ ГОРОДАМИ

Шилков Владимир Ильич
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mail: radioustus@yandex.ru

Аннотация. Обсуждаются возможности применения современных информационных технологий для управления городом. Обсуждаются проблемы умных городов, связанных с новыми целями, задачами, информационно-технологическими решениями. Предлагается трактовка термина информационно-экономическая безопасность умного города. Обсуждаются риски снижения информационной безопасности умных городов.

Ключевые слова: цифровизация, умный город, IoT (интернет вещей), риски, информационно-экономическая безопасность, кибербезопасность.

INFORMATION TECHNOLOGIES AND PROBLEMS OF MANAGING SMART CITIES

Shilkov Vladimir
The Ural Federal University named after the first President of Russia B. N. Yeltsin
19 Mira St, Yekaterinburg, 620002, Russia
e-mail: radioustus@yandex.ru

Abstract. The possibilities of using modern information technologies for city management are discussed. The problems of smart cities related to new goals, tasks, and information technology solutions are discussed. The risks of reducing the information security of smart cities are discussed. An interpretation of the term information and economic security of a smart city is proposed.

Keywords: digitalization, smart city, IoT (Internet of things), risks, information and economic security, cybersecurity.

Информатизация и интеллектуализация процессов управления современными городами нашла свое воплощение в концепциях цифрового города, интеллектуального города, умного города. К перспективным информационным технологиям, которые необходимы для реализации концепции умных городов, по мнению авторов работы [1], следует отнести сквозные технологии, технологии беспроводной связи, технологии искусственного интеллекта, промышленный интернет.

Информационно-технологические комплексы и отдельные информационные технологии, способные обеспечить поддержку широкого круга задач умного города, входят в состав городских критических инфраструктур. К данным комплексам могут быть отнесены отдельные технические устройства, оборудование, узкоспециализированные программные средства и технологии, требующиеся для решения определенных задач управления. Ожидается рост глобального рынка умных датчиков (контроля температуры, влажности, давления, уровня воды и освещения) с 18 млрд USD в 2015 году до 57 млрд USD в 2022-м.

В работе [2] отмечено, что практическое воплощение концепции умного города может быть осуществлено на основе современной технологии сбора и анализа информации BigData. BigData, позволяет оперативно обрабатывать огромные объёмы плохо структурированных данных значительного многообразия в рамках решения нескольких задач. Авторы работы [3] предлагают подход позволяющий осуществлять более эффективную идентификацию, объединение и управление большими данными. Пример и особенности использования технологий BigData для создания умной транспортной системы для решения задач умного города и приведен в работе [4]. К информационным технологиям городского умного транспорта могут быть отнесены умные системы наблюдения, системы оплата проезда, системы управления парковочными пространствами и системы информирования пассажиров.

Важным направлением реализации концепции умного города является информатизация широкого спектра задач в сфере управления жилищно-коммунальным хозяйством (ЖКХ). Применение информационных технологий для управления умным ЖКХ, необходимо при создании интеллектуальных систем управления освещением, учета и контроля воды, тепла и умного обращения с отходами. Умное обращение с отходами, предполагает оснащение мусорных баков IoT-датчиками, которые по каналам GSM обеспечивают передачу данных о степени наполнения баков твердо-коммунальными отходами (ТКО).

Умная энергетика позволяет повысить экономическую эффективность использования электроэнергии, например, за счет установки контроллеров и датчиков освещенности для управления светодиодными светильниками.

К 2022 году по сравнению с 2017 годом прогнозируется рост рынков: технологий умной энергетики и умных распределенных сетей (Smart Grid); технологий в области интернета вещей (IoT) и технологий в области кибербезопасности. Ожидается рост сегментов рынка, связанных с удаленным мониторингом, управлением данными и аналитикой данных в реальном времени.

Проблемы, управления современными городами, могут быть связаны не только с необходимостью оперативного привлечения ресурсов для обеспечения безопасности жителей города, но и возникновением рисков изменения социально-экономических ориентиров, возникновением новых требований к качеству жизни, в том числе требований, предъявляемых к здравоохранению и социальному обслуживанию. Необходимость учета вероятности возникновения глобальных рисков отмечается в работе [5]. Новые проблемы управления средой обитания связаны с большей интенсивностью загрязнения воздуха и почвы, увеличением объемов потребляемой воды, сложностью утилизации отходов.

Возникновение опасных гидрометеорологических явлений часто является следствием глобальных изменений климата и является значительным фактором риска для современных городов. К рискам резкого изменения климатических условий в современных городах приводит и интенсивное воздействие антропогенных факторов. Экстремальные погодные явления, вместе с другими погодно-климатическими рисками могут оказывать значительное влияние на состояние социально-экономической сферы не только отдельных городов и экономических регионов, но и различных стран.

На новый уровень выходят и проблемы управления городскими грузопассажирскими перевозками и масштабными городскими спортивными и культурно-развлекательными мероприятиями.

Применение информационно-коммуникационных технологий для управления критическими инфраструктурами городского хозяйства, в ряде случаев, может приводить к возникновению дополнительных проблем и угроз для информационной и экономической безопасности умного города.

В связи с данными обстоятельствами, информационные технологии и программно-аппаратные комплексы, задействованные в управлении умными городами, должны учитывать вероятности возникновения различных рисков, обусловленных особенностями функционирования городов в современных условиях.

Несмотря на то, что интеграция устройств, приборов и компонентов программных средств, взаимодействующих в режиме реального времени, с одной стороны способствует достижению новых возможностей, но с другой стороны, приводит к возникновению различных информационно-технологических рисков и увеличению вероятности сбоев и отказов в работе систем.

Под информационно-экономической безопасностью умного города можно понимать оптимальное состояние муниципального образования, характеризующееся способностью информационно-технологических систем управления организационными структурами эффективно и устойчиво функционировать в соответствии с социальными и экономическими критериями и ориентирами, в том числе в условиях случайного воздействия критических факторов.

Особое место среди проблем управления умными городами занимают проблемы, связанные с рисками снижения уровня информационной безопасности. В работе [6] отмечено, что данные риски должны учитываться на всех этапах разработки и реализации концепции умных городов, так как искажения или потери, казалось бы, малозначимой информации, могут приводить к катастрофам с чрезвычайно тяжелыми реальными последствиями. Для повышения уровня информационной безопасности умного города может быть рекомендован целый ряд организационно-технических методов защиты информации, к которым могут быть отнесены мероприятия, связанные с тестированием и оценкой опасностей возникновения специфических угроз со стороны новых:

- источников информации (возможной недостоверности и ненадежности данных);
- пользователей и обслуживающего персонала.
- информационных технологий (программно-технологические компоненты);

– целей использования информации (альтернативного использования данных);
– организационно-управленческих мероприятий (организационные процедуры и процессы преобразования информации).

К росту уровня угроз информационной безопасности умного города может привести не только отсутствие системного подхода при внедрении информационных технологий, но даже наличие отдельных несогласованностей между отдельными технологиями городского хозяйства. Поэтому залогом нормального функционирования всех объектов и подсистем является комплексный, системный подход к обеспечению информационно-экономической безопасности умного города.

СПИСОК ЛИТЕРАТУРЫ

1. Проблемы и перспективы развития цифровой экономики Российской Федерации. Кириченко Д.А. // В сборнике: Теоретические и практические аспекты трансформации налоговой системы России. Материалы Всероссийской научно-практической конференции. Ростов-на-Дону, 2018. С. 169-175.
2. Инновационно-стратегические направления обеспечения информационной безопасности региона Матвеев Е.А. // В сборнике: материалы конференций ГНИИ "Нацразвитие". Май 2017. Сборник избранных статей. 2017. С. 81-86.
3. Characterization and Efficient Management of Big Data in IoT-Driven Smart City Development Alsaig, Alaa;Alagar, Vangalur ; Chammaa, Zaki //SENSORS. Volume: 19, Issue: 11, JUN 1 2019
4. Designing a smart transportation system: an Internet of Things and Big Data approach. Jan, Bilal; Farman, Haleem; Khan, Murad //IEEE wireless communications. Volume: 26 Issue: 4, AUG 2019, pages: 73-79.
5. Цифровая модель города: принципы и подходы к реализации. Митягин С.А., Соболевский С.Л., Дрожжин А.И., Воронин Д.Ю., Евстигнеев В.П., Садовникова Н.П., Парыгин Д.С., Чугунов А.В. International Journal of Open Information Technologies. 2019. Т. 7. № 12. С. 94-103.
6. Риски "умных" городов. Стефанова Н.А., Хисравова Я.Ш. Карельский научный журнал. 2018. Т. 7. № 2 (23). С. 125-126.

КРУГЛЫЙ СТОЛ «ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ФИНАНСОВО-КРЕДИТНОЙ СФЕРЫ И БИЗНЕСА»

УДК 004

ИНФОРМАТИЗАЦИЯ РЕГИОНАЛЬНЫХ БИЗНЕС-СТРУКТУР

Богачев Виктор Фомич
Институт экономических проблем им. Г.П. Лузина КНЦ РАН
Ферсмана ул., 24а, Апатиты, 184200, Россия
e-mail: vic-bogacetv@mail.ru

Аннотация. В статье исследуется история развития теории и практики автоматизации процессов в сфере управления. Анализируются особенности содержания различных этапов этих работ, первый из которых относится к 50-м годам XX столетия; качественно новый этап, связанный с использования принципов и методов автоматизации в управленческой деятельности и появлением термина «цифровизация» датируется началом XXI века.

Ключевые слова: цифровизация, автоматизация, автоматизированная система управления, цифровые технологии, «умный город», цифровая трансформация.

INFORMATIZATION OF REGIONAL BUSINESS STRUCTURES

Bogachev Victor
Institute of economic problems G. P. Luzin KNC RAN
24a Fersman St, Apatity, 184200, Russia
e-mail: vic-bogacetv@mail.ru

Abstract. The article explores the history of the automation theory and practice development in the area management. The features of the content in various stages of these works are analysed, where the first of which relates to the 50s of the XX century. This is a qualitatively new stage related to the use of principles and methods of automation in management operations and the emergence of the “digitalization” term dates back to the early XXI century.

Keywords: digitalization, automation, automated management system, digital technologies, “smart city”, digital transformation.

Введение. Развитие теории и практики автоматизации процессов в области технологии производства неизбежно привело к необходимости изменения информационных подходов к сфере менеджмента и бизнес-процессов. Анализ содержания различных этапов этих работ, первый из которых относится к 50-м годам XX столетия свидетельствует о качественно новом этапе, связанным с использования принципов и методов автоматизации в управленческой деятельности и появлением термина «цифровизация», который датируется началом XXI века.

К концу XX века в России был создан серьезный задел в виде созданных усилиями группы ученых (В.М. Глушков, А.И. Китов, А.А. Ляпунов, А.И. Берг и другие) комплекса автоматизированных систем управления (АСУП), в которых объединялись функции автоматического проектирования (САПР); технологической подготовки производства (АСПП); организационного управления предприятием (АСУП) [1-3]. Эти системы строились на более современных импортных ЭВМ и явились предшественниками современных ERP-систем, пришедших на российский рынок в 90-е и 2000- е годы.

Эти системы дали возможность в рамках организации координировать деятельность руководителей, интересы которых не всегда совпадают: финансового директора (функция снижения уровня запасов); директора по производству (функция загрузка мощностей); директора по продажам (функция снижения объема невыполненных заказов).

В качестве примеров можно привести две из самых востребованных систем. Так, система PM (Project Management) ориентирована на проектное управление и дает возможность расставить приоритеты и координировать деятельность различных служб для повышения эффективности организации. В качестве примера универсальной системы управления организацией можно привести BPMS (Business Process Management Systems), позволяющую строить бизнес-процесс как автоматизированную последовательность действий участников проекта.

Заключение. Сегодня достаточно сложно прогнозировать перспективы дальнейшего развития этого процесса, что обусловлено серьезным отставанием научных разработок в современной России и ограниченными

возможностями пользоваться достижениями мировой науки. В качестве важной составляющей развития информационных технологий в будущем следует отметить необходимость создания системы подготовки специалистов, способных разрабатывать и реализовывать стратегию цифровой трансформации в организации и обладающие соответствующими компетенциями в данной сфере.

СПИСОК ЛИТЕРАТУРЫ

1. Берг А. И., Китов А. И., Ляпунов А. А. О возможностях автоматизации управления народным хозяйством / Проблемы кибернетики. Выпуск 6. 1961. С. 83-100.
2. Глушков В.М. Введение в АСУ. Киев: Техника, 1972. 312 с.
3. Китов А.И. Электронные цифровые машины. М.: Советское радио, 1956. 358 с.

УДК 608.2

ВЫРАБОТКА ПРАВИЛ И ФОРМ ИЗЛОЖЕНИЯ БИЗНЕС-ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ КАК СРЕДСТВО ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСКИМ СХЕМАМ

Горенбургов Михаил Абрамович[1], Гончаров Вадим Владимирович[2]

[1] Федеральный исследовательский центр Кольский Научный Центр РАН
Ферсмана ул., 14, Апатиты, Мурманская обл., 184209, Россия
[2] ООО «МЭС»
Пискарёвский пр., 25, Санкт-Петербург, 190000, Россия
e-mail**s**: gorenburgow@mail.ru**,** gonchww@gmail.com

Аннотация. Доклад посвящён противодействию интернет-мошенничеству в бизнесе на уровне специализированного вэб-сайта и приводятся соответствующие рекомендации. Рассмотрены преимущественно сферы недвижимости и трудоустройства.

Ключевые слова: бизнес-коммуникации, интернет-сайт, удалённая работа, сделки, недвижимость, рациональность, реклама, маркетинг.

DEVELOPMENT OF RULES AND FORMS OF PRESENTATION OF BUSINESS INFORMATION ON THE INTERNET AS A MEANS OF COUNTERING FRAUD SCHEMES

Goncharov Vadim[1], Gorenburgov Mikhail[2]

[1] Federal research center Kola Research Center of the Russian Academy of Sciences
14 Fersman St., Apatity, Murmanskaya Oblast, 184209, Russia
[2] Ltd"MES"
25 Piskarevsky Av, St. Petersburg, 190000, Russia
e-mail**s**: gorenburgow@mail.ru**,** gonchww@gmail.com

Abstract. The report focuses on countering Internet fraud in business at the level of a specialized website and provides relevant recommendations. The areas of real estate and employment are mainly considered.

Keywords: business communications, website, remote work, transactions, real estate, rationality, advertising, marketing.

Введение. На протяжении предшествующих десятилетий сеть Интернет постепенно развивалась в сторону доминирующего канала взаимодействия между субъектами экономики. В то же время наблюдаемые усилия правительства по дальнейшей цифровизации административной и предпринимательской деятельности содействуют распространению удалённых средств бизнес и политических коммуникаций. На этом фоне растёт доверие обывателей к сделкам и коммуникациям, совершаемым удалённо на веб-сайтах.

Между тем Интернет обладает рядом особенностей, позволяющих осуществлять обманные схемы, как незаконные, так и находящиеся в границах действующих правовых норм. Вэб-сеть позволяет сохранять анонимность и влиять на клиентов лишь виртуальными, малозатратными, средствами. При этом влияние обычно оказывается посредством обращения к эмоциональной сфере клиентов, не обладающих достаточными знаниями для совершения сделок определённого типа [1]. В этой связи мошенники часто ориентируются на рынки труда и недвижимости, которые способны легче пробуждать эмоции в силу их большой жизнеобеспечивающей значимости.

Известно, что агрессивное апеллирование к эмоциям в целях снизить критичность мышления и склонить к принятию экономически неэффективных инвестиционных решений является общей чертой большей части современной рекламы. Однако в отношении таких сфер, как трудоустройство и сделки с недвижимостью такая реклама становится для клиентов особенно вредоносной. На актуальность проблемы указывают данные, согласно которым в разных странах на одно законное предложение об удалённой работе приходится в среднем 30-50 незаконных. Учитывая масштаб мошеннической деятельности, владельцам вэб-сайтов, на которых происходят бизнес-коммуникации целесообразно рассмотреть вопрос о введении для этих типов сделок определённых правил и форм изложения информации.

Схемы интернет-мошенничеств в трудоустройстве и недвижимости имеют сходство также в том, что чаще всего они направлены на отчуждение от клиента суммы денежных средств под видом задатка.

В сделках с недвижимостью задаток не возвращается, если клиент передумал покупать. По этой причине до получения задатка продавец может умышленно скрывать критически важную для покупателя информацию об объекте, а после получения денег раскрыть её. В результате покупатель вынужден мириться либо с потерей задатка, либо соглашаться на невыгодную покупку. И, если вэб-сайт в интересах своей репутации стремится к профилактике подобных ситуаций, то следует учитывать, что необходимые знания об объекте недвижимости часто можно получить из внешних источников, в том числе посредством отзывов очевидцев и жителей, знакомых с объектом.

Значительная часть мошеннического посыла к клиенту может передаваться по электронной почте, что лишает вэб-сайт инструментов контроля над ним. В таком случае защитить пользователей способна рекомендация к продавцам и покупателям, призывающая осуществлять только открытую переписку на вэб-ресурсе, что оградит их от целого класса мошеннических схем, рассчитанных на манипуляции через e-mail.

Достоверность информации об объекте недвижимости может обеспечиваться посредством публикации на сайте данных, независимо оценивающих район, улицы, объекты недвижимости. При этом целесообразно организовать публикацию отзывов о соответствии оценок текущей ситуации в районе, касающихся, как информации сайта, так и сведений от продавцов.

Под контроль пользователей и модераторов сайта должны попадать публикации характеристик объекта недвижимости: адрес (существует ли данный объект по указанному продавцом адресу), параметры объекта, право собственности, данные о строении, доп. сведения о месторасположении, изначальное количество комнат (выявление негласной перепланировки), тип квартир, наличие справки о числе прописанных в квартире людей (наличие жалоб от обманутых покупателей), справки о законности перепланировки (сканы оригиналов), долях (сканы оригиналов чертежей). Особо следует выделить: наличие предпосылок для реконструкции, сноса, расселения объекта; перспективы развития района и улицы; время которое объект находится в продаже; информация о репутации посредников, в том числе отзывы и наличие претензий на сайтах судов (при их наличии следует сделать на сайте пометку, что объект был предметом судебных разбирательств или риелтор был ответчиком по сделкам с недвижимостью, с указанием ссылок на номера дел и сайт суда.

Важно также контролировать или дополнять характеристика места, в котором располагается объект недвижимости: название и характеристики района города, транспортное сообщение (в т.ч. места для парковок, показатели загруженности дорог), экологические характеристики (основные источники загрязнения, шумовое загрязнение для района, улицы, дома, конкретной квартиры), заболеваемость болезнями, связанными с плохой экологией, здравоохранение (скорость госпитализации с учётом автомобильных пробок), социологические характеристики, такие как частота разбойных нападений, грабежей, ДТП, показатели уровня доходов, полово-возрастной структуры населения, структуры местной занятости и безработицы. Дополнять сведения о характеристиках места расположения может сравнительная оценка плотности населения и описание близлежащей спортивной и рекреационной инфраструктуры [2, 3].

Относительно формально-стилистической стороны изложения бизнес-информации предпочтительны наглядные и лаконичные средства, такие как таблицы и списки, составленные по принципу анкеты. Модератор сверяет по ключевым показателям данные об объекте из объявления со справочными данными сайта и отзывами пользователей и выставляет «!» напротив показателей с сомнительной достоверностью, размещённых под объявлением. В случае, если показатель поддаётся количественной оценке, то её рекомендуется комбинировать с качественным описанием. Пользователю должны быть доступны готовые выводы, полученные в результате проведённого анализа цифровых данных, снабженные комментариями, ясно объясняющими смысл и значимость показателя для неспециалистов и малоопытных инвесторов. Достаточно широкий спектр независимой информации об объекте будет способствовать снижению эмоциональной составляющей при принятии инвестиционных решений и, как следствие, повышению их экономической эффективности.

Заключение. Таким образом, значительный потенциал противодействия интернет-мошенничеству кроется в политике и технологиях владельцев интернет-ресурсов. Поощрение инициативы таких ресурсов представляется перспективной альтернативой политике государственных ограничений.

СПИСОК ЛИТЕРАТУРЫ

1. Горенбургов М.А., Крутик А.А., Гончаров В.В. Инновационные стратегии развития гостиничного бизнеса: монография. СПб.: Астерион, 2012. 172 с.
2. Крутик А.А., Горенбургов М.А., Горенбургов Ю.М. Экономика недвижимости. СПб.: Изд-во «Лань», 2000. 480 с.
3. Горенбургов М.А. Гончаров В.В. Обоснование экономической эффективности инвестиций в городскую недвижимость на основе теории игр: монография. СПб.: Д.А.Р.К., 2012. 160 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ТЕХНИЧЕСКИМИ СИСТЕМАМИ

УДК 004.067

ПРОБЛЕМЫ СБОРА ДАННЫХ В КИБЕР-ФИЗИЧЕСКИХ СИСТЕМАХ

Аббас Саддам Ахмед[1], Водяхо Александр Иванович[1], Жукова Наталия Александровна[2], Червонцев Михаил Александрович[1,3]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[3] Научно-инженерный центр Санкт-Петербургского электротехнического университета
Политехническая ул.,22, Санкт-Петербург, 194021, Россия
e-mails: saddamabbas077@gmail.com, aivodyaho@mail.ru, nazhukova@mail.ru, chervontsev.mikhail@nicetu.spb.ru

Аннотация. Рассматривается возможный подход к построению систем сбора данных в кибер-физических системах, реализованных на туманных платформах. Отличительной особенностью предлагаемого подхода является использование моделей наблюдаемой системы, представленной в терминах знаний.

Ключевые слова: системы сбора данных; модели; кибер-физические системы; Интернет вещей; окружающий интеллект; туманные вычисления.

DATA COLLECTION PROBLEMS IN CYBER-PHYSICAL SYSTEMS

Abbas Saddam[1], Vodyaho Alexander[1], Zhukova Nataly[2], Chervontsev Mikhail[1,3]

[1] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[3] Research and Engineering Center of Saint Petersburg Electro-Technical University,
22 Politechnicheskaya St, St. Petersburg, 197022, Russia
e-mails: saddamabbas077@gmail.com, aivodyaho@mail.ru, nazhukova@mail.ru, chervontsev.mikhail@nicetu.spb.ru

Abstract. A possible approach to the development of data collection systems which are used for data acquisition from cyber-physical systems built on fog platforms is considered. A distinctive feature of the proposed approach is the use of observable system models presented in terms of knowledge.

Keywords: data acquisition systems; models; cyber-physical systems; Internet of Things; ambient intelligence; fog computing.

Успехи в области микроэлектроники, телекоммуникаций и программной инженерии позволили выйти на принципиально новый уровень сложности создаваемых систем, включающих элементы разной физической природы, а также людей. Сложность систем определяется такими факторами, как число элементов, число уровней иерархии, а также уровнем интеллекта систем. Кроме того, структура системы и структура бизнес-процессов (БП) может изменяться в процессе функционирования.

Увеличение числа доступных для разработчиков технологий и инструментария приводит к появлению новых парадигм построения информационно-ориентированных систем, большинство из которых являются интеграционными и базируются на нескольких существующих парадигмах. В качестве современных парадигм, которые в полной мере отвечают современным тенденциям, можно назвать такие парадигмы как Интернет вещей, кибер-физические системы (КФС), социо-кибернетические системы, системы окружающего интеллекта (ОИ) [1].

Современные КФС все чаще строятся на распределенных платформах. В последние годы значительное распространение получили облачные и туманные платформы [2].

Системы нового поколения создаются для решения самых разнообразных задач, в частности, разного рода задач управления, сбора данных для последующего их анализа. Решение всех этих задач требует реализации процедур сбора данных как о наблюдаемых системах, так и о самой системе. Увеличение числа источников данных, в свою очередь, приводит к появлению хорошо известной проблемы больших данных. Решением этой проблемы может быть хранение не столько данных, сколько знаний. Возникает вопрос о том,

какие знания надо извлекать и хранить. Существует много типов знаний и подходов к их классификации. На верхнем уровне чаще всего говорят о таких типах знаний как процедурное, декларативное знание, метазнание, онтологическое знание и др. [3]. На более низких уровнях, в частности доменных уровнях, могут появляться другие типы знаний, такие как модельное знание, архитектурное знание. Для описания этого типа знаний обычно используются способы представления знаний верхнего уровня. Для решения задач, связанных с построением КФС, существенный практический интерес представляет модельное знание, которое можно определить как модель, построенную в терминах знаний.

Предлагается новый подход к построению систем сбора данных (ССД), ориентированный на использование в распределенных КФС, построенных на платформах туманных вычислений.

Идея развиваемого подхода заключается в использовании явной модели наблюдаемой системы, построенной в терминах знаний. Сущность предлагаемого подхода состоит в использовании механизмов работы с модельным знанием и в построении системы моделей, описывающих структуру и поведение наблюдаемой системы. Модели представляют собой модели знаний, а их актуальность поддерживается посредством снятия и анализа лог-файлов. При этом запросы всех заинтересованных сторон осуществляются только к моделям. Использование моделей, представленных в терминах знаний, позволяет оперативно отслеживать изменения структуры и поведения наблюдаемой КФС, сократить время отклика на запросы пользователей о состоянии наблюдаемой системы, поскольку нет необходимости каждый раз строить запросы к самой наблюдаемой системе, оперативно получать данные о прошлых состояниях и в определенных пределах предсказывать поведение наблюдаемой системы, если речь идет о реализации механизмов self* (самодиагностики, самолечения и т.п.), то модель позволяет накапливать знания о самой системе, т.е. создаются предпосылки для реализации механизмов когнитивности.

В самом общем виде функционирование ССД предлагается описывать в терминах 4 параллельно и асинхронно функционирующих автоматов (процессоров) и репозитария, в котором хранятся данные, информация и модели. Процессор формирования политик управления процессом сбора данных формирует скрипт, реализующий процедуру сбора данных. Процессор исполнения политик отвечает за реализацию сгенерированных скриптов. Процессор моделей отвечает за работу с модельным знанием. Процессор формирования представлений обрабатывает запросы пользователей на получение информации о состоянии наблюдаемой системы. В докладе рассматриваются алгоритмы функционирования этих процессоров.

Выделяются и рассматриваются 3 частных случая: ССД строится как система трансформации представлений, ССД строится как контекстно-ориентированная система и ССД строится как распределенная система, отдельные элементы которой встроены в подсистемы наблюдаемой КФС.

Ключевым моментом, связанным с практической реализацией предлагаемого подхода, является автоматическое построение моделей. Для автоматического построения структурных моделей предлагается использовать разработанный авторами метод синтеза моделей по лог-файлам [4], а для синтеза моделей поведения предлагается использовать алгоритмы Process Mining [5].

В докладе подобно рассматриваются основные типы задач сбора данных, модели, описывающие наблюдаемую КФС, модель туманной платформы, анализируются возможные подходы к реализации ССД в рамках сервисно-ориентированного подхода с учетом специфики туманной платформы, а также рассматриваются возможные подходы к проектированию и предлагается архитектурный фреймворк. Приводится пример практического использования предлагаемого подхода.

Предлагаемый подход и модели также могут быть с успехом использованы для реализации процесса сбора данных в разного рода КФС, включающих в себя в качестве элементов КФС, построенные на платформах туманных вычислений. Использование модельного подхода к построению ССД в таких системах позволяет выйти на новый уровень сложности создаваемых КФС, который недостижим при использовании традиционных подходов. Следует заметить, что ожидаемый переход к системам, которые способны к самообучению (когнитивным системам) делает задачу сбора данных еще более сложной и ее можно будет решить только с использованием модельного подхода, который может найти применение в самых разных предметных доменах.

СПИСОК ЛИТЕРАТУРЫ

1. Streitz N., Charitos D., Kaptein M., Böhlen M. Grand challenges for ambient intelligence and implications for design contexts and smart societies. Journal of Ambient Intelligence and Smart Environments 11 (2019) 87–107 87. IOS Press, NL, Amsterdam.
2. IEEE Standard Association. FOG − Fog Computing and Networking Architecture Framework, [Online] http://standards.ieee.org/develop/wg/FOG.html (датаобращения 17.11.2019).
3. Russell S., Norvig P. Artificial Intelligence: A Modern Approach, 4th Edition. Pearson. – 2020. – 1072 p.
4. Distributed Technical Object Model Synthesis Based on Monitoring Data / V. Yu. Osipov, A. I. Vodyaho, N. A. Zhukova, M. Tianxing, S. Lebedev // International Journal of Knowledge and Systems Science (IJKSS). – 2019. – Vol. 10, Iss. 3. – Art. 3. – P. 27–43.
5. Van der Aalst W. Process Mining Data Science in Action. Second Edition. – Heidelberg. Springer, 2016. – 468 p.

УДК 004

КОМПЛЕКСНОЕ ПЛАНИРОВАНИЕ ФУНКЦИОНИРОВАНИЯ И МОДЕРНИЗАЦИИ УНАСЛЕДОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Захаров Валерий Вячеславович
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: valeriov@yandex.ru

Аннотация. В докладе предложена постановка многокритериальной задачи планирования модернизации и функционирования унаследованной информационной системы (УИС), которая свелась к задаче многокритериальной оптимизации на комплексе логико-динамических моделей.

Ключевые слова: планирование модернизации и функционирования; комбинированная оптимизация.

INTEGATED PLANNING AND SCHEDULING OF FUNCTIONING AND MODERNIZATION OF LEGACY INFORMATIONS SYSTEM

Zakharov Valerii
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: valeriov@yandex.ru

Abstract. The paper proposed formulation a multicriterial problem of modernization and functioning of planning legacy information system, which has been reduced to multi-criterion optimization task on the complex logical-dynamic models.

Keywords: modernization planning and scheduling; EIS modernization; combined optimization.

Введение. В докладе в качестве основных объектов исследований рассматривается унаследованные информационные системы (УИС) [1]. Под данными системами понимают информационные системы, для которых используется эволюционный путь развития, т.е., другими словами, переход от их “старой” архитектуры к “новой” архитектуре осуществляется в течение заданных промежутков времени и состоит в плановой замене отдельных подсистем и элементов функционирующей УИС в целях повышения ее производительности и снижения затрат на эксплуатацию. Данный этап жизненного цикла УИС называют этапом модернизации [1]. Традиционно для принятия решения на проведение модернизации УИС необходимо решить следующие задачи: синтез облика модернизируемой УИС (ищется ответ на вопрос – что и когда надо модернизировать); определение срока (момента времени), к которому надо завершить модернизацию; синтез технологии модернизации (ищется ответ на вопрос – в какой последовательности надо проводить модернизацию); синтез плана проведения модернизации.

Анализ [1-2] показывает, что задача планирования и управления модернизацией УИС должна решаться совместно с задачей планирования и управления функционированием УИС в целях обеспечения устойчивой текущей деятельности соответствующей бизнес-системы (БС), в интересах которой создавалась УИС. При этом само планирование и управление должно осуществляться комплексно и затрагивать все основные элементы и подсистемы существующей и создаваемой УИС [3].

Это означает, что в процессе выбора программ модернизации облика данной системы каждый раз требуется обоснованно определять, в каком месте и в какое время должна быть произведена замена того или иного элемента структуры (структур) существующей УИС на новый, перспективный элемент. Кроме того, требуется проводить оценивание того, как влияют изменения структур УИС на процесс функционирования БС. Для этого должна использоваться соответствующая система показателей эффективности и качества планирования модернизации (функционирования) УИС.

К числу таких показателей будем, в первую очередь, относить [3-8]: показатели эффективности применения УИС; показатели технической эффективности; эргономические и социально-психологические показатели; показатели экономической эффективности и ресурсосберегаемости; показатели, характеризующие эффективность адаптации и самоорганизации УИС на этапе её модернизации и функционирования; показатели, характеризующие длительность реализационного периода УИС и периода полезной жизни до следующей модернизации (время эксплуатации); показатели эффективности управления функционированием и модернизации УИС.

Проведенный анализ показал, что совместное решение задач комплексного планирования модернизации и функционирования УИС наряду с заданием перечисленных показателей предполагает: построение соответствующего полимодельного комплекса, описывающего все основные аспекты исследуемых процессов; разработку комбинированных методов, алгоритмов и методик многокритериального полимодельного синтеза программ управления модернизацией и функционированием существующей и внедряемой УИС [9].

Решение перечисленных задач многокритериального оценивания, анализа и выбора эффективных вариантов программ управления модернизацией и функционирования УИС в докладе предлагается осуществлять с использованием развиваемой автором доклада теории проактивного управления структурной динамикой (УСД) сложных объектов (СлО). Данная теория имеет междисциплинарный характер и основывается на результатах, полученных к настоящему времени в классической теории управления и исследовании операций и в общей теории систем и системном анализе [1, 5, 6].

В докладе показано, что на аналитическом уровне описания процесс модернизации и функционирования УИС можно интерпретировать как процесс выполнения комплексов целевых, обеспечивающих и вспомогательных операций, связанных с переходом УИС из одного многоструктурного макросостояния состояния в другое. Для формального описания указанной выше задачи планирования операций и распределения ресурсов в УИС использовался комплекс логико-динамических моделей.

Важным результатом проведенных исследований является выявленная автором зависимость значений обобщенного показателя качества модернизации УИС от назначенных экспертами весов показателей. Экспериментальное моделирование процесса модернизации УИС показало, что в этом случае корректно синтезировать оптимальный план распределения операций и ресурсов в СлО (с точки зрения максимизации значений обобщенного показателя качества) можно только в случае полного перебора (с заданным шагом) вариантов значений весовых коэффициентов, отражающих значимость частных показателей качества модернизации. Также полученные результаты моделирования подтвердили наличие неочевидных (неявных) связей как между стратами СлО на этапе модернизации УИС, так и между частными показателями качества модернизации. Таким образом, традиционный подход, основанный на назначении весовых коэффициентов, исключает возможность учета неявные знания экспертов о предметной области, что, по мнению автора, снижает обоснованность принимаемых решений.

В докладе представлены результаты, которые были получены в результате исследований разработанного прототипа программно-математического обеспечения. Попытки использования при оптимизации процессов модернизации и функционирования УИС в соответствующих логико-динамических моделях (модель управления БП, модель функционирования УИС, модель модернизации ИС) больше 4-5 показателей качества существенно усложняет интерпретацию результатов. Необоснованная избыточность требований к разрабатываемым планам приводит к неустойчивости получаемых решений. В ходе исследований было установлено, что при решении рассматриваемой задачи планирования целесообразно не более трех показателей качества программного управления модернизацией и функционированием УИС.

Исследования, выполненные по данной тематике, проводились при частичной финансовой поддержке грантов РФФИ (№№ 17-29-07073-офи-м, 18-07-01272, 18-08-01505, 19–08–00989, 20-08-01046), в рамках бюджетной темы №№0073–2019–0004.

СПИСОК ЛИТЕРАТУРЫ

1. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. 410 с.
2. Технология системного моделирования / Е.Ф. Аврамчук, А.А. Вавилов, С.В. Емельянов и др.; Под общ. ред. С.В. Емельянова и др. – М.: Машиностроение; Берлин: Техника, 1988.
3. Имитационное моделирование производственных систем / А.А. Вавилов, Д.Х. Имаев, В.И. Плескунин и др. – М.: Машиностроение; Берлин: Ферлаг Техник, 1983.
4. Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. – М.: Высшая школа, 1989.
5. Калинин В.Н., Резников Б.А. Теория систем и управления (структурно-математический подход). – Л.: ВИКИ, 1987
6. Соколов Б.В., Юсупов Р.М. Комплексное моделирование функционирования автоматизированной системы управления навигационными космическими аппаратами // Проблемы управления и информатики.- 2002.-№5.
7. Нечёткие множества в моделях управления и искусственного интеллекта / Под ред. Д.А. Поспелова. – М.: Наука, 1986.
8. Скурихин В.И., Забродский В.А., Копейченко Ю.В. Адаптивные системы управления машиностроительным производством. – М.: Машиностроение, 1989.
9. Захаров В. В. Динамическая интерпретация формального описания и решения задачи модернизации сложных объектов // Приборостроение. 2019. №10.

УДК 519.2

ДИНАМИЧЕСКАЯ МОДЕЛЬ НАДЕЖНОСТИ ТЕХНИЧЕСКОЙ СИСТЕМЫ С УЧЕТОМ ВЛИЯНИЯ ЭКСПЛУАТАЦИОННЫХ НАГРУЗОК

Марков Вячеслав Сергеевич, Сидоренко Татьяна Владимировна
Санкт-Петербургский научный Центр Российской академии наук
Университетская наб., 5, Санкт-Петербург, 199034, Россия
e-mails: markov@spbrc.nw.ru, puma@spbrc.nw.ru

Аннотация. В статье предлагается математическая модель надежности, описывающая динамику накоплений повреждений в технической системе (ТС) с учетом влияния переменных эксплуатационных нагрузок. Решена задача синтеза управлений, оптимальных по показателям надежности,безопасности и риска.

Ключевые слова: динамическая модель надежности, параметры надежности, эксплуатационные нагрузки.

DYNAMIC MODEL OF TECHNICAL SYSTEM RELIABILITY TAKING INTO ACCOUNT THE INFLUENCE OF OPERATIONAL LOADS

Markov Vyacheslav, Sidorenko Tatiana
The St. Petersburg scientific Center of the Russian Academy of Sciences Russia
5 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: markov@spbrc.nw.ru, puma@spbrc.nw.ru

Abstract. The article proposes a mathematical model of reliability that describes the dynamics of damage accumulation in a technical system (TS), taking into account the influence of variable operating loads. The problem of synthesizing controls that are optimal in terms of reliability, safety and risk is solved.

Keywords: dynamic reliability model, reliability parameters, operational loads.

Одной из актуальных задач проектирования и эксплуатации технических систем является задача надежной оценки их ресурса, диагностики выработанного и прогноза остаточного ресурса в процессе эксплуатации. На практике способ учета влияния эксплуатационных нагрузок на систему применяется при рассмотрении эмпирических моделей, построенных по экспериментальным данным зависимостей показателей надежности от уровней эксплуатационных факторов, если накоплен достаточный экспериментальный материал путем испытаний на натурных образцах [1]. Полуэмпирические модели накопления повреждений не включают явного описания физических явлений, которые происходят в материале в процессе его повреждения. Расчет накопления усталостных повреждений элементов ТС выполняется с использованием гипотезы кумулятивного разрушения (гипотезы Майнера) [2]. Согласно гипотезе, усталостные повреждения, вызываемые различными по величине напряжениями, суммируются. Повреждение отличается от отказа тем, что объект сохраняет своё работоспособное состояние. При накоплении повреждений конструкция или ее элемент теряет своё работоспособное состояние, что в свою очередь, может привести к отказу. Для большинства технических систем в настоящее время разработаны детерминированные модели, достаточно точно описывающие состояние системы с учетом внешних управляющих и эксплуатационных воздействий, но они отражают только те процессы, в которых предполагается отсутствие всяких случайных воздействий.

В данной работе рассматривается динамическая модель надежности системы, описывающая динамику накопления повреждений в ТС и возникновение в ней нежелательных случайных событий с учетом влияния переменных управляющих и эксплуатационных нагрузок. Сам процесс эксплуатации системы описывается движением изображающей точки вдоль траектории в многомерном векторном пространстве состояний системы. Каждому состоянию системы и текущему значению внешнего воздействия сопоставляется значение, характеризующее опасность отказа. Динамика самой системы (изменение ее вектора состояния во времени) достаточно точно описывается системой обыкновенных дифференциальных уравнений. Сам отказ трактуется как случайное событие, изображающее остановку точки при движении вдоль детерминированной траектории [3]. После отказа дальнейшее функционирование системы не рассматривается. Таким образом, на траекториях функционирования системы, имеем семейство распределений случайной величины - момент отказа. В дальнейшем полагаем, что рассматриваемое семейство распределений времени отказа можно описать марковским процессом. Изменяя различные начальные условия, внешние возмущающие и управляющие воздействия, можно получить различные траектории системы в пространстве состояний, для каждой из которых процесс накопления повреждений будет различным.

В результате этого от модели со случайным процессом и детерминированной границей области безотказной работы можно перейти к модели с детерминированным процессом и случайной границей области безотказной работы. Система уравнений, задающая динамику ТС в пространстве состояний, дополняется уравнением, вытекающим из свойств функции опасности, и учитывает изменение вероятности безотказной работы на траекториях эксплуатации системы. Полученная расширенная система дифференциальных уравнений полностью определяет функционирование ТС при произвольных возмущающих и управляющих воздействиях, оптимальных по показателям надежности, безопасности и риска.

СПИСОК ЛИТЕРАТУРЫ

1. Копур К.,Ламберсон Л.Надежность и проектирование систем./ К.Копур.-М.;Мир,1980.- 231с.
2. Miner, M.A., Cumulative damage in fatigue / M.A. Miner // J. Appl. Mech.,1945, no.67,pp.159-164.
3. Проурзин В.А.Алгоритмы анализа и оптимизации технико-экономического риска при проектировании сложных систем.//Автоматика и телемеханика.2003, №7

УДК 519.725, 512.62

МЕТОД СИНТЕЗА ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

Стародубцев Виктор Геннадьевич[1,3], Салухов Владимир Иванович[2], Краев Вячеслав Денисович[1]

[1] Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия

[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

[3] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mails: vgstarod@mail.ru, vis2601@bk.ru

Аннотация. Разработан метод синтеза последовательностей Гордона-Миллса-Велча (ГМВП), основанный на аналитическом определении полиномов-сомножителей $h_{ci}(x)$ проверочного полинома $h_{\Gamma}(x)$ ГМВП с учетом взаимосвязи корней $h_{ci}(x)$ с корнями проверочного полинома $h_{МП}(x)$ базисной М-последовательности.

Ключевые слова: псевдослучайные последовательности, конечные поля, неприводимые и примитивные полиномы, структурная скрытность, децимация, регистры сдвига.

METHOD FOR SYNTHESIS OF GORDON–MILLS–WELCH SEQUENCES FOR DIGITAL INFORMATION TRANSMISSION SYSTEMS

Starodubtsev Viktor[1,3], Salukhov Vladimir[2], Kraev Vyacheslav[1]
[1] Mozhaysky Military Space Academy
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[3] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: vgstarod@mail.ru, vis2601@bk.ru

Abstract. A method for synthesis of Gordon–Mills–Welch sequences (GMWS), based on determining polynomial factors $h_{ci}(x)$ of check polynomial $h_{\Gamma}(x)$ for the GMWS analytically taking into account the relationship of their roots with the roots of check polynomial $h_{МП}(x)$ for the basic M-sequence is developed.

Keywords: pseudorandom sequences, finite fields, indivisible and primitive polynomials, structural secrecy, decimation, shift registers.

Одним из направлений повышения достоверности передачи цифровой информации по радиоканалам, включая каналы спутниковой связи, является применение сигналов с расширенным спектром, формируемых на основе псевдослучайных последовательностей (ПСП) [1–3]. В качестве ПСП широко используются М-последовательности (МП), последовательности Голда, малого и большого множеств Касами, ГМВП [4–6].

Среди ПСП, обладающих двухуровневой периодической автокорреляционной функцией (ПАКФ), можно выделить МП и ГМВП [7–8]. При этом ГМВП обладают более высокой структурной скрытностью, что определяет приоритетность их использования в системах передачи дискретной информации, к которым предъявляются повышенные требования по конфиденциальности.

Формирование двоичных ГМВП осуществляется над конечными полями с двойным расширением GF[(2m)n]=GF(2s) (s=m·n). Известные методы формирования ГМВП [9–11] основаны на предварительном формировании и матричном представлении базисной МП, ее преобразовании в ГМВП, вычислении проверочного полинома hГ(x) с помощью алгоритма Берлекемпа и разложении полученного полинома на сомножители hci(x). На основании данных сомножителей строятся регистры сдвига, входящие в устройство формирования ГМВП.

Цель работы – разработка метода синтеза ГМВП, основанного на аналитическом определении полиномов-сомножителей hci(x) проверочного полинома hГ(x).

При разработке метода учитывалась взаимосвязь корней проверочного полинома hМП(x) базисной МП и корней полиномов-сомножителей hci(x) проверочного полинома hГ(x) ГМВП, формируемой над расширенным полем GF[(2m)n].

Метод синтеза включает три составляющих: алгоритм определения полиномов-сомножителей hci(x) проверочного полинома ГМВП, методику определения полных перечней проверочных полиномов hr(x) и алгоритм определения начальных состояний регистров сдвига, построенных по полиномам hci(x) в устройствах формирования ГМВП.

Основу метода синтеза составляет алгоритм определения полиномов-сомножителей hci(x), отличительной особенностью которого является то, что общий проверочный полином hГ(x) ГМВП не вычисляется, а его сомножители hci(x) находится непосредственно по значению параметра r, определяемого в поле GF(2m) [7-12].

Второй составляющей метода является методика определения полных перечней проверочных полиномов hГ(x), разработанная в [11-12]. Основой методики является положение о том, что корни полиномов hci(x) – сомножителей проверочного полинома hГ(x) – являются определенными фиксированными степенями корней проверочного полинома hМП(x) базисной МП, с помощью которой формируется ГМВП. Методика определения полных перечней проверочных полиномов hГ(x) ГМВП учитывает свойство повторяемости соотношений между корнями базисной МП и корнями полиномов-сомножителей для всех примитивных полиномов расширенного поля GF[(2m)n].

Третьей составляющей метода является предложенный в [11] алгоритм определения начальных состояний регистров сдвига, входящих в устройство формирования ГМВП, который основан на децимации символов базисной МП по индексам, определяемым соотношением показателей степени корней полинома hМП(x) базисной МП и корней полиномов-сомножителей hci(x).

Научная новизна предлагаемого метода заключается в разработке алгоритма определения полиномов-сомножителей hci(x), которая проводилась на основе анализа результатов, полученных в [10-12].

Для допустимых значений периода N и параметров m и n расширенного поля GF[(2m)n] вид формируемой ГМВП, ЭЛС и перечень сомножителей проверочного полинома полностью определяется значением параметра r. При этом показатели степени корней всех полиномов-сомножителей формируемой ГМВП должны иметь одинаковые значения функции g(r), определяемой как число единиц в двоичном представлении параметра r.

Алгоритм определения полиномов-сомножителей hci(x) основан на том, что для элемента βr = (trmn,m(αi))r, принадлежащего подполю GF(2m), его p-сопряженные элементы с нечетными показателями

степени являются, во-первых, непосредственно корнями части сомножителей степени s=m·n проверочного полинома ГМВП, а во-вторых, выступают в качестве образующих элементов для различных p-сопряженных классов поля GF[(2m)n] при вычислении остальных сомножителей hci(x). Данные элементы рассматриваются как корни полиномов-сомножителей нулевого уровня. Отметим, что для каждого значения r общее число элементов с нечетными показателями степени в подполе GF(2m), равно значению функции g(r). Например, в подполе GF(25) поля GF[(25)2] для значения r=13 p-сопряженными элементами для элемента β13 являются элементы β26, β21, β11, β22. Число элементов с нечетными показателями степени равно значению функции g(1310)=g(11012)=3, то есть это элементы β13, β21, β11.

Для определения полиномов первого и более высоких уровней вводится вспомогательный параметр ki = 2i(2m–1), i=1, 2,…, 2mn-m-1, необходимый для вычисления показателей степени корней данных полиномов. Выражение для параметра ki получено эмпирическим путем на основе анализа показателей степени корней полиномов-сомножителей для ГМВП с периодами N=63, 255, 511, 1023.

На i-ом уровне показатели степени корней полиномов определяются путем сложения показателей нулевого уровня и параметра ki. При выполнении данной операции могут быть получены показатели степени корней неприводимых полиномов, не являющихся полиномами-сомножителями проверочного полинома ГМВП. Поэтому полученные показатели необходимо проверить, во-первых, по параметру g(r) и, во-вторых, по совпадению с показателями корней полиномов более низкого уровня. Обе проверки являются достаточно тривиальными. Вычисления для более высоких уровней продолжаются до получения общего числа сомножителей M = ls /S степени S проверочного полинома ГМВП.

Полученные результаты позволяют синтезировать устройства формирования ГМВП с заданными показателями линейной сложности в широкополосных радиоканалах систем передачи цифровой информации, к которым предъявляются повышенные требования по конфиденциальности, включая требования по повышению их структурной скрытности.

СПИСОК ЛИТЕРАТУРЫ

1. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992.
2. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: пер. с англ. М.: Вильямс, 2003.
4. Cho Chang-Min, Kim Ji-Youp, No Jong-Seon. New p-ary sequence families of period (p^n-1)/2 with good correlation property using two decimated m-sequences // IEICE Transactions on Communications. 2015. Vol. E98, № 7, P. 1268.
5. Zhang T., Li S., Feng T., Ge G. Some new results on the cross correlation of m-sequences / IEEE Transactions on Information Theory. 2014. Vol. 60, № 5. P. 3062.
6. Golomb S.W. Two-valued sequences with perfect periodic autocorrelation // IEEE Transactions on Aerospace and Electronic Systems. 1992. Vol. 28, № 2. P. 383.
7. No Jong-Seon. Generalization of GMW sequences and No sequences // IEEE Transactions on Information Theory. 1996. Vol. 42, № 1, P. 260.
8. Chung H., No J.S. Linear span of extended sequences and cascaded GMW sequences // IEEE Transactions on Information Theory. 1999. Vol. 45, №6, P. 2060.
9. Юдачев С.С., Калмыков В.В. Ансамбли последовательностей GMW для систем с кодовым разделением каналов // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. №1. URL: http:// elibrary.ru/item.asp?id=17650851 (дата обращения 13.06.2020).
10. Стародубцев В.Г. Алгоритм формирования последовательностей Гордона-Миллса-Велча // Изв. вузов. Приборостроение. 2012. Т. 55, № 7. С. 5.
11. Стародубцев В.Г. Формирование последовательностей Гордона-Миллса-Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2015. Т. 58, №6. С.451.
12. Стародубцев В.Г., Попов А.М. Последовательности Гордона-Миллса-Велча с периодом *N*=1023 // Изв. вузов. Приборостроение. 2017. Т. 60, № 4. С. 318.

УДК 519.725

АЛГОРИТМ ФОРМИРОВАНИЯ ПЯТЕРИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА ДЛЯ СИСТЕМ ПЕРЕДАЧИ ЦИФРОВОЙ ИНФОРМАЦИИ

Стародубцев Виктор Геннадьевич[1,3], Салухов Владимир Иванович[2], Черкасов Андрей Юрьевич[1]

[1] Военно-космическая академия имени А.Ф. Можайского
Ждановская ул., 13, Санкт-Петербург, 197198, Россия

[2] Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

[3] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия

e-mails: vgstarod@mail.ru, vis2601@bk.ru

Аннотация. Разработан алгоритм формирования пятеричных последовательностей Гордона-Миллса-Велча (ГМВП) с периодом $N=5^4-1=624$ над конечным полем GF $[(5^2)^2]$. Общее число пятеричных ГМВП с периодом $N=624$ равно 144. Эквивалентная линейная сложность пятеричных ГМВП равна ls=12, 24, 40.

Ключевые слова: пятеричные псевдослучайные последовательности; конечные поля; примитивные полиномы; функция корреляции; эквивалентная линейная сложность.

ALGORITHM FOR THE FORMATION OF THE QUINARY GORDON–MILLS–WELCH EQUENCES FOR DIGITAL INFORMATION TRANSFER SYSTEMS

Starodubtsev Viktor[1,3], Salukhov Vladimir[2], Cherkasov Andrey[1]
[1] Mozhaysky Military Space Academy
13 Zhdanovskaya St, St. Petersburg, 197198, Russia
[2] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[3] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: vgstarod@mail.ru, vis2601@bk.ru

Abstract. An algorithm has been developed for the formation of the quinary Gordon-Mills-Welch sequences (GMWS) with a period of $N=5^4-1=624$ over a finite field $GF[(5^2)^2]$. The total number of quinary GMWS with a period of $N=624$ is 144. The equivalent linear complexity of the quinary GMWS is equal to ls = 12, 24, 40.

Keywords: quinary pseudorandom sequences; finite fields; primitive polynomials; correlation function; equivalent linear complexity.

В современных системах передачи цифровой информации (СПЦИ), включающих системы управления, связи и навигации, широко используются сигналы с расширенным спектром (СРС), которые строятся на основе дискретных псевдослучайных последовательностей (ПСП) с заданными корреляционными и структурными свойствами [1–2]. При этом в системах связи с множественным доступом с кодовым разделением в основном применяются двоичные последовательности [3–4].

В СПЦИ при выборе ПСП должны учитываться как их корреляционные свойства, так и структурная скрытность. В качестве показателя структурной скрытности ПСП используется такой параметр как эквивалентная линейная сложность (ЭЛС), численно равная степени проверочного полинома, на основании которого формируется данная последовательность [5–6].

В существующих телекоммуникационных системах применяются в основном двоичные МП, последовательности Голда, малого и большого множеств Касами, а также ГМВП [7–10].

Перспективным направлением развития СПЦИ является переход от двоичных к многопозиционным сигналам. Недвоичные сигналы с расширенным спектром формируются на основе недвоичных ПСП и обладают более высокой информативностью [3]. Кроме того, для определенных значений периода недвоичные ПСП могут обеспечить более высокую ЭЛС по сравнению с двоичными последовательностями. Среди недвоичных последовательностей, обладающих одинаковой двухуровневой ПАКФ, можно выделить МП и ГМВП. При этом предпочтительность применения ГМВП определяется их более высокой структурной скрытностью по сравнению с МП. Например, в [11] разработан алгоритм формирования и выполнена оценка линейной сложности троичных ГМВП с периодом N=80.

Широкому применению недвоичных ГМВП в системах передачи данных препятствует отсутствие практически реализуемых алгоритмов формирования данных последовательностей.

Цель работы – разработка алгоритма формирования пятеричных ГМВП с периодом N=624, основанного на матричном представлении базисной МП с использованием структурных свойств проверочных полиномов.

Формирование ГМВП осуществляется в конечных полях с двойным расширением GF[(5m)n]=GF(5S) (S=m·n) на основе базисной МП с аналогичным периодом, построение которой реализуется с помощью примитивного полинома, называемого проверочным и определяемого из таблиц неприводимых полиномов [12].

В [5, 9-10] показано, что двоичные ГМВП строятся над конечными полями с двойным расширением вида GF[(2m)n] путем представления МП, которые будем называются базисными последовательностями, в виде матрицы размерности [J×L]=[(2m–1)×(2m+1)].

Для формирования недвоичных ГМВ-последовательностей может быть использован аналогичный подход с учетом особенностей построения конечных полей с характеристикой p > 2.

Алгоритм формирования пятеричных ГМВП над конечным полем с двойным расширением GF[(52)2] с периодом N=54–1=624 основан на матричном представлении пятеричной М-последовательности (МП) с примитивным полиномом hМП(x) [3]. Проверочный полином hГ(x) ГМВП может быть представлен в виде произведения неприводимых полиномов-сомножителей hci(x) четвертой степени. На основании соотношений между корнями полинома hМП(x) базисной МП и корнями полиномов hci(x) может быть сформирован весь перечень ГМВП с периодом N=624.

Формализованная запись алгоритма.

Шаг 1. Ввод исходных данных: выбор минимального примитивного полинома h1(x) в конечном поле GF[(52)2]=GF(54); задание периода М-последовательности N=54–1=624 с параметром r1=1; задание параметра ri >r1 (ri =7, 13, 19), определяющего ЭЛС формируемой ГМВ-последовательности.

Шаг 2. Формирование МП в соответствии с коэффициентами полинома h1(x) для S=4 начальных символов d0 = trS,1α0, d1 = trS,1α1,d2 = trS,1α2, …, dS-1 = trS,1αS-1, где trS,1α1 – функция следа из расширенного поля в простом поле.

Шаг 3. Представление МП в виде квазиквадратной матрицы FМП размерности [J×L] = [(54–1) ×(54+1)]. Столбцы матрицы FМП (кроме столбца, состоящего из нулей) являются различными циклическими сдвигами более короткой МП с периодом N = 24, называемой характеристической последовательностью (ХП).

Шаг 4. Определение номеров сдвигов ХП1, последовательная запись которых образует правило формирования (ПФ) Ip.

Шаг 5. Для последовательности ХП1 определение по алгоритму Берлекемпа-Месси проверочного полинома hХП1(x).

Шаг 6. Выбор полинома hХП2(x), отличного от hХП1(x), и формирование ГМВП из базисной МП путем замены в матрице FМП столбцов ХП1 на ХП2 в соответствии с правилом формирования Ip.

Шаг 7. Определение (по алгоритму Берлекемпа-Месси) проверочного полинома ГМВП hГ(x).

Шаг 8. Разложение полинома hГ(x) ГМВП и определение полиномов-сомножителей hci(x) и минимальных показателей степени их корней, последовательность которых образует вектор сомножителей.

Шаг 9. Построение регистров сдвига с линейными обратными связями (РС ЛОС) в соответствии с полиномами hci(x).

Шаг 10. Определение начальных состояний регистров сдвига путем децимации символов базисной МП в соответствии с показателями степени корней полиномов hci(x) и вычисление начальных сдвигов формируемых последовательностей в соответствии с разработанным в [11] алгоритмом.

Шаг 11. Формирование выходной ГМВП путем посимвольного сложения по mod 5последовательностей с выходов регистров сдвига. Конец алгоритма.

Для каждого из 48 примитивных полиномов четвертой степени, являющихся проверочными полиномами для базисных МП, может быть сформировано по три ГМВП с ЭЛС ls=12, 24, 40. Общее число пятеричных ГМВП с периодом N=624 равно 144.

Устройство формирования ГМВП может быть представлено в виде совокупности трех, шести или десяти регистров сдвига при представлении полинома hГ(x) в виде произведения неприводимых полиномов hci(x).

Полученные результаты могут найти применение при формировании СРС в помехозащищенных СПЦИ, а также при формировании производных ПСП, допускающих аналитическое представление в конечных полях.

СПИСОК ЛИТЕРАТУРЫ

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: пер. с англ. // М.: Вильямс. 2003. 1104 с.
2. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения: пер. с англ. / Под ред. В.П. Ипатова // М.: Техносфера. 2007. 488 с.
3. Golomb S.W., Gong G. Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar // Cambridge University Press. 2005. 438 p.
4. CDMA: прошлое, настоящее, будущее / Под ред. Л.Е. Варакина и Ю.С. Шинакова // М.: МАС. 2003. 608 с.
5. Chung H.B., No J.S. Linear span of extended sequences and cascaded GMW sequences // IEEE Transactions on Information Theory. 1999. vol. 45, no. 6. pp. 2060–2065.
6. Rizomiliotis P., Kalouptsidis N. Results on the nonlinear span of binary sequences // IEEE Transactions on Information Theory. 2005. vol. IT–51. pp. 1555–1563.
7. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами // М.: Радио и связь. 1992. 152 с.
8. No Jong-Seon. Generalization of GMW sequences and No sequences // IEEE Transactions on Information Theory. 1996. vol. 42.no. 1.pp. 260–262.
9. Стародубцев В.Г., Бородько Д.Н., Мышко В.В. Алгоритм формирования ГМВ-последовательностей с периодом N=4095 в системах передачи телеметрической информации // Авиакосмическое приборостроение. 2018. №5. С. 3–15.
10. Стародубцев В.Г., Мышко В.В., Ткаченко В.В. Аппаратная и программная реализация алгоритма формирования последовательностей Гордона–Миллса–Велча // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. №3. С. 13–20.
11. Стародубцев В.Г., Чернявских А.Е. Формирование троичных последовательностей Гордона–Миллса–Велча на основе регистров сдвига // Изв. высш. учебн. заведений: Приборостроение. 2016. Т. 59, №3. С. 201–210.
12. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: пер. с англ. / Под ред. Р.Л. Добрушина и С.И. Самойленко // М.: Мир. 1976. 594 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

УДК 004.622

ПОДХОДЫ К ФОРМИРОВАНИЮ ЖУРНАЛОВ СОБЫТИЙ В РАЗНОРОДНЫХ СИСТЕМАХ МОНИТОРИНГА

Бекенева Яна Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: yana.barc@mail.ru

Аннотация. В работе представлены подходы, позволяющие формировать журналы событий на основе данных от разнородных устройств мониторинга. Рассмотрены особенности журналов событий, являющихся исходными данными для алгоритмов интеллектуального анализа процессов. Основной целью предлагаемых подходов является возможность учета нескольких параметров при формировании атрибутов журналов событий с целью получения более информативных моделей процесса. Приведены достоинства и недостатки, а также особенности использования каждого из подходов. Намечены пути для будущего исследования и развития предложенных подходов.

Ключевые слова: интеллектуальный анализ процессов; разнородные системы мониторинга; журналы событий; .xes файлы.

APPROACHES TO EVENT LOGS GENERATION IN HETEROGENEOUS MONITORING SYSTEMS

Bekeneva Yana
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: yana.barc@mail.ru

Abstract. The paper presents approaches for generating event logs based on data from heterogeneous monitoring devices. The features of event logs, which are the initial data for algorithms for intelligent analysis of processes, are considered. The main goal of the proposed approaches is the ability to take into account several parameters when forming attributes of event logs in order to obtain more informative process models. The advantages and disadvantages, as well as the features of using each of the approaches, are presented. Ways for future research and development of the proposed approaches are outlined.

Keywords: intelligent analysis of processes; heterogeneous monitoring systems; event logs; .xes files.

Современные информационные системы для мониторинга распределенных объектов имеют сложную иерархическую структуру и часто состоят из большого количества разнородных устройств. В таких системах мониторинга регистрация события осуществляется несколькими устройствами: видеокамерами, датчиками движения, системами контроля доступа, межсетевыми экранами, измерительными системами и т. д. Некоторые устройства генерируют данные в формате .xes [1], который применяется в качестве формата исходных данных для алгоритмов интеллектуального анализа процессов.

Обычно такие журналы событий содержат следующую информацию:

– Case ID: хранит дела (объекты), для которых организована последовательность событий журнала.
– Activity: хранит действия, выполненные как часть событий журнала.
– Timestamp: хранит дату и время регистрации событий.
– Resource: хранит главных действующих лиц событий журнала (тех, кто выполняет действия в рамках событий журнала).
– Other (другие данные): другая информация, с помощью которой описываются события.

При построении модели процесса используются первые четыре атрибута, а другие данные удаляются и не учитываются.

При анализе процессов в гетерогенных системах существуют следующие проблемы:

– Одно событие может быть описано с использованием данных с разных устройств мониторинга.
– Гетерогенные устройства мониторинга генерируют данные в разных форматах, т. е. не все устройства генерируют информацию в формате .xes.
– Формат .xes имеет ограниченное количество атрибутов. Анализируются только четыре атрибута, в то время как другие атрибуты удаляются и не учитываются. При этом возникает проблема удаления данных,

которые могут содержать важную информацию, которая может иметь решающее значение для результатов анализа.

В традиционных системах мониторинга, состоящих из устройств одного типа, можно генерировать данные в формате .xes и затем передавать их на центральный узел обработки [2]. Однако при использовании разнородных инструментов мониторинга данные требуют дополнительного преобразования. Существует много подходов к параллельной и распределенной обработке данных, формированию необходимых наборов данных в местах их генерации [3, 4]. Туманные вычисления стали широко использоваться в системах мониторинга здоровья пациентов [5, 6], системах умного дома [7] и т. д. Однако среди предложенных подходов создание объединенных журналов событий в формате .xes не рассматривается.

Существует целый ряд исследований, посвященных извлечению журналов событий из исходных данных в системах мониторинга [8, 9]. Существующие подходы основаны на объединении данных с устройств мониторинга и выборе отдельных атрибутов в качестве атрибутов формата .xes. Большинство подходов предоставляют только инструменты для выбора четырех значимых атрибутов из многомерного набора данных, и один из атрибутов должен быть меткой времени. Оставшиеся атрибуты отбрасываются и более не учитываются в процессе анализа.

Область исследований, связанных с внедрением технологий Process Mining в облачных вычислениях, активно развивается [10]. В [11] выделены основные проблемы, связанные с использованием Process Mining в среде облачных вычислений:

– Журналы на основе облачных вычислений создаются различными системами мониторинга, часто принадлежащими разным организациям, что приводит к проблемам выравнивания идентификаторов / случаев, особенно при наличии ограничений конфиденциальности.

– Облачные журналы часто содержат сотни редко заполненных атрибутов, которые требуют от аналитиков тщательного выбора / объединения атрибутов во время предварительной обработки.

Для решения данной проблемы выбора атрибутов и построения информативных моделей процессов предлагается два подхода к генерации журналов событий: централизованный и распределенный.

Данные подходы основаны на идее о том, что в каждой зоне мониторинга имеется заранее известный набор устройств мониторинга, генерирующих данные, содержащие определенные атрибуты. В то же время можно выделить ряд атрибутов, наиболее значимых для каждого типа событий, которые могут быть зафиксированы устройствами мониторинга. В рамках предлагаемых подходов предполагается выделение наиболее значимых атрибутов и их интеграция в атрибуты журнала событий.

Централизованный подход предполагает сбор и обработку данных от систем мониторинга централизованным устройством [12]. Такой подход может использоваться как для обработки данных, поступающих в режиме реального времени, так и данных, накопленных в течение некоторого периода времени и хранящихся в базах данных. Для корректного формирования журнала событий необходимо сначала сформировать единую запись о событии. Так как одно и то же событие может быть зафиксировано разными, подчас разнородными устройствами, то в базе данных может содержаться несколько записей, относящихся к одному событию. Следовательно, требуется объединить эти записи в одну, руководствуясь следующим правилом: для записей об одном событии должны совпадать пространственно-временные характеристики, а также должен быть одинаковым объект наблюдения. При этом предполагается, что разные устройства могут регистрировать события с некоторой задержкой, следовательно, временные характеристики могут отличаться на некоторое значение, которое признается допустимым для отдельно взятой зоны мониторинга.

После формирования записей о событии может быть реализовано формирование журналов событий в соответствии с форматом .xes.

Существенным недостатком такого подхода для решения задачи обработки данных в режиме реального времени является необходимость централизованного сбора данных, что предполагает существенную нагрузку как на каналы связи при передаче большого объема данных, так и на устройство, реализующее обработку данных.

Распределенный подход предполагает формирование журналов событий непосредственно на местах и предназначен для обработки данных в режиме реального времени [13]. Такой подход основан на набирающих популярность технологиях Интернета вещей и туманных вычислений. Основным достоинством туманных вычислений является возможность обрабатывать данные непосредственно у источника, а затем пересылать на центральный узел только необходимую информацию. Также, благодаря близости к источнику, «туман» помогает снизить время, затраченное на обработку и отправку данных. Также туманные вычисления позволяют установить дополнительные уровни защиты данных в локальной сети, что обеспечивает дополнительный уровень безопасности. Предполагается, что для извлечения необходимой информации из данных может быть использована вычислительная мощность самих устройств мониторинга. Информация от устройств, расположенных в зоне мониторинга, передается определенному устройству, которое осуществляет её обработку и генерацию лог-файла. Для обработки может быть как выделено некоторое специальное устройство, так и использована вычислительная мощность одного из устройств мониторинга, если это представляется возможным. Полученный лог-файл передается на центральный узел, где осуществляется интеграция лог-файлов со всех зон мониторинга и реализуется построение моделей интеллектуального анализа процессов.

Достоинством данного подхода является значительное снижение объема трафика по сравнению с централизованным подходом. Однако распределенный подход требует использования более современных устройств, способных осуществлять не только регистрацию событий, но и первичное преобразование данных, а

в некоторых случаях и обработку данных от всех устройств мониторинга, расположенных в данной зоне. Если же для каждой зоны использовать отдельное устройство для обработки данных, даже применение маломощного устройства потребует затрат как на его приобретение, так и на установку и интеграцию в локальную сеть.

В дальнейших работах планируется более детальная проработка каждого из подходов, исследование влияния атрибутов на информативность получаемых моделей, а также исследование нагрузки на каналы связи при использовании каждого из предложенных подходов.

Работа выполнена при финансовой поддержке Стипендии Президента Российской Федерации СП-2581.2019.5

СПИСОК ЛИТЕРАТУРЫ

1. W. M. P. van der Aalst, Extracting event data from databases to unleash process mining, BPM-Driving innovation in a digital world, Berlin Heidelberg, Springer, Cham, 2015, P. 105-128.
2. K. Diba, K. Batoulis, M. Weidlich, M. Weske, Extraction, correlation, and abstraction of event data for process mining, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2019, e1346.
3. A. Bakulev, M. Bakuleva, Moving Enterprise Integration Middleware toward the Distributed Stream Processing Architecture, In 2019 8th Mediterranean Conference on Embedded Computing (MECO), 2019, pp. 1-4.
4. J. Gialelis, G. Theodorou, M. Fokaeos, D. Karadimas, An Integrated Low Cost IoT Node based on Discrete Components for Customized Smart Applications; Use case on Precision Agriculture, In 2019 8th Mediterranean Conference on Embedded Computing (MECO), 2019, pp. 1-4.
5. S. Tuli, N. Basumatary, S. S. Gill, M. Kahani, R.C. Arya, G.S. Wander, G. S., R. Buyya, R. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments, Future Generation Computer Systems, 2020, 104, pp. 187-200.
6. A.A. Mutlag, M.K.A. Ghani, N.A. Arunkumar, M.A. Mohammed, O. Mohd, Enabling technologies for fog computing in healthcare IoT systems, Future Generation Computer Systems, 2020, 90, pp. 62-78.
7. M. Amadeo, A. Giordano, C. Mastroianni, A. Molinaro, On the integration of information centric networking and fog computing for smart home services, In The Internet of Things for Smart Urban Ecosystems, 2019, pp. 75-93, Springer, Cham.
8. A. Valencia-Parra, B. Ramos-Gutierrez, A.J. Varela-Vaca, M.T. Gomez-Lopez, A.G. Bernal, Enabling Process Mining in Aircraft Manufactures: Extracting Event Logs and Discovering Processes from Complex Data, In Proceedings of the Industry Forum at BPM 2019, pp. 166-177.
9. R. Andrews, C.G.J. van Dun, M.T. Wynn, W. Kratsch, M.K.E. Roglinger, A.H.M. ter Hofstede, Quality-informed semi-automated event log generation for process mining, Decision Support Systems, 2020, 113265.
10. N. M. El-Gharib, D. Amyot, Process Mining for Cloud-Based Applications: A Systematic Literature Review, 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), Jeju Island, Korea (South), 2019, pp. 34-43.
11. N.M. El-Gharib, Using Process Mining Technology to Understand User Behavior in SaaS Applications, Doctoral dissertation, Universite d'Ottawa/University of Ottawa, 2019, 133 p.
12. Y. Bekeneva, Algorithm for Generating Event Logs Based on Data from Heterogeneous Sources, In 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2020, pp. 233-236. IEEE
13. Bekeneva, Y. A., An Approach to the Distributed Generation of Event Logs Based on Data from Heterogeneous Monitoring Devices. In 2020 9th Mediterranean Conference on Embedded Computing (MECO), 2020, pp. 1-4.

УДК 517.98:519.2:621.039

НЕОБРАТИМОСТЬ, ХАОС И ВРЕМЯ ЛЯПУНОВА В ТЕОРИИ ДОЛГОСРОЧНОГО ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ СЛОЖНЫХ СИСТЕМ

Острейковский Владислав Алексеевич, Шевченко Елена Николаевна, Волков Александр Владиславович
Сургутский государственный университет
Ленина пр., 1, Сургут, 628412, Россия
e-mails: ova@surgu.ru, elenan_27@mail.ru, volk_234@mail.ru

Аннотация. Статья рассматривает вопросы применения теории детерминистического хаоса для прогнозирования необратимых макропроцессов в сложных динамических системах.

Ключевые слова: необратимость, детерминистический хаос, время Ляпунова.

IRREVERSIBILITY, CHAOS, AND LYAPUNOV TIME IN THE THEORY OF LONG-TERM FORECASTING THE STATE OF COMPLEX SYSTEMS

Ostreykovsky Vladislav, Shevchenko Elena, Volkov Alexander
Surgut State University
1 Lenin Av., Surgut, 628412, Russia
e-mails: ova@surgu.ru, elenan_27@mail.ru, volk_234@mail.ru

Abstract. The article examines the application of the theory of deterministic chaos for predicting irreversible macroprocesses in complex dynamical systems.

Keywords: irreversibility, deterministic chaos, Lyapunov time.

Время одно из самых загадочных свойств бытия человечества. Онтологии феномена время времени посвящено множество научных и публицистических книг, монографий и статей. С глубокой древности и до нашего просвещенного периода жизни накоплен огромный научный материал и несмотря на это некоторые аспекты онтологии феномена времени продолжают волновать многие поколения человечества. И в настоящее время еще далеко не все проблемы времени решены. Особо важны вопросы времени в задачах долговечности теорий надежности, безопасности и эффективности структурно и функционально сложных системы. Поэтому целью данной статьи является краткий анализ соотношений необратимых процессов, функций Ляпунова и

времени с позиций теоретико-вероятностного подхода и достижений теории операторов современного функционального анализа [1-4].

В качестве материальных объектов в статье рассматриваются сложные высокоответственные системы с длительным сроком эксплуатации: транспортные коммуникации, энергетические системы, комплексы летательных аппаратов , ядерные электростанции, подводные лодки и др. в сложных системах в связи с огромным количеством конструктивных элементов (до 10^6 и более) невозможно определить поведения (состояние) каждого элемента во времени, причём индивидуально они все “живут” под влиянием большого числа факторов внешней среды в том числе и фактора времени. Такие системы, как правило, неустойчивы и подвержены флуктуациям, т.е. их состояния являются хаотическими, понятие траектории для них утрачивает смысл. Для таких систем больше подходит название “хаотические” или система с “хаотическим режимом”.

Под хаотическим режимом понимается поведение системы, при котором первоначально близкие траектории экспоненциально разбегаются со временем. Разбегание траекторий описывается функцией $\exp(t/\tau)$, где $1/\tau$ – для хаотических систем по определению положительная величина. Величина $1/\tau$ - называется показателем Ляпунова, а само τ временем Ляпунова [5, 6]. Если для системы исследуется сравнительно большой отрезок времени, то “память” системы о её начальном состоянии почти полностью утрачивается. Этот характер хаотических систем определяется так называемым временным горизонтом, пропорциональным времени Ляпунова. Обнаруживается интересное свойство сложных хаотических систем: их временной горизонт порождает различия между прошлым и будущим. Теперь эволюция не допускает описание состояния системы в терминах траектории, а только в терминах ансамблей и вероятностей, каким бы ни было начальное состояние системы. В XX веке вероятности перестали быть воплощением незнания, а обрели объективной смысл.

Здесь следует подчеркнуть, что XX век характерен появлением структурно и функционально сложных динамических систем, так называемых "больших" систем с комплексом своеобразных свойств типа: уникальность и малосерийность структуры при крупносерийной элементной базе; восстанавливаемость и плановая профилактика, наличие сложных последовательно-параллельных структур, в которых присутствует большое число взаимосвязанных и взаимодействующих между собой подсистем, блоков и элементов, способных выполнять сложную функцию, функциональная избыточность, широкий спектр конструктивных элементов и разнообразие их отказов, большое количество точек контроля и управления и практически всегда наличие человека в контуре управления

При этом в теории сложных систем и физике неравновесных процессов считается, что основными физико-химическими процессами, ответственными за изменения физических свойств конструкционных материалов и, как следствие, за изменения функциональных характеристик элементов, является следующее: диффузия, химические реакции, адсорбция, распад твердых растворов, изменения механических, электрических и магнитных свойств твердых тел. Эти процессы – причина более сложных деградационных макропроцессов, которые проявляются при применении по назначению сложных систем.

Причем эти макропроцессы развиваются под воздействием комплекса эксплуатационных факторов, таких как: динамические и статистические механические нагрузки, термодинамические и тепловые удары, взаимодействия внешних и внутренних факторов с конструктивными элементами узлов, блоков и подсистем, перенос и осаждение продуктов коррозии, примесей и т.д., т.е. имеют типовой необратимый характер [2, 3].

Таким образом, можно сформулировать следующие выводы:

1) законы природы, управляющие поведением устойчивых систем детерминистичны и обратимы во времени. И, наоборот, законы описывающие хаотические системы, соответствуют вероятности и включают в себя необратимость;

2) эволюция хаотических систем во времени требует несводимого вероятностного описания, причём в терминах ансамблей и распределения вероятностей;

3) эволюцию распределения вероятностей состояния сложных систем надлежит описывать в пространстве, которое зависит от времени с учетом его модусов "прошлое- настоящее-будущее" [4].

Работа выполнена при финансовой поддержке РФФИ (проекты №№18-47-860007, 18-07-00391).

СПИСОК ЛИТЕРАТУРЫ

1. Пригожин И. Время. Хаос. Квант: К решению парадокса времени. / И. Пригожин, И. Стенгерс. / Изд. 5-е. – М.: Едиториал, 2003. – 240 с.
2. Острейковский В.А. Феномен асимметрии времени в теории неустойчивых и необратимых процессов сложных динамических систем: монография / В. А. Острейковский; Сургут. гос. ун-т. – Сургут : Печатный мир г. Сургут, 2017. – 268с. –(Серия «25 лет СурГУ»)
3. Острейковский, В. А. Феномен асимметрии внутреннего времени с учетом неустойчивости и необратимости процессов в теории прогнозирования состояния сложных динамических систем / В. А. Острейковский, С. А. Лысенкова, Е. Н. Шевченко // Надежность и качество сложных систем. – 2019. – № 1 (25). – С. 3–10. – DOI 10.21685/2307-4205-2019-1-1.
4. Острейковский В.А. Операторы энтропии, преобразования и внутреннего времени в теории долговечности сложных систем / В.А. Острейковский, Е.Н. Шевченко // Фундаментальные и прикладные проблемы науки. Том 1. – Материалы XIV Международного симпозиума. – М. РАН, 2019. – С. 91–98.
5. Ляпунов А.М. Общая задача об устойчивости движения / Собрание сочинений, Т.2. – М.: Изд. АН СССР, 1956.
6. Ляпунов А.М. Собрание сочинений. Т.2. – М.-Л., 1956. – 263 с.

УДК 517.98:519.2:621.039

ОНТОЛОГИЯ НЕОБРАТИМОСТИ И КОРНЕЙ ВРЕМЕНИ В ЗАДАЧАХ ДОЛГОВЕЧНОСТИ СЛОЖНЫХ СИСТЕМ

Острейковский Владислав Алексеевич, Шевченко Елена Николаевна, Андрей Викторович Сорочкин
Сургутский государственный университет
Ленина пр., 1, Сургут, 628412, Россия
e-mails: ova@surgu.ru, elenan_27@mail.ru, sorochkin_av@surgu.ru

Аннотация. Статья посвящена изучению вопросов использования понятий, описывающих характеристики самоорганизации, необратимости и свойств времени, в сложных динамических системах.

Ключевые слова: необратимость, детерминистический хаос, корни времени, сводимое описание.

ONTOLOGY OF IRREVERSIBILITY AND ROOTS OF TIME IN THE PROBLEMS OF LONGEVITY OF COMPLEX SYSTEMS

Ostreykovsky Vladislav, Shevchenko Elena, Sorochkin Andrey
Surgut State University
1 Lenin Av., Surgut, 628412, Russia
e-mails: ova@surgu.ru, elenan_27@mail.ru, sorochkin_av@surgu.ru

Abstract. The article is devoted to the study of the use of concepts that describe the characteristics of self-organization, irreversibility and properties of time in complex dynamical systems.

Keywords: irreversibility, deterministic chaos, roots of time, reducible description.

В настоящее время известны три формы законов природы:

– первая оперирует траекториями в классической механике (И. Ньютон) и волновыми функциями в квантовой механике (М. Планк);

– вторая оперирует статистической формулировкой законов природы (Дж. Гиббс, А. Эйнштейн), которая “приводима” или “сводима”;

– третья: законы природы носит вероятностный, но недостоверный характер.

Законы, описывающие поведение устойчивых систем, детерминистичны и обратимы во времени. И, наоборот, законы, описывающие поведение неустойчивых систем, соответствуют вероятностям и включают в себя необратимость. Эволюция неустойчивых (хаотических) систем требует несводимого вероятностного описания в терминах ансамблей и распределения вероятностей в пространстве, которое зависит от времени. Причём пространство становится “темпорализованным”, так как прошлое будущее играют разные роли. Эволюция систем при $t \to +\infty$ и при $t \to -\infty$ различна. А все системы, допускающие несводимое вероятностное описание, считаются хаотическими [1, 2].

В современной научной литературе проблеме асимметрии времени уделено большое внимание. Решены многие теоретические вопросы. Однако целый ряд проблем в этой области остаётся до сих пор до конца не решенными. Одна из таких проблем “старение-долговечность” ещё далека от своего решения. Особенно это касается сложных критически важных систем долгосрочного применения.

Поэтому целью данной статьи является описание результатов исследований в области онтологии необратимых процессов и корней времени в задачах долговечности сложных систем.

Ключевые слова: неустойчивость, необратимость, асимметрия времени, модусы времени "прошлое-настоящее-будущее", долгосрочное прогнозирование.

XIX век подарил человечеству новую теорию энтропии в области термодинамики, которая стала фундаментальным фактом в науке. От XIX века наука унаследовала два конфликтующих взгляда на описание природы: обратимую во времени, основанную на законах динамики, и эволюционную, основанную на энтропии. В природе встречаются как обратимые во времени процессы, так и необратимые. В обратимых процессах будущее и прошлое играют одинаковую роль. В необратимых процессах будущее ($t \to +\infty$) и прошлое ($t \to -\infty$) имеют разное направление времени.

Необходимо отметить, что необратимые процессы являются правилом, а обратимые – исключением. Обратимые процессы описываются уравнениями классической динамики, инвариантными относительно обращения времени как в случае второго закона Ньютона классической механики, так и в уравнении Шредингера в квантовой механике. Для необратимых процессов необходимо описание, которое нарушает симметрию времени. Различие между обратимыми и необратимыми процессами вошло в естествознании через понятие энтропии (эволюции), связанное со вторым началом термодинамики Р.Ю. Клаузиуса. Необратимые процессы производят энтропию. Увеличение энтропии обусловлено необратимыми процессами, происходящими во Вселенной. Формулировка второго начала термодинамики, предложенная Р.Ю. Клуазиусом, стала первой формулировкой эволюционный картины мира, основанной на существовании необратимых процессов.

По возражению А.С. Эддингтона энтропия – это "стрела времени". Но самое удивительное, что количественно эволюция времени “в прошлом” отличается от эволюции “в будущем” и при этом количество эволюций может быть больше единицы, как в теоретических построениях Ч. Дарвина в биологии.

Последние достижения неравновесных физики и химии XX века свидетельствуют о том, что стрела времени служит источником порядка (пример с термодиффузией).

Таким образом, достижения физики неравновесных процессов можно считать событием номер один в науке последних двух столетий, в котором описаны эффекты однонаправленности времени и по-новому интерпретируется термин “необратимость " и конструктивная роль стрелы времени. При этом строго доказано в [2], что необратимость приводит и к порядку, и к беспорядку. И не менее важно: конструктивная роль необратимых процессов становится еще более поразительный в сильно неравновесных ситуациях, в которых неравновесность приводит к новым формам когерентности. Именно с помощью необратимых процессов, связанных со стрелой времени, природа создает свои наиболее тонкие и сложные структуры такие, как как самоорганизация и диссипативные структуры.

Но это ещё не всё. Мы стали свидетелями, когда в XX веке физика неустойчивых систем, результатом которой стала идея “хаоса”, а понятия хаотической системы, детерминистического хаоса, несомненно, завоевали себе право называться вторым великим событием, повлиявшим на научное мировоззрение.

Таким образом приходим к формулированию некоторых выводов.

Макроскопическая необратимость представляет собой проявление случайного характера вероятностных процессов, происходящих в микроскопических масштабах.

Так как принятие второго закона термодинамики является фундаментальным фактом и появляется стрела времени, то любая формулировка законов природы, не учитывающая конструктивную роль энтропии, необратимости и стрелы времени, не может считаться удовлетворительной.

Достижения современной физики неравновесных и неустойчивых процессов свидетельствуют, что флуктуации, бифуркации и неустойчивости встречаются на всех уровнях описания систем.

Устойчивые и обратимые системы, порождающие определённость, соответствуют только идеализациям или аппроксимациям, и поэтому стрела времени сразу же объясняет две основные характеристики природы: её единство и разнообразие. Единство – потому что стрела времени является общей для всех частей мира (будущее у любых объектов существует всегда). Разнообразие – любые высокоорганизованные объекты (Земля, звезды, галактики) благодаря временным, неравновесным и необратимым процессам обладают общим свойством, позволяющим устанавливать связь случайности с моделями теории операторов функционального анализа.

В сложных системах порядок может поддерживаться с помощью самоорганизации. Самоорганизующиеся системы обладают возможностью адаптации к доминирующему типу окружающей среды, то есть могут реагировать на изменения в окружающей среде. Именно их термодинамическая реакция делает такие системы чрезвычайно гибкими и устойчивыми к возмущениям внешних условий.

Такое превосходство самоорганизующихся систем отчетливо видно на примере биологических систем. Последние могут создавать сложные продукты с непревзойденной точностью, эффективностью и скоростью.

Природа часто создает непредсказуемые новации, где возможности богаче реального. Наша Вселенная следует по пути, включающем в себя последовательность бифуркаций.

В соответствии с постулатом Ляпунова об экспоненциально разбегающихся траекториях это служит отличительным признаком детерминистического хаоса. Такое свойство позволяет применить методы теории операторов микроскопической энтропии, преобразования и внутреннего времени для расчета “возраста” систем (ресурса, срока службы и их остаточных значений) в теории долговечности сложных динамических систем [4,5].

Работа выполнена при финансовой поддержке РФФИ (проекты №№18-47-860007, 18-07-00391).

СПИСОК ЛИТЕРАТУРЫ

1. Пригожин И. От существующего к возникающему: Время и сложность в физических науках: Пер. с англ. / Под ред. Ю. Л. Климонтовича. – Изд. 2-е, доп. – М.: Едиториал УРСС, 2002. – 288 с.
2. Пригожин И. Р. Конец определенности. Время, хаос и новые законы природы / И. Р. Пригожин. – Ижевск: Ижевская республиканская типография. –1999. –216 с.
3. Острейковский В. А. Асимметрия времени в теории прогнозирования состояния сложных динамических систем: монография / В. А. Острейковский, Т. Ю. Денисова, Е.Н.Шевченко: Сургут.гос.ун-т – Сургут: ООО «Печатный мир». г.Сургут, 2018. – 574 с.
4. Острейковский, В.А. Математическое моделирование эффекта асимметрии внутреннего времени в теории долговечности структурно и функционально сложных критически важных систем / В.А. Острейковский, Е.Н. Шевченко // В книге: Итоги науки. Выпуск 37. Избранные труды Международного симпозиума по фундаментальным и прикладным проблемам науки. – М. : РАН, 2018. – С. 69–111.
5. Острейковский, В.А. О возможности использования эффекта асимметрии времени в задачах оценки долговечности сложных технических систем / В. А. Острейковский, С.А. Лысенкова, Е. Н. Шевченко // Надежность и качество сложных систем. 2019. – № 1. – С. 21–34.

УДК 004.42

СТРЕССОВОЕ ТЕСТИРОВАНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ РЕАЛЬНОГО ВРЕМЕНИ «FREERTOS» НА АППАРАТНЫХ МОДУЛЯХ, ПОСТРОЕННЫХ НА БАЗЕ ПРОЦЕССОРОВ «ЭЛВИС»

Павлов Фёдор Андреевич
Акционерное общество «Научно-производственное объединение «Импульс»
Киришская ул., 2, Санкт-Петербург, 195299, Россия
e-mail: pavlfyodor@yandex.ru

Аннотация. В статье рассмотрена методика создания и результаты стресс-теста операционной системы реального времени FreeRTOS на процессоры российской компании «Элвис».

Ключевые слова: операционная система реального времени, FreeRTOS, портирование на российскую элементную базу, процессоры компании «Элвис», Мультикор, стрессовое тестирование.

STRESS TESTING OF THE REAL-TIME OPERATING SYSTEM “FREERTOS” FOR HARDWARE MODULES BUILT ON THE BASIS ON “ELVIS” PROCESSORS

Pavlov Fedor
JSC "Scientific and Production Association" Impulse "
2 Kirishskaya St, St. Petersburg, 195299, Russia
e-mail: pavlfyodor@yandex.ru

Abstract. The article discusses the methodology for creating and the results of a stress test of the FreeRTOS real-time operating system on the processors of the Russian company Elvis.

Keywords: real-time operating system, FreeRTOS, porting to the Russian element base, Elvis processors, Multicor, stress tests.

Введение. Уровень развития вычислительной техники не стоит на месте. Операционные системы (ОС), обеспечивающие псевдопараллельное выполнение задач путём их поочерёдного переключения, получают всё большее распространение при проектировании встраиваемых систем. Работы по адаптации ОС для функционирования на процессорах различных архитектур становятся актуальной задачей, как для разработчиков самой ОС, так и для сторонних программистов. Но стабильное функционирование разрабатываемого программного обеспечения будет серьёзно затруднено или вовсе невозможно при малой стрессовой устойчивости операционной системы на конкретной элементной базе.

В контексте этой задачи использовалась ОСРВ FreeRTOS, которая была адаптирована для функционирования на базе интегральной микросхемы микроконтроллера 1892ВМ3Т, которая представляет собой однокристальную двухпроцессорную «систему на кристалле». Она разработана на основе спроектированной в ГУП НПЦ «ЭЛВИС» IP-ядерной платформы «МУЛЬТИКОР». На рисунке 2.2.1приведена структурная схема МС-12.

Проект стрес-стеста, помимо ядра ОСРВ содержит драйверы интерфейсов UART, Link (функционирует посредством DMA), функцию сбора статистики занятости процессора, а также простейшую функцию, выполняющуюся DSP-ядром.

Для осуществления стресс-теста необходимо во flash-память второго процессора платы УПМ-016 записать проект, осуществляющий работу Link-порта в режиме петли.

Суть теста заключается в следующем: в прикладной задаче, выполняемой FreeRTOS на первом процессоре, генерируется массив данных формата int на 0x10 элементов. Этот массив отправляется в очередь драйвера Link, который, в свою очередь, осуществляет его передачу в данный интерфейс. Второй процессор получает этот массив и отправляет его обратно. Первый процессор принимает его. Пакеты отправляются по факту уведомления о приёме предыдущего пакета. Так же в фоне выполняется функция DSP-ядра. Уведомления о каждом из этапов выполнения данного теста, а также его содержимое, отправляются в консоль посредством интерфейса UART. Частота отображения уведомлений – 1 уведомление на 500 выполнений отправки-приёма. Вывод статистики занятости процессора – два раза в одну минуту. Вместе с сообщением о распределении вычислительного ресурса процессора в консоль отправляется информация об общем времени работы системы и процент, который показывает время пребывания системы в прерывании по отношению ко всему времени работы.

ОСРВ стабильно осуществляет приём-передачу в стрессовом режиме в течение длительного периода времени. Нарушений в работе приёмопередатчиков и DSP-ядра не выявлено. Максимальное время функционирования системы составило 8 часов 24 минуты, по истечении данного срока стресс-тест был остановлен по инициативе испытателя. Время пребывания в прерывании не превышает 1% от всего времени функционирования системы.

Заключение. ОСРВ FreeRTOS показала свою стабильность при длительном воздействии стрессового характера на систему. Для завершения работ над ОСРВ на элементной базе НПЦ «ЭЛВИС» в целях оптимизации имеет смысл переработать текущий обработчик прерываний. Также нужно организовать работу прерываний от DSP при помощи своего обработчика прерываний. Данные замечания не являются критичными и на начало портирования ОСРВ к элементной базе АО «ПКК Миландр».

СПИСОК ЛИТЕРАТУРЫ

1. Павлов Ф. Использование ОСРВ FreeRTOS для обработки данных на микропроцессорах фирмы "ЭЛВИС"// Выпускная квалификационная работа магистра – 2019.
2. Павлов Ф. Адаптация ос реального времени FreeRTOS для функционирования на цифровых микропроцессорах фирмы «ЭЛВИС» // Выпускная квалификационная работа бакалавра – 2017.
3. А. Курниц, цикл статей о FreeRTOS из журнала // Компоненты и Технологии, 2011, вып. № 2.

УДК 004.82

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА ПРОЦЕССОВ И ЯВЛЕНИЙ В АКВАТОРИИ ЧЕРНОГО МОРЯ

Рябовая Валентина Олеговна, Холод Антон Леонидович
Федеральный исследовательский центр «Морской гидрофизический институт РАН» (МГИ)
Капитанская ул., 2, Севастополь, 299011, Россия
e-mail: valentina_rb@mail.ru

Аннотация. В статье рассматриваются информационные системы экологического мониторинга процессов и явлений в акватории Черного моря, дается оценка функционирования системы на основе метода структурного синтеза.

Ключевые слова: информационная система, мониторинг, анализ, синтез, прогноз.

INFORMATION SYSTEMS FOR ENVIRONMENTAL MONITORING OF PROCESSES AND PHENOMENA IN THE BLACK SEA AREA

Ryabovaya Valentina, Holod Anton
Federal Research Center "Marine Hydrophysical Institute of the Russian Academy of Sciences" (MGI)
2 Captain's St, Sevastopol, 299011, Russia
e-mail: valentina_rb@mail.ru

Abstract. The article discusses information systems for environmental monitoring of processes and phenomena in the black sea, and assesses the functioning of the System based on the method of structural synthesis.

Keywords: information system, monitoring, analysis, synthesis, forecast.

Введение. Развитие информационных систем мониторинга процессов и явлений в морской среде, а именно анализ и прогноз её состояния, всегда представляет собой актуальную задачу по мере того, как изменяется их сложность.

Ухудшение экологии и, прежде всего, морской среды, приобрело такие масштабы, что требуются неотложные согласованные действия [1]. Загрязнение нефтью Черного моря, поверхностного слоя и донных отложений говорит о значительной устойчивой деградации экосистемы.

Одной из стратегических целей современных информационных систем мониторинга является повышение эффективности их функционирования. Основной задачей исследования береговой и шельфовой зон является минимизация или полное исключение негативного влияния производственной деятельности на экосистему за счет внедрения современных природоохранных технологий и специального оборудования.

Информационные системы экологического мониторинга процессов и явлений в акватории Черного моря относятся к инновационным решениям и теоретически они должны быть оценены на основе существующих методик. Однако на деле применение стандартных методов анализа инноваций к таким системам связано с существенными трудностями [2].

Для развития информационных систем экологического мониторинга морской среды необходимо провести анализ данных, синтез, прогноз состояний, их оценку и т.п.

В новых научно-обоснованных программах мониторинга окружающей среды разработан ряд показателей качества, чтобы интегрировать значительные объемы обрабатываемых данных, классифицировать их и интерпретировать смысл интегральных оценок [3].

В Черноморском центре морских прогнозов (ЧЦМП) ФГБУН МГИ функционирует автоматическая оперативная система анализа и прогноза состояния Черного моря (http://bsmfc.net).

В состав системы входит два основных модуля: модуль, предназначенный для выполнения морских прогнозов, и модуль, предназначенный для хранения данных и их передачи потребителям в графической и цифровой формах представления данных. Взаимодействие между модулями осуществляется посредством внутренних компьютерных сетей передачи данных, файл-сервера данных и средств сети Internet. В модуль выполнения морских прогнозов входят подсистема ввода и подготовки входных данных, необходимых для выполнения морских прогнозов, три подсистемы диагноза и прогноза состояния морской среды и подсистема валидации результатов диагноза и прогноза физических полей Черного моря [4].

Безотказное функционирование системы морских прогнозов основано на тщательном проектировании ее структуры и достижения максимально возможного уровня автоматизации ее работы. Однако не всегда удается получить полный объем данных (ошибки при получении, на сервере, и т.д.) и в этом случае, для обеспечения более точного прогноза, их приходится дублировать или вводить «вручную».

Интерпретация данных экологических мониторинга морской среды, даже полученных от эффективной программы, часто неоднозначна. Нередко имеются результаты анализа или «предвзятых результатов» мониторинга, или достаточно спорное использование статистики, чтобы продемонстрировать правильность той или иной точки зрения.

В качестве теоретической платформы для построения такой методики выбрано проверенное сочетание вероятностно-статистического подхода к оцениванию эффективности с общими принципами системного анализа [5]. Главным показателем качества системы выбрана эффективность ее функционирования. Для описания

понятия эффективности применяется набор разнородных показателей, отражающих определенные квалиметрические признаки: квалификационные (по интегральности, принадлежности, характеру оценивания и наблюдений, типу шкалы, степени достаточности) и относительности наблюдений.

В процессе исследований также было выявлено, что при возникновении новых требований (или их корректировке) к данным (достоверность, своевременность и т.д.) и к работе самой системы (быстродействие, надежность, изменение частоты измерений), возможны проблемы оценки моделей системы. Для решения этой задачи применяется критериальный подход. Критериями, участвующими в отборе, являются: достоверность информации, своевременность реализации требований к системе и к данным мониторинга, надежность системы [6].

Для решения поставленной задачи используется метод структурного синтеза, а именно реструктуризация информационной системы экологического мониторинга морской среды, которая позволяет учесть дополнительную информацию о сочетаемости объектов и их функциональностей в составе одного решения [7].

Преимущество представленного метода, по сравнению с существующими – более полный учет данных, минимизация функциональной избыточности элементов системы в составе одного решения по мере наращивания задач.

Сбор и обработка данных мониторинга осуществляется множеством способов [8], однако время реорганизации системы (в зависимости от поставленных целей) может быть различным.

Особенностью информационных систем экологического мониторинга морской среды, по отношению к другим информационным системам, является необходимость сочетания точности оценок параметров, учета предельно-допустимой концентрации, сбора первичной информации, создания и ведения баз данных о состоянии и загрязнении компонентов природной среды, формирования (на основе первичной информации) комплексной оценки экологического состояния природных сред, анализа текущей экологической обстановки и прогнозирования динамики её развития.

Заключение. Информационные системы экологического мониторинга процессов и явлений в акватории Черного моря должны быть ориентированы на комплексное использование результатов экологического мониторинга, обеспечивая преобразование первичных результатов измерений в форму, пригодную для поддержки принятия решений, способствующих устойчивому развитию отдельных регионов и планеты в целом. По мере перехода от первичных результатов экомониторинга к знаниям о состоянии окружающей среды, следует менять и методы работы с информацией.

Работа выполнена при поддержке гранта РНФ № 17-77-30001 «Новые методы и суперкомпьютерные технологии анализа и прогноза Мирового океана и Арктического бассейна».

СПИСОК ЛИТЕРАТУРЫ

1. Дорофеев В.Л. Моделирование декадной изменчивости экосистемы Черного моря // Морской гидрофизический журнал. 2009. № 6. С. 71–81.
2. Korotaev G.K., Oguz T., Dorofeyev V.L. et al. Development of Black Sea nowcasting and forecasting system // Ocean Sci. 2011. V. 7. P. 1–21.
3. Иванчик А.М., Иванчик М.В. Процедуры контроля работы автоматизированных систем морского прогноза. Интеграция науки и практики как механизм эффективного развития современного общества: материалы XVI международной научно-практической конференции, г. Москва, 30 июня 2015 г. М.: Изд-во “Институт стратегических исследований”, 2015. С. 52–55.
4. Ратнер Ю.Б., Холод А.Л. Структура системы валидации результатов диагноза и прогноза состояния Черного моря // Экологическая безопасность прибрежной и шельфовой зон и комплексное использование ресурсов шельфа. Сб. научных трудов. Вып. 19. Севастополь: НПЦ “ЭКОСИ-Гидрофизика”, 2009. С. 199–202.
5. Юсупов Р.М. Концептуальные и научно-методические основы информатизации: научная монография / Р.М. Юсупов, В.П. Золотолотский // СПб. – 2000. – 455 с.
6. Рябовая В.О., Доронина Ю.В., Чесноков Д.И. Применение модельно-ориентированного проектирования для решения задачи структурного синтеза / В.О. Рябовая, Ю.В. Доронина, Д.И. Чесноков // Труды СПИИРАН. Выпуск 6 (49) — Санкт-Петербург: Изд-во СПИИРАН, 2016. — С. 122-143.
7. Imboden D., Pfenninger S. Introduction to Systems Analysis: Mathematically Modeling Natural Systems // Berlin, New York, Springer. — 2013. — 8. — P.235-252.
8. Кандырин Ю.В., Шкурина Г.Л. Процедуры генерации и выбора при проектировании технических объектов / Ю.В. Кандырин, Г.Л. Шкурина. — Волгоград.: Политехник,1999. — 105 с.

УДК 004.05

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРОЦЕССА ИНФОРМАЦИОННОГО ОБМЕНА В ВОЕННО-ТЕХНИЧЕСКОЙ СИСТЕМЕ

Тоискин Василий Евгеньевич
Филиал военной академии Ракетных войск стратегического назначения имени Петра Великого
Бригадная ул., 17, Серпухов, Московская обл., 142210, Россия
e-mail: vetoiskin@mail.ru

Аннотация. Рассматриваются свойства процесса информационного обмена, их показатели и взаимосвязи. Производится теоретико-множественная постановка проблемы оценивания эффективности процесса информационного обмена в интересах системы управления специального назначения.

Ключевые слова: информационный обмен; цикл управления; своевременность, достоверность, безопасность, устойчивость.

A CONCEPTUAL APPROACH TO EVALUATING THE EFFECTIVENESS OF THE INFORMATION EXCHANGE PROCESS IN THE MILITARY-TECHNICAL SYSTEM

Toiskin Vasiliy
Branch of military academy of the Strategic Missile Troops of Peter the Great
17 Brigadnaya St, Serpuhov, Moscow region, 142210, Russia
e-mail: vetoiskin@mail.ru

Abstract. The properties of the information exchange process, their indicators and relationships are considered. A set-theoretic formulation of the problem of evaluating the effectiveness of the information exchange process in the interests of a special-purpose management system is made.

Keywords: information exchange; cycle of management; timeliness, reliability, safety, stability.

Любая военно-техническая система является сложной организационно-технической системой в силу ряда особенностей [1]. Это обуславливает наличие системы управления в военно-технический системе как главной подсистемы, позволяющей достигать основной цели функционирования. В системе управления реализуется цикл управления. Следует отметить, что для выполнения требований к управлению по устойчивости, непрерывности, оперативности и скрытности накладываются определенные ограничения на время выполнения рассматриваемого цикла. Это обусловлено тем, что военно-техническая система должна выполнять свои функции в любых условиях обстановки, в том числе и при наличии деструктивных воздействий. Тогда увеличение времени выполнения одного этапа цикла управления приводит к сокращению времени на остальные этапы.

Пусть с точки зрения системы управления основными этапами цикла управления являются этапы принятия решения и его выполнения. Тогда из изложенного следует недопустимость увеличения времени на этап оценки обстановки и этап осуществления управляющего воздействия. Время выполнения данных этапов является случайным, что во многом определяется стохастичностью процесса информационного обмена (ИО). ИО осуществляется по средствам передачи сообщений различных типов – речь, видео, данные. ИО организуется с использованием ресурсов системы связи. В свою очередь система связи является также сложной организационно-технической системой, состоящей из множества узлов связи и множества каналов связи, объединение которых образует сеть связи, а также системы управления связью в интересах которой организуется служебный ИО.

Из изложенного выше следует взаимосвязь требований к управлению с требованиями к ИО и системе связи. Такая взаимосвязь формируется через соответствующие показатели основных свойств системы управления, ИО и системы связи и их взаимозависимости. Вербальное описание свойств и схем их взаимосвязи представлены в [2-5]. Из указанного следует, необходимость выполнения требований к ИО в интересах системы управления с использованием ресурсов системы связи, в условиях ограничений по времени и вероятности доведения информации с учетом наличия внутренних и внешних дестабилизирующих факторов.

Известно [6], что каждое свойство описывается некоторой переменной величиной, называемой показателем свойства, а совокупность этих показателей (определяемая взаимосвязью самих свойств) формирует показатель качества всей системы. В работе приводится анализ подходов к определению показателей основных свойств системы управления и системы связи, в результате которого делается вывод о целесообразности установления взаимосвязи рассмотренных показателей через определение показателей эффективности процесса информационного обмена.

Указано, что согласно методологии теории эффективности целенаправленных процессов [6], эффективность процесса информационного обмена есть комплексное операционное свойство, характеризующее его приспособленность к достижению цели реализуемой системой связи в интересах системы управления. Комплексность данного свойства заключается в наличии у процесса ИО атрибутивных свойств – достоверности, своевременности и безопасности.

В ГОСТ РВ 52216–2004 [7] даны следующие определения указанных атрибутивных свойств:

– достоверность – способность военной связи обеспечивать воспроизведение передаваемых сообщений в пунктах приема с заданной точностью;

– своевременность – способность военной связи обеспечивать передачу или доставку сообщений, или ведение переговоров в заданные сроки;

– безопасность – способность военной связи сохранение в тайне от противника содержания передаваемых сообщений и факта их передачи.

Проведено теоретико-множественное описание показателей данных свойств, в ходе которого отмечена их зависимость от внешних и внутренних деструктивных воздействий.

Отмечено, что ухудшение значений показателей эффективности ИО, вызванное воздействием внешних и внутренних факторов, могут носить комплексный характер за счет осуществления воздействия на несколько элементов военно-технической системы в течение короткого интервала времени. Следовательно, задача определения подходящего закона распределения показателей ИО в таких условиях носит нетривиальный характер и не может быть сведена к выбору одного из широко применяемых законов распределения.

Рассмотрен пример влияния комплексного воздействия деструктивных факторов на военно-техническую систему на значение одного из рассматриваемых показателей эффективности ИО, в предположении, что количество циклов «воздействие-восстановление» ограничено ресурсами каждой из сторон конфликта.

Проведен анализ показателей основных свойств процесса ИО. Сделан вывод о том, что рассмотренные показатели достоверности, своевременности и безопасности адекватно описывают процесс ИО в случае если за время доведения информации характеристики системы связи и системы управления в совокупности с интенсивностью и характером дестабилизирующих воздействий не претерпевают резких и значительных изменений. В противном случае указанных показателей недостаточно для адекватной оценки сложившейся ситуации и принятия мер по управлению процессом ИО, что приводит к увеличению времени самого ИО и времени на выполнение цикла управления.

Для устранения указанного недостатка предложено ввести понятие устойчивости процесса информационного обмена, по аналогии с устойчивостью управления и устойчивостью системы связи. Под устойчивостью ИО предложено понимать свойство процесса информационного обмена характеризующее его способность сохранять и восстанавливать заданное значение показателей эффективности процесса ИО на протяжении времени функционирования системы в условиях деструктивных воздействий различного происхождения. Оценивание устойчивости процесса информационного обмена целесообразно проводить по трем направлениям.

Во-первых, устойчивость процесса информационного обмена в направлении связи (соединение «точка-точка»). Здесь оценивается способность выполнять требования по своевременности, достоверности и безопасности при доведении некоторой информационной единицы (пакет, сообщение) на всем интервале функционирования рассматриваемой военно-технической системы в условиях воздействия деструктивных факторов.

Во-вторых, устойчивость процесса информационного обмена в совокупности направлений связи. Здесь оценивается способность выполнять требования по своевременности, достоверности и безопасности при одновременном доведении некоторых информационных единиц по разным направлениям связи в условиях воздействия деструктивных факторов.

И в-третьих, устойчивость процесса информационного обмена в сети связи. Здесь оценивается способность выполнять требования по своевременности, достоверности и безопасности при одновременном доведении некоторых информационных единиц по разным направлениям связи на всем интервале функционирования рассматриваемой военно-технической системы в условиях воздействия деструктивных факторов.

Таким образом, в работе рассмотрены свойства процесса информационного обмена, их показатели и взаимосвязи. Определена их зависимость от деструктивных факторов. Предложено оценивать эффективность процесса ИО на базе его устойчивости к совокупности внутренних и внешних деструктивных факторов.

СПИСОК ЛИТЕРАТУРЫ

1. Молчанов, А.А. Моделирование и проектирование сложных систем / А.А. Молчанов. – Киев : Выща шк. Головное изд-во, 1988. – 359 с.
2. Макаренко С. И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 113-164. URL: http://sccs.intelgr.com/archive/2017-02/05-Makarenko.pdf.
3. Михайлов, Р.Л. Помехозащищенность транспортных сетей связи специального назначения. Монография / Р.Л. Михайлов. – Череповец: ЧВВИУРЭ, 2016. – 128 с.
4. Касанин, С.Н. Методика совершенствования системы связи территориальных войск / С.Н. Касанин, С.И. Паскробка, А.А. Родионов, В.А. Сергиенко // Проблемы инфокоммуникаций. – Минск : 2017 №1 (5). – с. 24-33.
5. Боговик, А.В. Эффективность систем военной связи и методы ее оценки / А.В. Боговик, В.В. Игнатов. – СПб : ВАС, 2006. – 184 с.
6. Петухов, Г.Б. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем / Г.Б. Петухов, В.И. Якунин. – М.: АСТ, 2006. – 504 с.
7. ГОСТ РВ 52216–2004. Связь военная. Термины и определения : государственный военный стандарт Российской Федерации : издание официальное : принят и введен в действие Постановлением Госстандарта России от 29 января 2004 г. № 42-ст : введен впервые : дата введения 2004-01-29 / разработан 16 Центральным научно-исследовательским испытательным институтом Министерства обороны Российской Федерации (16 ЦНИИИ МО РФ). – Москва : Издательство стандартов, 2004. – 12 с.

УДК 621.391

ОЦЕНКА КАЧЕСТВА ДЕТЕКТИРОВАНИЯ ПРИНИМАЕМОГО СИГНАЛА ДЛЯ РАЗЛИЧНЫХ МЕТОДИК РЕКОНФИГУРАЦИИ ПАРАМЕТРОВ ПОДСИСТЕМЫ ЧАСТОТНО-ФАЗОВОЙ СИНХРОНИЗАЦИИ

Цимбал Владимир Анатольевич, Мокринский Дмитрий Викторович
Филиал военной академии Ракетных войск стратегического назначения имени Петра Великого
Бригадная ул., 17, Серпухов, Московская обл., 142210, Россия
e-mails: tsimbalva@mail.ru, dmitrimokrinski1991@mail.ru

Аннотация. Для подсистемы фазовой синхронизации на основе цифрового контура фазовой автоподстройки частоты и адаптивного RLS эквалайзера, приведены характеристики приема при различных вариантах реконфигурации управляющих параметров.

Ключевые слова: синхронизация; фазовая автоподстройка частоты; адаптивный эквалайзер, передаточная функция, вероятность битовой ошибки.

QUALITY ASSESSMENT OF DETECTION OF THE RECEIVED SIGNAL FOR DIFFERENT METHODS OF RECONFIGURATION SUBSYSTEM PARAMETERS: FREQUENCY-PHASE SYNCHRONIZATION

Tsimbal Vladimir, Mokrinskiy Dmitriy
Branch of military academy of the Strategic Missile Troops of Peter the Great
17 Brigadnaya St, Serpuhov, Moscow region, 142210, Russia
e-mails: tsimbalva@mail.ru, dmitrimokrinski1991@mail.ru

Abstract. For the phase synchronization subsystem based on the digital loop of the phase auto-tuning frequency and adaptive RLS equalizer, the characteristics of reception for various types of reconfiguration of control parameters are given.

Keywords: synchronization; phase-locked loop frequency; an adaptive equalizer, the transfer function, probability of bit error.

Известно, что декаметровый канал (ДКМВ) характеризуется целым комплексом негативных эффектов, существенно осложняющих качественное детектирование принимаемого сигнала. Одним из факторов (наравне с аддитивной и мультипликативной помехой [1-3]), вносящим критический вклад в качество приема, является наличие динамически изменяющегося во времени ухода частоты. Уход частоты может быть связан с движением передатчика и приемника относительно друг друга, а также с равномерным подниманием или опусканием отражающей области ионосферы в течение ограниченного интервала времени. Во втором случае будет иметь место классический эффект Доплера, т.е. изменение частоты принимаемого сигнала. По оценке П. Грина и М. П. Долуханова [4] значение максимального ухода частоты декаметровой (ДКМВ) линии связи во время сильных ионосферных возмущений может достигать 100 Гц. Сама по себе задача компенсации ухода частоты в канале связи не является новой. Основные подходы описаны в классических трудах теории фазовой синхронизации [5-7] - на современном этапе для цифровых систем связи в основе подсистемы фазовой синхронизации сигнала (ПФСС) лежат адаптированные классические методы, основанные на реализации цифрового (программно-реализованного) контура фазовой автоподстройки частоты (ЦФАПЧ) [8-9]. Тем не менее задача компенсации ухода частоты в условиях наличия замираний в канале связи, является не недостаточно изученной.

В ходе проведенных исследований по обоснованию структуры подсистемы частотно-фазовой синхронизации для комплекса модемного оборудования перспективного приемо-передающего комплекса декаметровой (ДКМВ) радиосвязи был предложен вариант [10,11], на основе цифрового контура фазовой автоподстройки частоты (ФАПЧ) и адаптивного эквалайзера (АЭ), включенного в контур цепи обратной связи. На основе математического аппарата z-преобразований были получены передаточные функции (ПФ) исследуемой системы [12,13] и проведен анализ их устойчивости при воздействии типовых возмущений в канале связи.

На основе анализа ПФ (1-5) методами теории автоматического управления и цифровой обработки сигналов [14], было показано, что контур ФАПЧ с фильтром второго порядка и АЭ, при воздействии типовых возмущений, является неустойчивым. При использовании в системе петлевого фильтра первого порядка, сохраняются качественные характеристики типового ФАПЧ [15] (астатизм первого порядка), изменяется лишь динамика переходного процесса, что не вносит существенного вклада в установившийся режим. Существенным недостатком полученной системы (из-за наличия первого порядка астатизма) является необходимость ее реконфигурации в зависимости от значения мгновенного ухода частоты в канале связи [16].

Существуют различные подходы к реконфигурированию подобных систем, классическим является использование схем поиска частоты, с последующей перестройкой ГУН (*Stand*), (при значениях ухода частоты превышающих полосу захвата и удержания контура) [17]. Существенным недостатком подобных систем является наличие длительного переходного процесса, в ходе которого не обеспечивается качественное детектирование принимаемого сигнала и возникают неустранимые ошибки приема. В соответствии с этим, предлагаются методики реконфигурации подсистемы частотно-фазовой синхронизации, основанные на перестройке пропорционального коэффициента усиления петлевого фильтра, а именно:

1. на основе поиска значения мгновенного ухода частоты, с использованием набора блоков согласованных фильтров, каждый из которых согласуется с ожидаемым сигналом с определенным сдвигом частоты несущей [18] (*M-1*);

2. на основе статистической обработки сигнала обучающей последовательности АЭ [19] (*M-2*).

На основе математической модели функционирования системы фазовой синхронизации, была построена имитационная модель в среде визуально-ориентированного программирования Simulink (пакет MatLab), состоящая из передающей стороны, приемной стороны и линии связи. Передающая сторона содержит следующие основные структурные элементы: генератор случайной бинарной последовательности; генератор обучающей последовательности АЭ; формирователь структуры пакета; конвертер бинарной последовательности в числовую; цифровой модулятор. Линия связи содержит: блок частотно-фазового рассогласования канала; блок мультипликативных помех; блок генерации аддитивной помехи. Приемная сторона состоит из подсистемы фазовой синхронизации; генератора обучающей последовательности; демодулятора; блока устранения избыточности и получателя сообщений.

Имитационное моделирование проводилось при следующих начальных условиях: структура пакета передачи информации (информационная последовательность *frn*=20 бит, обучающая последовательность для АЭ

frk=20 бит); тип алгоритма сходимости АЭ - *RLS* (рекуррентное вычисление весовых коэффициентов по критерию минимума суммы квадратов сигнала ошибки); количество прямых ветвей АЭ: *Fa_n*=20; количество обратных ветвей АЭ: *Fa_m*=20; параметры контура ФАПЧ: *Kd* = 1; *G1* - регулируемый параметр; *G2* = 0; KNCO = 1; тип модуляции сигнала: *QPSK*; характеристики канала связи: количество лучей распространения – 1, аддитивная помеха - ОСШ 1-30 (дБ); мультипликативная помеха - амплитудно-фазовое распределение пришедшего луча по закону Релея (коэффициент замираний - 0); параметры возмущения: величина ухода частоты $f_З$ = 72 (Гц), скорость ухода частоты – 4.4(Гц/с).

Анализ результатов имитационного позволил сделать следующие выводы: 1. при наличии аддитивной и мультипликативной помехи (с учетом одного луча распространения), при малых отношениях сигнал/шум (ОСШ < 5 (дБ)) существенными преимуществами обладает методика на основе системы согласованных по частоте фильтров (*M-1*) (при учете, что N > 4), по сравнению с *M-1*, выигрыш может составлять до 10%, по сравнению с *Stand* выигрыш может составлять до 5%; 2. при ОСШ >5 (дБ) результаты при использовании *M-1* с *N* > 4 и *M-3* – практически идентичные, при этом по сравнению с Stand выигрыш может составлять до 20%;

Учитывая специфику ДКМВ радиоканала, а именно, низкие значения коэффициента готовности (надежности) при ОСШ < 10 (дБ) [20] (как следствие возможности корректного функционирования с вероятностями битовой ошибки порядка, не менее чем 10^{-2}), также учитывая, что *M-2* существенно менее требовательна к вычислительным ресурсам цифровых сигнальных процессоров (из за отсутствия системы цифровых согласованных фильтров), по сравнению с *M-1*, обоснованным, для данного канала связи, является использование методики на основе статистической обработки сигнала обучающей последовательности АЭ.

СПИСОК ЛИТЕРАТУРЫ

1. Yoshii K., Saitou M., Liu J, Shimamoto S, “Prediction of Ionospheric fading for long distance emergency communication” 2019 IEEE International Conference on Communications Workshops, ICC Workshops 2019, Proceedings 2019. pp. 875-881.
2. Bianchi C., Baskaradas J.A., Pezzopane M., Pietrella M., Sciacca U., Zuccheretti E. “Fading in the HF ionospheric channel and the role ofirregularities” Advances in Space Research (includes Cospar Information Bulletin) 2013. Vol. 52. No. 3. pp. 403-411.
3. Феер Д. К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. М.: Радио и связь, 2000. 520 с.
4. Долуханов М.П. Флуктационные процессы при распространении радиоволн. М.: Связь, 1971. 187 с.
5. Шахгильдян В.В., Ляховский А.А. Фазовая автоподстройка частоты. М.: Связь, 1966. 336 с.
6. Gardner F.M. Phaselock Techniques, Second Edition. New York: John Wiley and Sons, 1979.189 p.
7. Белых В.Н. Математические модели системы фазовой синхронизации. – Радиоавтоматика и электроника, 1976 г. т. 21, № 10. С. 2155.
8. Shu Z Shen D Wang G Tian X Chen G Pham K Blasch E. A high order composite automatic frequency control Costas loop for synchronization IEEE Aerospace Conference Proceedings Ser. "2017 IEEE Aerospace Conference" 2017. pp. 794-802.
9. Mario S C Dolecek G J Design and simulation of QPSK reconfigurable digital receiver 53rd IEEE International Midwest Symposium on Circuits and Systems, sponsors: IEEE Circuits and Systems Society. Seattle, WA, 2010. pp. 656-659.
10. Оценка эффективности работы систем частотно-фазовой синхронизации в условиях многолучевого распространения сигнала. [Текст] / В. А. Цимбал, Д. В. Мокринский, А. А. Парфентьев // 21-я Международная конференция «Цифровая обработка сигналов и ее применение» (DSPA-2019); Сб. докладов / Рос. науч.-техн. общ. радиотехн., электрон, и связи им. А.С. Попова. – М.: ИД «Манускрипт», 2019. – Вып. XXI. – Часть:1-2. – С. 327–331.
11. Варианты реализации схем частотно-фазовой синхронизации в условиях многолучевого распространения сигнала. / В. А. Цимбал, Д. В. Мокринский, А. А. Парфентьев //Труды XXV международной научно-технической конференции «Радиолокация, навигация, связь» / ФГБОУ «Воронежский государственный университет», АО «Концерн «Созвездие» - Воронеж, 2019 – Т. 2 – С. 212-218.
12. Реакция контура цифровой фазовой автоподстройки частоты на типовые возмущения / Мокринский Д.В. / Российское научно-техническое общество радиотехники, электроники и связи им. А. С. Попова, 2-я Всероссийская конференция «Современные технологии обработки сигналов» Доклады конференции. – Москва: ООО «Брис-М», 2019. – С. 41-44.
13. Исследование отклика системы цифровой фазовой автоподстройки частоты второго порядка на типовые возмущения / Мокринский Д.В. //Сборник докладов XX Всероссийской научно-практической конференции «Проблемы развития и применения средств противовоздушной обороны на современном этапе. Средства противовоздушной обороны России и других стран мира, сравнительный анализ (11 октября 2019 г.)» Секции 1-8. – Материалы конференции – Ярославль: Ярославское Высшее военное училище противовоздушной обороны, 2019. – С. 263-269.
14. Stephens R. Phase-Locked Loops for Wireless Communications. Digital, Analog, and Optical Implementations. Second Edition. New York: Kluwer Academic Publishers, 2002. 434 p.
15. Лайонс Р. Цифровая обработка сигналов. Второе издание. М.: Бином, 2006. 652 с.
16. Шахгильдян В.В., Ляховский А.А. Фазовая автоподстройка частоты. М.: Связь, 1966. 336 с.
17. Пашинцев В.П. Принципы построения трактов радиоприёмников систем военной связи. М.: МО РФ, 1998. 259 с.
18. Проксис Дж. Цифровая связь. М.: Радио и связь, 2000. 800 с.
19. Феер Д. К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. М.: Радио и связь, 2000. 520 с.
20. Кловский Д.Д. Передача дискретных сообщений по радиоканалам. М.: Радио и связь, 1982. 304 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОИЗВОДСТВЕ

УДК 004.94

РИСКИ ОБЛАЧНОЙ МИГРАЦИИ ДЛЯ ПРЕДПРИЯТИЙ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Андреевский Игорь Леонидович, Перова Ксения Константиновна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: ail@unecon.ru, ksuy.perova.98@mail.ru

Аннотация. Рассматриваются риски облачной миграции для предприятий малого и среднего бизнеса.

Ключевые слова: облачная миграция; риски; информационная безопасность.

CLOUD MIGRATION RISKS FOR ENTERPRISES OF SMALL AND MEDIUM BUSINESS

Andreevskiy Igor, Perova Ksenia
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mails: ail@unecon.ru, ksuy.perova.98@mail.ru

Abstract. The risks of cloud migration for small and medium enterprises are considered.

Keywords: cloud migration; risks; information security.

С каждым годом все больше предприятий малого и среднего бизнеса используют облачные технологии, которые имеют ряд неоспоримых преимуществ перед традиционными технологиями.

Проекты облачной миграции могут включать миграцию приложений, миграцию отдельных элементов существующей ИТ-инфраструктуры, а также миграцию данных.

План облачной миграции для предприятий малого и среднего бизнеса включает в себя ряд традиционных этапов: инвентаризацию существующей ИТ-инфраструктуры и формирование схемы зависимости приложений и компонентов, выбор облачного провайдера, выбор инструментов миграции, обеспечение сетевой связности, составление детального плана миграции, тестовую миграцию, проверку работоспособности перенесенных программных продуктов и компонентов, промышленную эксплуатацию.

Проекты облачной миграции можно рассматривать как отдельный класс ИТ-проектов. Подавляющее большинство проектов облачной миграции связано с определенным риском, который можно оценивать как качественно, так и количественно.

Ключевыми показателями плана миграции выступают RTO (время простоя) и RPO (величина потери данных).

К основным рискам проекта облачной миграции ИТ-инфраструктуры для предприятий малого и среднего бизнеса в облако относятся:

- превышение бюджета;
- превышение сроков реализации проекта;
- несоответствие заявленным требованиям заказчика;
- неопределенность/неточность требований заказчика.

При планировании мероприятий облачной миграции для снижения негативных последствий рекомендуется проводить детальное планирование плана осуществляемых мероприятий, составлять сетевые графики работ и распределения задач и ресурсов, заключение договора с фиксированной сметой и сроками. Важную роль играет постоянный контакт с заказчиком на протяжении всего проекта, поддерживание связи и уточнение деталей.

Отдельное место среди рисков облачной миграции для предприятий малого и среднего бизнеса занимают риски, связанные с рисками информационной безопасности, которые связаны с конфиденциальностью и доступностью данных, их целостностью.

Оценка рисков облачной миграции для оценивания безопасности использования облачных технологий для предприятий малого и среднего бизнеса может быть проведена количественно с использованием модели ожидания отдельных затрат (SLE) и размера среднегодовых затрат (ALE).

СПИСОК ЛИТЕРАТУРЫ

1. Миграция в облако [Электронный ресурс] – Режим доступа: https://selectel.ru/solutions/cloud-migration.
2. Миграция в облако – руководство [Электронный ресурс] - Режим доступа: https://www.clarusft.com/migrating-to-cloud-an-insiders-guide.
3. Стратегия облачной миграции [Электронный ресурс] - Режим доступа: https://medium.com/@satechglobal/the-5-rs-of-cloud-migration-strategy-3b6a5676dda2.

УДК 007.2

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ СОТРУДНИКОВ ПРЕДПРИЯТИЯ С ПОМОЩЬЮ ТЕХНОЛОГИИ НКИ

Байдужа Дарья Александровна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: darjabayd@gmail.com

Аннотация. Отражены результаты исследования по разработке программного обеспечения на основе использования неинвазивных нейрокомпьютерных интерфейсов. Применение этой технологии позволит осуществлять анализ психосоматического состояния сотрудников, по результатам которого будут предлагаться мероприятия для снижения утомляемости персонала, что приведёт к улучшению экономических показателей деятельности предприятия.

Ключевые слова: нейрокомпьютерный интерфейс; биопотенциалы мозга; когнитивная нагрузка; программное обеспечение.

INCREASING THE EFFICIENCY OF EMPLOYEES BY USING THE BCI TECHNOLOGY

Baiduja Daria
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: darjabayd@gmail.com

Abstract. Considering results of research for development software based on using non-invasive BCI. Technology will be analyses psychosomatic state of employees and recommend actions for reduce staff fatigue. It needs to improve economic performance of the enterprise.

Keywords: neurocomputer interface; brain biopotentials; cognitive load; software.

В процессе длительной непрерывной работы на предприятиях у сотрудников из-за монотонной работы возникает переутомление и ухудшается самочувствие, в результате чего они выполняют свои функциональные обязанности недостаточно эффективно [6]. В результате бизнес-процессы реализуются со значительными ошибками, задержками и т.п., что приводит к убыткам предприятия. Чтобы решить эту проблему, можно применять различные подходы – например, увеличивать длительность перерывов; привлекать специалистов-психологов, проводящих тренинги, направленные на снятие стресса у сотрудников; создавать специализированные спортивные площадки, чтобы работники во время перерывов могли отвлечься от монотонной работы. Проблема описанных подходов заключается в том, что все они требуют привлечения существенных финансовых и организационных ресурсов, и период окупаемости капиталовложений при их реализации весьма значителен [1]. В качестве альтернативного решения представляется перспективным создание методики, которая позволит оценивать с достаточной степенью точности состояние сотрудников, степень их утомления и предлагать какие-либо мероприятия, направленные на улучшение самочувствия работников.

Для создания подобной технологии необходимо учесть ряд факторов. Каждый человек имеет строго индивидуальный спектр психофизических особенностей, обуславливающих его когнитивную и интеллектуальную деятельность [3]. Вследствие этого, нельзя разработать какую-либо общую, универсальную шаблонную систему тестирования, которая подойдет каждому. Необходимо создание программно-аппаратного комплекса, который будет осуществлять мониторинг психосоматических показателей состояния каждого сотрудника во время выполнения его профессиональной деятельности, анализируя выраженность и направленность утомления, так как данная характеристика имеет множество различных вариаций.

В качестве основного метода необходимо использовать оценку состояния психики человека. Для решения данной задачи существует множество способов: системы психологического тестирования, диагностика с помощью методов электроэнцефалографии и миографии, анализ уровня оксигенации крови, измерение частоты сердечных сокращений и т.п. По результатам проведенного исследования, включавшего в себя оценку валидности различных методик, факторы времени и простоты реализации, оценки стоимости разработки и внедрения, наиболее эффективным представляется метод нейрокомпьютерных интерфейсов (НКИ) на базе неинвазивного подхода.

Технология НКИ воплощает механизмы, которые позволяют человеку взаимодействовать с внешним миром на основе регистрации электрической активности мозга – электроэнцефалограммы. Желание человека совершить какое-то действие отображается в изменениях показателей в режиме реального времени, которые, в свою очередь, интерпретируются аппаратно-программным комплексом на основе алгоритмических моделей. Данная технология не требует хирургического вмешательства, а также имеет максимально простой способ эксплуатации [2].

В коре головного мозга содержится большое количество нейронов, которые функционально связаны друг с другом. Каждый из них способен посылать электрический импульс. Отдельные части коры воспринимают и анализируют разные виды информации, поэтому каждый отдел больших полушарий

бодрствующего человека занят получением, интеграцией и передачей множества электрических импульсов, которые в сумме формируют электрическую активность в виде нервных импульсов, посылаемых и получаемых корковыми нейронами. Так как кора головного мозга находится сразу под черепом, электроды, расположенные на коже головы, могут обнаружить электрическую активность, связанную с функционирующими нейронами. Электрический сигнал, получаемый электродами, слабый, поэтому канал электроэнцефалографа включает в себя усилитель биопотенциалов, позволяющий увеличивать их значения и противодействовать электрическим помехам. Также аппаратная часть ЭЭГ включает в себя аналого-цифровой преобразователь и фильтр, который необходим для повышения качества оцифровки сигнала [4].

С помощью электроэнцефалографии можно зарегистрировать четыре основных периодических ритма (или так называемых «волновых диапазона» – альфа, бета, дельта и тета), связанных с различными состояниями мозга. Как показано в [5], умственные нагрузки вызывают серьезные изменения в электроэнцефалограмме в диапазоне альфа-ритма, а именно – снижение частоты колебаний. Многочисленные исследования в этом направлении показали также наличие вторичных изменений динамики амплитудно-частотных параметров ЭЭГ во всех ритмических диапазонах. Отмечено усиление дельта- и тета-активности волновых поддиапазнов. При выполнении когнитивных задач усиление тета-ритма, называемого также ритмом напряжения, положительно соотносится с успешностью их решения. Перестройки в диапазоне бета-активности не столь однозначны – это зависит от типа когнитивной нагрузки: внутренней, посторонней, уместной.

С помощью данных механизмов представляется возможным создание аппаратно-программного комплекса, который позволит на основании раннее перечисленных характеристик определять степень утомления сотрудников и выдавать рекомендации по тому, как улучшить их самочувствие. Результаты мониторинга также станут отправляться в центр обработки данных предприятия. На основании многофакторного статистического анализа будут разрабатываться стратегические меры по снижению уровня утомляемости всех сотрудников, выявляться более эффективные решения по улучшению самочувствия работников, производиться перестройка задач и бизнес-процессов предприятия.

При внедрении предприятием описанной методики по повышению работоспособности сотрудников можно существенно снизить убытки и увеличить прибыль.

СПИСОК ЛИТЕРАТУРЫ

1. Аминов Х.И. Модели цифровизации экономической деятельности: монография / Аминов Х.И., Андреевский И.Л., Безрук Г.Г., Верзун Н.А., Воробьева Д.М., Головкин Ю.Б., Горулев Д.А., Емельянов А.А., Карташов П.Н., Касаткин В.В., Кефели И.Ф., Колбанев М.О., Коршунов И.Л., Кунтуров А.Л., Кунтурова Н.Б., Левкин И.М., Левкин О.М., Микадзе С.Ю., Омельян А.В., Пойманова Е.Д., Пуха Г.П., Савченко В.А., Соколов Р.В., Татарникова Т.М., Цихлер А.О., Шахова Е.Ю. – СПб: изд-во СПбГЭУ, 2019.– 179 с.
2. Долецкий А.Н. Интерфейс «мозг-компьютер»: современный этап развития и перспективы / Долецкий А.Н., Гузенко Д.С.// Волгоградский научно-медицинский журнал: сб. статей - Волгоград: ВолГМУ, 2017. - с. 15-18
3. Емельянов А. А. Использование технологии НКИ в сфере информационной безопасности // Сквозные технологии цифровой экономики: сб. статей – СПб: СПбГЭУ, 2019, с. 13-18
4. Махров С.С. Анализ методов формирования и выделения ЭЭГ-паттернов при регистрации сигналов в нейроинтерфейсах/ Махров С.С., Ерохин С.Д.// T-Comm - Телекоммуникации и Транспорт. - 2017. - №10. - С. 56-58
5. Поликанова И.С. Влияние длительной когнитивной нагрузки на параметры ЭЭГ/ Долецкий А.Н., Сергеев А. В. // Национальный психологический журнал: сб. статей – Москва: МГУ им. Ломоносова, 2015. - №1 – с. 83-90
6. Станкевич Л.А. Оценка уровня умственной работоспособности на основе анализа сигналов ЭЭГ/ Станкевич Л.А., Аманбаева С.С., Самочадин А.В.// Научно-технические ведомости СПбГПУ. Информатика, телекоммуникации и управление. - Т. 11. №4. с. 151-161

УДК 681.3

МОДЕЛЬ СОБЫТИЙНОГО УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич,
Цехановский Владислав Владимирович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: dudvl@list.ru

Аннотация. Рассматривается объектная модель, позволяющая решать задачи событийного управления производством. Предлагается расширенная модель конструкторско-технологической спецификации, основным классом которой является Изделие-Операция. Показана возможность применения данной модели для описания разнообразных классов деятельности. Предложенное решение позволяет применить единый подход к решению задач управления производственной деятельностью на основе заказов и событий.

Ключевые слова: объектная модель; управление производством; рабочий центр; события; заказ.

EVENT-BASED PRODUCTION MANAGEMENT MODEL

Dubenetsky Vladislav, Kuznetsov Alexander, Tsekhanovsky Vladislav
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: dudvl@list.ru

Abstract. We consider an object model that allows us to solve the problems of event-based production management. An extended model of the design and technological specification is proposed, the main class of which is the Product-Operation. The possibility of using this model to describe various classes of activity is shown. The proposed solution allows you to apply a unified approach to solving problems of managing production activities based on orders and events.

Keywords: object model; production management; work center; events; order.

Обсуждается проект разработки модуля событийного управления производством. Основная цель проекта – повышение качества управления мелкосерийным и единичным многономенклатурным производством.

Основными задачами проекта являются: - определение преимуществ и недостатков событийной модели управления производством; - разработка объектной модели событийного управления производством; - модификикация системы класса ERP для решения задач событийного управления производством.

Системы подобны цепям. В каждой системе есть самое слабое звено (ограничение), которое в конечном счете снижает результативность всей системы [1]. Системы вытягивания соответствуют принципам «бережливого» производства [2]. Управление производством по системе вытягивания соответствует событийной модели и обладает рядом преимуществ по сравнению с моделями оперативно-календарного планирования. Событийная модель позволяет: исключить объемные и трудоемкие перерасчеты графиков изготовления продукции в связи с потоками разнообразных изменений; оперативно перераспределять материальные ресурсы, ресурсы оборудования и трудовые ресурсы; учитывать реальное состояние производства при оперативном управлении потоками заказов рабочим центрам; перестраивать правила управления на основе накопления статистических данных о загрузке рабочих центров и состоянии заказов.

В качестве недостатков использования модели событийного управления можно отметить следующее:

– данная модель предполагает некоторое увеличение производственных запасов;

– время выполнения заказа может быть оценено как случайная величина;

– календарный график производства является ориентировочным – время выполнения заказа имеет случайную составляющую.

Для обеспечения основной цели логистики производства необходимо в комплексе решать задачи планирования, организации и оперативного управления движением материального потока [3]. Рассмотрим типовую структуру изделия, состоящего из узлов и деталей. Каждая партия компонентов изделия и партия самого изделия должны пройти по определенному маршруту через цепочку групповых рабочих центров (ГРЦ) в соответствии с маршрутной технологией. При классическом подходе основной сущностью для области производства является класс Изделие, которое должно пройти определенные позиции технологического маршрута (ассоциативный класс Позиция ТМ с ролью Технологический маршрут) [4]. В свою очередь, с классом Позиция ТМ связан ассоциативный класс Ресурс для позиции ТМ через ассоциацию с ролью Требуемый ресурс. Для класса Позиция ТМ также указаны оборудование (ассоциация с ролью Требуемый исполнитель, класс Групповой РЦ). Если известен План выпуска и временные ресурсы Рабочих центров и Сотрудников, то модель маршрутной технологии позволяет рассчитать Календарный график изготовления для всех компонентов всех изделий из плана. Любые отклонения в сроках выполнения графика, изменениях в трудовых ресурсах, ресурсах оборудования, материальных ресурсах требуют перерасчета Календарного графика изготовления. Для мелкосерийного дискретного производства такой перерасчет может быть выполнен не чаще одного раза в сутки. Приостановить заказ, ускорить его выполнение, включить новый заказ с назначением ему заданных ресурсов, синхронизировать выполнение заказов с закупками, кооперацией оказывается достаточно трудоемко и неудобно.

В [5] предлагается решение по управлению производством по схеме вытягивания. Однако, единая модель управления потоками в этом решении отсутствует. При построении модели событийного управления предлагается перейти от классов Изделие и Технологическая операция к сущности Изделие-Операция и сделать ее основной во всех дальнейших аспектах рассмотрения. Модель конструкторско-технологических спецификаций (КТС) в аспекте событийного управления производством представлена придется изменить. Ассоциативный класс Изделие-Операция описывает изделия-операции КТС, а ассоциация Маршрут описывает состав изделий-операций для конкретного изделия. Зависимости изделий-операций задают ассоциативный класс Позиция входного ресурса с ролью Входной ресурс. Роль После операции указывает на изделие-операции, от которых зависит исходная изделие-операция. Таким образом, класс Позиция входного ресурса для некоторого изделия, с одной стороны указывает как на другие изделие-операции этого изделия, задавая порядок выполнения операций маршрута, с другой стороны, указывает изделие-операции других Изделий, являющиеся входным ресурсом, с указанием норм расхода. Особенностью предлагаемой модели является выделение двух подклассов класса Изделие-Операция. Подкласс Позиция тех-маршрута описывает классические операции технологии изготовления. Классы Профессия, Квалификация и ассоциации с ролями Треб. профессия, Треб. квалификация позволяют задать требования к профессии и квалификации исполнителя операции по позиции маршрута. Класс Групповой РЦ и ассоциация с ролью Требуемый ГРЦ позволяют указать требования к оборудованию для исполнения операции позиции маршрута. Метакласс Классификатор операций, класс Технологическая операция и ассоциация с ролью ТО позволяют указать типовую технологическую операцию для позиции маршрута.

Предложенное операционное описание деятельности может быть распространено не только на традиционные технологические операции и расширено на другие классы операций (Хозяйственная операция, Операция кооперации, Транспортировка, Заказ на закупку и другие).

Операционная деятельность осуществляется с формированием и исполнением заказов. Обычно объектом заказа является изделие, которое по умолчанию готово к использованию. С целью поддержки событийного управления производством сделаем объектом заказа не Изделие, а изделие после выполнения заданной операции (Изделие-Операция). Таким образом, каждый заказ содержит указание на получение заданного количества элементов *.Изделие-Операция и порождает сеть зависимых заказов при движении в виде обратной волны по схеме маршрутной технологии от исходной изделие-операции. Каждая ветвь полученной сети заказов заканчивается или первой операцией соответствующего изделия, или обнаружением и закреплением остатков необходимой изделие-операции.

При появлении Заказа на изготовление Партии изделий-операций в количестве N штук должна быть развернута сеть заказов, вершины которой связаны с элементом *.Групповой РЦ. ГРЦ многофункциональны, поэтому некоторые операции могут выполняться РЦ одного ГРЦ. С каждым компонентом сети заказов при его выполнении связывается *.Партия изделий-операций с количеством, определенным путем учета исполнения заказов. Так как каждый заказ связан только с одним изделием-операцией, то ему соответствует один ГРЦ. Таким образом, сеть заказов можно представить в виде сети ГРЦ с входными и выходными заказами и накопителями, содержащими экземпляры из Партий изделий-операций. К каждому ГРЦ будет выстраиваться очередь Заказов изделий-операций, готовых к исполнению на данном ГРЦ. Таким образом, каждый ГРЦ может быть представлен как обслуживающий прибор.

Для каждой запускаемой позиции заказа (Плана выпуска) строиться множество производственных операций (класс Производственные операции) с указанием выполняющего ГРЦ и состоянием «ожидание разрешения на выполнение». Необходимо определить список операций, которые готовы к выполнению. В соответствии с приоритетом позиций все операции разделяются на соответствующие группы. Для изделия-операции одного ГРЦ и одного Заказа дополнительно приоритеты могут быть назначены в соответствии с прогнозом времени от окончания операции до выполнения заказа. Например, операция, находящаяся дальше в графе изготовления по прогнозному времени, имеет больший приоритет.

Осталось решить вопрос об определении готовности объектов *.Заказ. Из графа зависимости Изделий-Операций можно получить список заказов **.Заказов , которые должны быть выполнены, чтобы искомый *.Заказ стал «готов к выполнению». Такая проверка реализуется достаточно просто. Определим моменты времени, когда такие проверки необходимо выполнять. Каждый раз, когда производится учет выполнения одного из **.Заказов, необходимо проверять «готовность к исполнению» тех заказов, которые зависят от выполненного заказа. При выполнении «условия готовности» текущий *.Заказ переходит в состояние «готов к выполнению» и ставится в очередь на выполнение. В соответсвии с правилами обслуживания очередной *.Заказ переходит в состояние «выполнение». При завершении выполнения *.Заказ переходит в состояние «выполнен», а использованные ранее заказы на входе **.Заказы переходят в состояние «использованы». Множество вариантов взаимодействия достаточно велико. Применительно к решению задачи управления производством по вытягивающей схеме требуется решить вопрос синхронности взаимодействия.

Выводы. Предложена объектная модель управления производством, обеспечивающая единое описание разнообразных производственно-логистических процессов и, как следствие, общую реализацию исполнения.

СПИСОК ЛИТЕРАТУРЫ

1. Детмер У. Теория ограничений Голдратта: Системный подход к непрерывному совершенствованию / Уильям Детмер; Пер. с англ. — 2-е изд. — М.: Альпина Бизнес Букс, 2008. — 444 с.
2. Дэвид Хэллет Обзор систем вытягивания: wkazarin.ru/ URL: http://www.pullscheduling.com
3. Логистика и управление цепями поставок. Теория и практика. Основные и обеспечивающие подсистемы логистики: учебник / под ред. Б. А. Аникина и Т. А. Родкиной. – Москва: Проспект, 2015. – 608 с.
4. Дубенецкий В. А., Советов Б. Я., Цехановский В. В. Проектирование корпоративных информационных систем. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2013. -191 с.
5. Управление производством. URL: https://erp4u.expert/index/upravlenie_proizvodstvom/0-13

УДК 004.04

МЕТОДОЛОГИИ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ПОДДЕРЖКИ ПРОЦЕССОВ ПОСТРОЕНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПРЕДПРИЯТИЯ

Касаткин Виктор Викторович[1], Михайлов Николай Семёнович[2], Михайлова Анна Сергеевна[3]
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14 линия, 39, Санкт-Петербург, Россия
[2]Санкт-Петербургский государственный университет аэрокосмического приборостроения
ул. Большая Морская, д. 67, лит. А, Санкт-Петербург, Россия
[3]Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова
1-я Красноармейская ул., д. 1, Санкт-Петербург, Россия
e-mails: v.v.kasatkin@iias.spb.su, mikhailov.ru@gmail.com, anna.mikhais@gmail.com

Аннотация. В докладе обсуждается методология построения единого информационного пространства предприятия. Представлены результаты исследования методов проектирования и предложены критерии выбора требований к единому информационному пространству предприятия, основанные на стратегии его развития. Предложена методология, позволяющая оперативно реагировать на изменяющиеся организационно-технические условия производства и воздействия внешней среды, уточнять и согласовывать требования к элементам системы управления предприятием, непрерывно совершенствовать и модернизировать единое информационное пространство в процессе функционирования предприятия.

Ключевые слова: бизнес-процесс; стратегия развития предприятия; единое информационное пространство предприятия; интегрированная информационная система.

METHODOLOGIES AND TOOLS TO SUPPORT PROCESSES FOR BUILDING A SINGLE ENTERPRISE INFORMATION SPACE

Kasatkin Viktor[1], Mikhailov Nikolai[2], Mikhailova Anna[3]
[1] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th Line St, St. Petersburg, Russia
[2] Saint Petersburg State University of Aerospace Instrumentation,
st. Bolshaya Morskaya, 67, lit. A, Saint Petersburg, Russia
[3] Baltic State Technical University "VOENMEKH" D.F. Ustinova
1st Krasnoarmeyskaya st., 1, Saint Petersburg, Russia
e-mails: v.v.kasatkin@iias.spb.su, mikhailov.ru@gmail.com, anna.mikhais@gmail.com

Abstract. The report discusses the methodology for building a single enterprise information space. The results of the study of design methods are presented and criteria for selection of requirements for a single information space of the enterprise based on its development strategy are proposed. The methodology is proposed, which allows to react quickly to changing organizational and technical conditions of production and impact of the external environment, to clarify and coordinate the requirements for elements of the enterprise management system, to continuously improve and modernize the single information space during the enterprise operation.

Keywords: business process; enterprise development strategy; common information space of the enterprise; integrated information system.

Необходимость успешного функционирования и развития промышленного предприятия в условиях жесткой конкуренции диктует свои требования к организации бизнес-процессов предприятия [1, 2]. Решение задачи повышения эффективности управления предприятием связано с необходимостью обеспечения информационно-аналитической поддержки основных и вспомогательных процессов на основе широкого внедрения цифровых бизнес-моделей [3].

В современных условиях деятельность предприятия сопровождается его непрерывной комплексной трансформацией, инновационными и антикризисными изменениями политики управления предприятием, структурными преобразованиями, реинжинирингом бизнес-процессов, в том числе обусловленными внедрением концепции «Индустрия 4.0», в рамках которой осуществляется широкомасштабная цифровизация предприятия, а данные в цифровой форме и цифровые технологии становятся ключевым фактором производства во всех сферах экономической деятельности. Любые значимые изменения на предприятии должны внедряться на основе глубоко продуманной стратегии развития предприятия, для которой в общем случае может быть выделено четыре уровня: корпоративная стратегия, бизнес-стратегия, функциональная стратегия и операционная стратегия [4, 5].

В настоящее время широко используются как различные модели управления предприятием, так и подходы к проектированию информационной архитектуры и организации бизнес-процессов предприятия. Обеспечение согласованного управления данными и информационным пространством предприятия невозможно без решения задачи построения единого информационного пространства (ЕИП) предприятия.

На решение задачи построения ЕИП предприятий направлена комплексная стратегия повышения эффективности бизнес-процессов, отражающих этапы жизненного цикла изделия и непосредственно влияющих на конкурентоспособность и качество продукции, за счет интеграции и преемственности информации, порождаемой на всех этапах жизненного цикла, т.е. сквозной информационной поддержки процессов на протяжении жизненного цикла изделия.

Под ЕИП предприятия понимается совокупность баз и банков данных, технологий их ведения и использования, информационно-телекоммуникационных систем и сетей, функционирующих на основе единых принципов и по общим правилам, обеспечивающим защищенное информационное взаимодействие всех участников, а также удовлетворение их информационных потребностей в соответствии с иерархией обязанностей и уровнем доступа к данным.

Отличительной особенностью концептуальной модели ЕИП предприятия является наличие интегрированной информационной системы, включающей:

– телекоммуникационную среду, коммуникационное программное обеспечение (ПО), средства организации совместной работы Groupware;

– информационные системы, информационные ресурсы и механизмы представления информации на их основе: ERP-системы; ПО управления электронным документооборотом; ПО информационной поддержки предметной области; ПО оперативного анализа информации и поддержки принятия решений; ПО управления проектами: встроенные инструментальные средства и другие продукты, такие как CAD/CAE/CAM/PDM-системы; ПО управления персоналом; системы управления производством MES; системы компьютерного менеджмента качества продукции предприятия на всех этапах жизненного цикла изделия; системы электронного сопровождения продукции предприятия в эксплуатации; CRM-системы взаимоотношения с клиентами;

– организационную инфраструктуру, обеспечивающую функционирование ЕИП предприятия;
– систему подготовки и переподготовки специалистов и пользователей ЕИП предприятия.

Проектируемая ЕИП предприятия должно обеспечивать требуемую динамику цифровой трансформации, связанной с перестройкой бизнеса и оперативным внедрением изменений. Для этого необходимо учитывать большое количество требований, содержащихся в многочисленных концептуальных, программных, проектных и регламентирующих документах. Представляется целесообразным структурировать указанные требования путем разделения их на три уровня:

1. Стратегический уровень (уровень бизнес-требований), включающий требования верхнего уровня к развитию предприятия, которые содержатся в стратегии развития предприятия (корпоративная стратегии, бизнес-стратегия, стратегия инновационного развития).

2. Функциональный уровень, учитывающий требования, выделенные из бизнес-уровня, и включающий различные функциональные стратегии, такие как стратегия развития информационных технологий, стратегия цифровой трансформации и т.п.

3. Уровень приложений, объединяющий требования прикладного уровня, определяемые техническими заданиями, техническими условиями, отраслевыми стандартами, лучшими практиками.

Для бизнес-уровня применима нотация IDEF0, в которой модель представляется в виде совокупности иерархически упорядоченных и взаимосвязанных диаграмм, а вершина древовидной структуры содержит самое общее описание системы. После описания системы в целом проводится ее функциональная декомпозиция. К достоинствам нотации IDEF0 относится возможность получения полной информации о каждой работе, благодаря ее жестко регламентированной структуре. С помощью нотации IDEF0 можно выявить все недостатки, касающиеся как описания самого процесса, так и его реализации: дублирование функций, отсутствие механизмов, регламентирующих процесс, отсутствие контрольных переходов и т.д.

На функциональном уровне проектирования ЕИП предприятия общепринятым методом является проектирование бизнес-процессов с использованием соответствующих нотаций моделирования, в качестве которых на основе проведенного анализа был обоснован выбор нотаций eEPC и BPMN.

На уровне приложений ЕИП предприятия архитекторы и разработчики программного обеспечения используют блок-схемы и различные методологии и нотации.

Примером одной из наиболее широко применяемых является нотация UML (Unified Modeling Language), которая предоставляет средства для создания визуальных моделей, единообразно интерпретируемых всеми разработчиками, вовлеченными в проект, и служит эффективным средством коммуникации в рамках проекта. При визуальном моделировании на UML используются восемь видов диаграмм, каждая из которых может содержать элементы определенного типа. Актуальным является метод управления и разработки программного обеспечения на основе agile-методов с использованием возможностей User Story Mapping.

Предложенная методология построения ЕИП предприятия базируется на трехуровневом представлении ЕИП и использовании на верхнем бизнес уровне нотация IDEF0 с последующей декомпозицией и моделированием бизнес-процессов на функциональном уровне в нотации BPMN или eEPC. Д

ля проектирования и разработки программного обеспечения на уровне приложений используются гибкие методологии разработки – agile-методы на основе использования соответствующих моделей: пользовательских историй, UML-моделей, блок-схем.

По завершении этапа экспериментальной апробации разработанная методология успешно внедрена на одном из приборостроительных предприятий Санкт-Петербурга, что позволило обеспечить сокращение сроков согласования требований и повышение качества разработки программного обеспечения, ускорить внедрение изменений в ЕИП и организовать курсы повышения квалификации персонала.

СПИСОК ЛИТЕРАТУРЫ

1. Варзунов А. В., Торосян Е. К., Сажнева Л. П. Анализ и управление бизнес- процессами: учебное пособие. СПб: Университет ИТМО, 2016. 112 с.
2. Васильева А. П. Сравнительный анализ методологии описания бизнес-процессов // Научные исследования: теория, методика и практика: материалы Междунар. науч.-практ. конф. (Чебоксары, 21 мая 2017 г.), 2017. С. 42–47.
3. Михайлов Н. С. Модель единого информационного пространства промышленного предприятия // Перспективные направления развития отечественных информационных технологий: материалы V межрегиональной научно-практической конф. Севастополь, 24-28 сентября 2019 г. / Севастопольский государственный университет; науч. ред. Б..В. Соколов. – Севастополь: СевГУ, 2019. . – С.146-149
4. Михайлов Н. С. Стратегия развития промышленного предприятия // Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 1-3 ноября 2017 г.: Материалы конференции. СПОИСУ. СПб., 2017. С. 235.
5. Михайлов Н. С., Петров В.А. Разработка интегрированной информационной системы организации и управления производством // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5 / СПОИСУ. – СПб., 2018. – С. 401-404.

УДК 001.891.57 + 541.67 + 677.494

ИНФОРМАЦИОННОЕ МОДЕЛИРОВАНИЕ ТЕХНОЛОГИИ СОЗДАНИЯ УГЛЕРОДНЫХ ЭЛЕКТРОПРОВОДЯЩИХ ВОЛОКОН НА ОСНОВЕ ПОЛИВИНИЛОВОГО СПИРТА

Лысенко Владимир Александрович, Крисковец Максим Викторович
Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: valys@mail.ru, kriskovets.maksim@list.ru

Аннотация. Выполнено информационное моделирование технологии создания углеродных электропроводящих волокон на основе поливинилового спирта. Проведена проверка результатов моделирования в условиях физического эксперимента. Подтверждена согласованность результатов информационного моделирования с экспериментальными данными.

Ключевые слова: информационное моделирование; углеродное волокно; поливиниловый спирт; электрическое сопротивление; высокотемпературная сверхпроводимость.

INFORMATION MODELING OF CREATING TECHNOLOGY FOR CARBON CONDUCTIVE FIBERS BASED ON POLYVINYL ALCOHOL

Lysenko Vladimir, Kriskovets Maksim
Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St, St. Petersburg, 191186, Russia
e-mails: valys@mail.ru, kriskovets.maksim@list.ru

Abstract. Information modeling of polyvinyl alcohol carbon conductive fibers creating technology was performed. The simulation results were verified under the conditions of physical experiment. The conformity of the modeling results with experimental data was confirmed.

Keywords: information modeling; carbon fiber; polyvinyl alcohol; electrical resistance; high-temperature superconductivity.

Ранее сообщалось об обнаруженном явлении возникновения сверхнизкого электрического сопротивления у углеродных волокон с высокой долей поликумуленовых и полииновых связей [1, 2]. Настоящий доклад посвящен дальнейшим исследованиям данного явления.

С использованием научного подхода, ранее разработанного для создания углеродных композиционных материалов и углеродных волокон [3, 4], проведено информационное моделирование технологии создания углеродных волокон на основе поливинилового спирта (ПВС) на каждой из технологических стадий процесса создания и технологии в целом с целью изготовления углеродных волокон на основе ПВС с минимальным электрическим сопротивлением.

Определён отклик электрического сопротивления углеродного ПВС в модели углеродного волокна как системы на следующие факторы воздействия: параметры технологического процесса дегидратации, параметры карбонизации, включая конечную температуру карбонизации. Информационное моделирование показало возможность существования минимумов на зависимостях электрического сопротивления углеродных ПВС волокон от температуры карбонизации, положение которых определяется отмеченными выше технологическими параметрами.

В условиях физических экспериментов проведена проверка полученных результатов моделирования. Показано, что на электрическое сопротивление системы углеродного волокна влияют следующие технологические параметры: концентрация пропитывающего раствора, время пропитки, степень отжима, время сушки, остаточная влажность, температура начала дегидратации, скорость подъема температуры дегидратации, температура окончания дегидратации, скорость подъема температуры при карбонизации, конечная температура карбонизации. Показано, что для изготовленных углеродных волокон, в зависимости от условий дегидратации, наблюдается наличие минимумов зависимостей электрических сопротивлений от конечной температуры карбонизации. Подтверждена ранее сформулированная гипотеза [1, 2] о формировании особой системы поликумуленовых связей, лежащей в основе открытого явления сверхнизкого, не более $0{,}193 \cdot 10^{-3}$ мОм·см, удельного электрического сопротивления элементарных углеродных поливинилспиртовых волокон и, возможно, наличии сверхпроводящих при комнатной температуре фаз в их структуре.

Таким образом, в результате выполненных исследований разработана информационная модель технологи создания углеродных волокон на основе поливинилового спирта; проведена проверка полученных результатов моделирования в условиях физических экспериментов; определены основные закономерности влияния режимов дегидратации и карбонизации на электрическое сопротивление углеродных волокон на основе поливинилового спирта.

Предложены и обсуждаются перспективы информационного моделирования для оптимизации технологии создания углеродных ПВС волокон со сверхнизким электрическим сопротивлением.

СПИСОК ЛИТЕРАТУРЫ

1. Лысенко В.А. Электрическое сопротивление карбонизованных волокон на основе поливинилового спирта / В.А. Лысенко, М.В. Крисковец, С.В. Буринский // Химические волокна. – 2019. – №5. – С. 26 – 31.
2. Лысенко В.А. Запись, хранение и передача информации на углеродных волокнах со структурой полисопряженных связей / В.А. Лысенко, М.В. Крисковец, С.В. Буринский // XVI Санкт-Петербургская международная конференция “Региональная информатика (РИ-2018)”: Материалы конференции. – СПб: СПОИСУ, 2018. – С. 343 – 345.
3. Лысенко В.А. Системное проектирование углеродных композиционных материалов. Теория и практика / В.А. Лысенко. – Palmarium Academic Publishing. – 2018. – 323 с. – ISBN 978-620-2-38124-6.
4. Лысенко В.А. Моделирование системных превращений в технологии создания углеродных волокон / В.А. Лысенко, М.В. Крисковец // Химические волокна. – 2018. – №4. – С. 28 – 35.

УДК 004.04

РЕКОМЕНДУЕМЫЕ ТРЕБОВАНИЯ ПРИ ПОСТРОЕНИИ ЕИП ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Михайлов Николай Семенович
Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Санкт-Петербург, ул. Большая Морская, д.67
e-mail: mikhailov.ru@gmail.com

Аннотация. В статье рассматриваются требования, предъявляемые к единому информационному пространству (ЕИП) промышленного предприятия

Ключевые слова:.единое информационное пространство, уровни ЕИП

RECOMMENDED REQUIREMENTS FOR THE CONSTRUCTION OF THE SIS OF THE MANUFACTURING ENTERPRISE

Mikhailov Nikolai
St. Petersburg State University of Aerospace Instrumentation (GUAP),
St. Petersburg, 67 Bolshaya Morskaya, Str.
e-mail: mikhailov.ru@gmail.com

Abstract.. The article discusses the requirements for common information space (CIS) of an manufacturing enterprise

Keywords:. common information space, levels of CIS

На решение задачи построения ЕИП промышленных предприятий направлена комплексная стратегия повышения эффективности бизнес-процессов, отражающих этапы жизненного цикла изделия и непосредственно влияющих на конкурентоспособность и качество продукции, за счет интеграции и преемственности информации, порождаемой на всех этапах жизненного цикла изделия [1].

Процесс построения ЕИП промышленного предприятия сопряжен с необходимостью учитывать большое количество требований, содержащихся в многочисленных концептуальных, программных, проектных и регламентирующих документах. Представляется целесообразным структурировать указанные требования путем разделения их на три уровня:

1. Стратегический уровень (уровень бизнес-требований), включающий требования верхнего уровня к развитию промышленного предприятия, которые содержатся в стратегии развития предприятия.
2. Функциональный уровень, учитывающий требования, выделенные из бизнес-уровня, и включающий различные функциональные стратегии, такие как стратегия развития информационных технологий, стратегия цифровой трансформации и т.п.
3. Уровень приложений, объединяющий требования прикладного уровня, определяемые техническими заданиями, техническими условиями, отраслевыми стандартами, лучшими практиками.

Для того, чтобы все участники процесса построения ЕИП промышленного предприятия могли системно взаимодействовать и учитывать требования разных уровней, предлагается формировать и использовать матрицу требований к ЕИП промышленного предприятия, представленную в табличной форме. В столбцах матрицы размещается информация, соответствующая трем уровням ЕИП:

I. Бизнес-уровень (стратегический уровень);

II. Функциональный уровень;

III. Уровень приложений.

В строках матрицы требования разделены по классам в соответствии с общепринятой методологией проектирования информационных систем промышленного предприятия:

1. Связь с контрагентами;
2. Корпоративное управление;
3. Управление данными об изделии;
4. Управление производством;
5. Управление инфраструктурой и оборудованием.

В качестве примера использования матрицы требований к ЕИП промышленного предприятия представлено решение задачи по снижению потерь времени при изготовлении заказа на приборостроительном промышленном предприятии Санкт-Петербурга.

1. Бизнес-уровень (стратегический уровень) включает: соблюдение сроков на поставку заказа, оперативный сквозной контроль изготовления заказа, централизованное хранение данных об изделии, оперативное планирование и контроль производства, надежность работы оборудования

2. Функциональный уровень включает контроль исполнения договорных отношений, интеграцию данных ERP, PLM и MES для учета затрат, сквозную идентификация в PLM, планирование и контроль на основе QR-кода, оборудование для сканирования QR-кода.

3. Уровень приложений включает идентификацию заказа в CRM системе, модули интеграции данных, получение данных из PLM, QR-код в производственной документации MES, совместимость оборудования с информационными системами.

СПИСОК ЛИТЕРАТУРЫ

1. Варзунов А. В., Торосян Е. К., Сажнева Л. П. Анализ и управление бизнес- процессами: учебное пособие. СПб: Университет ИТМО, 2016. 112 с.
2. Михайлов Н. С. Модель единого информационного пространства промышленного предприятия // Перспективные направления развития отечественных информационных технологий: материалы V межрегиональной научно-практической конф. Севастополь, 24-28 сентября 2019 г. / Севастопольский государственный университет; науч. ред. Б..В. Соколов. – Севастополь: СевГУ, 2019. . – С.146-149
3. Схиртладзе, А.Г. Проектирование единого информационного пространства виртуальных предприятий: учебник/ А.Г. Схиртладзе, А.В. Скворцов, Д.А. Чмырь. Изд. 2-е, стер. – М. ; Берлин: Директ-Медиа, 2017. - 616 с.

УДК 658.8.012.12

ФОРМИРОВАНИЕ МАРКЕТИНГОВОЙ СТРАТЕГИИ ПРЕДПРИЯТИЯ СВЯЗИ НА ОСНОВЕ ПРИМЕНЕНИЯ МЕТОДОВ ИССЛЕДОВАНИЯ ОПЕРАЦИЙ

Песиков Эдуард Борисович, Комлев Григорий Олегович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ed_pesikov@mail.ru, G.O.Komlev@yandex.ru

Аннотация. Рассматривается реализация одного из возможных подходов к формированию маркетинговой стратегии предприятия связи, основанного на применении методов исследования операций и позволяющего оптимизировать выбор сегментов рынка, ассортимента, объемов продаж и цен на услуги. Приводятся результаты решения задачи нелинейного частично-целочисленного программирования с помощью предлагаемого эвристического алгоритма, основанного на итерационном увеличении цен на услуги связи и решении на каждом шаге изменения цен соответствующей задачи линейного частично-целочисленного программирования методом Лэнда и Дойга.

Ключевые слова: предприятие; услуга связи;маркетинг;стратегия; целевой сегмент; метод анализа иерархий.

FORMATION OF A COMMUNICATION ENTERPRISE MARKETING STRATEGY BASEDON THE APPLICATION OF METHODS OF RESEARCH OF OPERATIONS

Pesikov Eduard, Komlev Gregory
Bonch-Bruevich Saint-Petersburg state university of communication
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ed_pesikov@mail.ru, G.O.Komlev@yandex.ru

Abstract. The implementation of one of the possible approaches to the formation of the marketing strategy of a communications enterprise based on the application of operational research methods and allowing to optimize the choice of market segments, assortment, sales volumes and service prices is considered. The results of solving the nonlinear partially integer programming problem using the proposed heuristic algorithm based on an iterative increase in prices for communication services and solving at each price change step the corresponding linear partially integer programming problem by the Land and Doig method are presented.

Keywords: enterprise; communication service; marketing; strategy; target segment;analytic hierarchy process.

Актуальность темы исследования обусловлена необходимостью формирования эффективной маркетинговой стратегии предприятия в условиях высокой динамики изменений параметров рынка, высокой остроты конкуренции и ограниченности наличных производственных ресурсов [1].

Целью работы является разработка аналитического инструментария для формирования маркетинговой стратегии предприятия связи, основанного на эвристических методах и моделях математического программирования. В основу предлагаемого инструментария положена математическая модель выбора оптимального ассортимента, объемов продаж, сегментов рынка и цен на услуги за плановый период [2]. С помощью предлагаемой оптимизационной модели представляется возможным планировать производство и реализацию как ранее оказываемых, так и новых видов услуг.

Постановка задачи. Пусть предприятие работает со своими услугами на определенных рынках (или сегментах рынка). В товарном портфеле предприятия имеются также виды услуг, с которыми предприятие еще не выходило на рынок и по которым необходимо принимать решение о целесообразности их вывода на рынок. Проведенные маркетинговые исследования позволили оценить емкости рынков сегментов, на которых предприятие уже работает или предполагает выходить со своими услугами. Маркетологи определили также по каждому сегменту рынка предельные значения цен, по которым потребитель согласен приобрести услуги. Руководство предприятия ставит перед собой задачу достичь в планируемом периоде определенных значений таких целевых показателей как прибыль от реализации услуг и доля рынка, контролируемая предприятием. Ожидаемые уровни наличных производственных ресурсов (материалов, времени работы оборудования и

трудовых ресурсов) в планируемом периоде определены и используются при планировании в качестве ограничивающих факторов. Предполагаются заданными нормы расхода ресурсов на единицу каждого вида услуги; затраты на реализацию (транспортные и торговые издержки, затраты на рекламу) однойуслуги для каждого сегмента рынка; цены единицы каждого вида ресурса.

Требуется определить на какие сегменты рынка, с какими услугами, объемами предложения и ценами следует выходить предприятию на рынок при условии, что будут реализованы цели предприятия, учтены ограничения по спросу и производственным ресурсам и при этом ожидаемая прибыль от реализации услуг достигнет своего максимального значения.

При построении математической модели случайные параметры модели (например, спрос на услуги на различных сегментах рынка) заменяются их математическими ожиданиями. Построение математической модели проводится для фиксированного временного интервала, т. е. процесс планирования исследуется в статической постановке. При необходимости построения динамической модели, т. е. рассмотрения процесса планирования в динамике, следует задавать временную определенность всем переменным и параметрам рассматриваемой математической модели. Оптимизационная модель относится к классу моделей нелинейного частично-целочисленного программирования с управляемыми переменными целого (булевого) и непрерывного типа [3, 4].

Для анализа модели предлагается применять эвристический алгоритм, основанный на поэтапном увеличении значений цен на услуги и решении на каждом этапе соответствующей задачи линейного частично-целочисленного программирования методом ветвей и границ (методом Лэнда и Дойга). При итерационном увеличении цен (начиная с себестоимости услуг) ожидаемая прибыль вначале должна расти за счет роста объема выручки. В дальнейшем отдельные виды услуг, для которых текущие значения цен будут превышать предельные цены для сегментов, начнут “выпадать” из сегментов. В результате рост прибыли должен замедлиться и начиная сопределенной итерации, прибыль будет уменьшаться. Значения объемов предложения и цен на услуги, а также множество оставшихся сегментов на определенном шаге итерационного процесса, при котором достигается максимальная прибыль предприятия, будут соответствовать оптимальному решению задачи.

Таким образом, в результате решения задачи представляется возможным оптимизировать выбор целевых сегментов, ассортимента и объемов продаж услуг, а также цен на услуги на каждом сегменте; наиболее полно учесть потребительский спрос; максимизировать ожидаемую прибыль от продаж услуг и эффективность использования ограниченных производственных ресурсов.

Применение методов исследования операций при формировании маркетинговой стратегии предприятия связи позволяет существенно повысить эффективность принимаемых маркетинговых решений. Предложенные в работе математическая модель и вычислительный алгоритм могут быть положены в основу компьютерных систем поддержки принятия решений при стратегическом управлении маркетингом предприятия связи.

В дальнейшем для предварительного выбора наиболее перспективных из множества альтернативных сегментов рынка предлагается использовать метод анализа иерархий (метод Т. Саати) [5].

СПИСОК ЛИТЕРАТУРЫ

1. Котлер Ф. Основы маркетинга; пер. с англ. Е. М. Пенькова. - М.: Прогресс, 2008.
2. Песиков Э. Б. Стратегическое планирование. Решение задачи выбора оптимальных сегментов рынка, ассортимента, объёмов предложения и цен изданий //«Print&Publishing». 2001. № 46. С. 48–50.
3. Вентцель Е. С. Исследование операций: задачи, принципы, методология. - М.: Дрофа, 2004.
4. Зайченко Ю. П. Исследование операций. Учебник. 6-е изд. - Киев: Слово, 2003.
5. Саати Т. Принятие решений. Метод анализа иерархий. - М.: Радио и связь, 1993.

УДК 658.8.012.12

ПРОГНОЗИРОВАНИЕ ОБЪЕМОВ ПРОДАЖ УСЛУГ ПРЕДПРИЯТИЯ СВЯЗИ С ПОМОЩЬЮ МЕТОДОВ МНОГОМЕРНОГО СТАТИСТИЧЕСКОГО АНАЛИЗА И НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Песиков Эдуард Борисович, Федотович Анна Сергеевна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ed_pesikov@mail.ru, An.Fedotovich@gmail.com

Аннотация. Рассматривается один из возможных подходов к построению системы прогнозирования объемов продаж услуг предприятия связи, основанный на применении однопараметрического метода экспоненциального сглаживания, моделей линейной множественной регрессии и искусственной нейронной сети. Для выявления факторов, наиболее существенно влияющих на объемы продаж услуг, предлагается использовать метод анализа иерархий.

Ключевые слова: предприятие связи, прогнозирование, услуга, объем продаж, метод экспоненциального сглаживания, метод регрессионного анализа, нейросетевые технологии, метод анализа иерархий.

FORECASTING OF VOLUMES OF SALES OF SERVICES OF THE ENTERPRISE OF COMMUNICATION USING METHODS OF MULTIDIMENSIONAL STATISTICAL ANALYSIS AND NEURAL NETWORK TECHNOLOGIES

Pesikov Eduard, Fedotovich Anna
Bonch-Bruevich Saint-Petersburg state university of communication
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ed_pesikov@mail.ru, An.Fedotovich@gmail.com

Abstract. One of the possible approaches to forecasting the sales of communication enterprise services is considered, it based on the application of analytic hierarchy process, exponential smoothing, regression analysis and neural network technologies.

Keywords: communication company, forecasting, service, sales volume, exponential smoothing method, regression analysis method, neural network technologies, Analytic Hierarchy Process.

Актуальность темы обусловлена необходимостью качественного прогнозирования спроса на услуги, которое позволяет обеспечить необходимый уровень эффективности принимаемых руководством предприятия связи управленческих решений, а также даёт возможность своевременно формировать эффективную маркетинговую стратегию [1].

Прогнозирование спроса (объемов продаж) позволяет на основе полученных статистических данных о прошлых фактических значениях объемов продаж и факторов, влияющих на продажи, выявить причинно-следственные связи между ними и заранее спланировать производственную деятельность в короткие сроки наиболее эффективным образом, обеспечивая ожидаемый результат в будущем. Проблема прогнозирования спроса заключаются в сложности выбора наиболее точного и эффективного метода прогнозирования из широкого спектра существующих методик и различных приемов.

Целью работы является разработка и исследование системы краткосрочного прогнозирования объемов продаж услуг предприятия связи, основанной на применении методов многомерного статистического анализа и нейросетевых технологий.

При построении системы краткосрочного прогнозирования объемов продаж услуг предприятия связи предлагается использовать однопараметрический метод экспоненциального сглаживания (метод Р. Брауна) [2], математические модели и методы линейной множественной регрессии [2] и искусственные нейронные сети [3]. Для выбора из заданного множества альтернатив факторов, наиболее существенно влияющих на объемы продаж услуг, предлагается использовать метод анализа иерархий (метод Т. Саати) [4]. Множество альтернативных факторов, влияющих на продажи, формируется методом экспертных оценок и состоит как из ценовых, так и не ценовых факторов воздействия [5].

Проверка точности методов прогнозирования проводится путем сравнения расчетных и фактических значений объемов продаж на основе ретроспективного анализа данных за предшествующие периоды.

Для решения задачи прогнозирования спроса на ПК используется статистический пакет прикладных программ Statistica.

В случае, если результаты прогнозирования объёма продаж методами экспоненциального сглаживания и регрессионного анализа, а также нейросетевых технологий существенно различаются между собой, то предлагается сформировать средневзвешенную оценку прогноза.

Применение методов анализа иерархий, экспоненциального сглаживания, регрессионного анализа и нейросетевых технологий при формировании маркетинговой стратегии предприятия связи позволяет существенно повысить эффективность принимаемых маркетинговых решений.

Рассмотренные в работе математические модели и методы могут быть положены в основу компьютерной системы поддержки принятия решений при управлении маркетингом предприятия связи.

СПИСОК ЛИТЕРАТУРЫ

1. Котлер Ф. Основы маркетинга. Перевод с англ. В. Б. Боброва; Общ. ред. Е. М. Пеньковой. - М.: Прогресс, 1991. - 733 с.
2. Бокс Дж., Дженкинс Г. Анализ временных рядов, прогноз и управление: Пер. с англ. – М.: Мир, 1974, кн. 1. – 406 с.
3. Хайкин С. Нейронные сети: полный курс = Neural Networks: A Comprehensive Foundation. 2-е изд. - М.: Вильямс, 2006. — 1104 с
4. Саати Томас Л. Принятие решений: Метод анализа иерархий /Т. Саати; Пер. с англ. Р. Г. Вачнадзе. - М.: Радио и связь, 1993. - 314 с.
5. Совокупный спрос. Ценовые и неценовые факторы совокупного спроса // Экономическая теория [Электронный ресурс] URL: http://modern-econ.ru/makro/mehanizm/sovokup/spros.html (дата обращения: 05.07.2020).

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

УДК 621.396.98: 629.783

СОВМЕСТНОЕ ИСПОЛЬЗОВАНИЕ НАВИГАЦИОННЫХ ПОЛЕЙ ГЛОНАСС И GPS В СЛОЖНЫХ УСЛОВИЯХ ПИЛОТИРОВАНИЯ ВОЗДУШНЫХ СУДОВ В АРКТИКЕ

Бабуров Владимир Иванович, Васильева Наталья Валентиновна, Иванцевич Наталия Вячеславовна
Институт Авиационного Приборостроения «Навигатор»
Шкиперский проток, 143/19, Санкт-Петербург, 199106, Россия
e-mails: baburov@navigat.ru, nvivantsevich@yandex.ru, nvv64@rambler.ru

Аннотация. Исследуются информационные характеристики совместного навигационного поля, создаваемого спутниковыми системами ГЛОНАСС и GPS в Арктическом регионе России, при различных значениях допустимых углов возвышения спутников. Оценивается возможность использования полученной информационной избыточности для формирования в аппаратуре ВС управляемых рабочих созвездий спутников в нештатных ситуациях.

Ключевые слова: имитационное моделирование; спутниковые системы; информационная избыточность; нештатные ситуации.

USING OF COMBINED GLONASS AND GPS NAVIGATION FIELD FOR AIRCRAFT POSITIONING UNDER DIFFICULT ARCTIC CONDITIONS

Baburov Vladimir, Vasileva Natalya, Ivantsevich Nataliya
Institute of Avionics Engineering “Navigator”
14Z/19, Shkiperski Protok, St. Petersburg, 199106, Russia
e-mails: baburov@navigat.ru, nvivantsevich@yandex.ru, nvv64@rambler.ru

Abstract. The information characteristics of the combined GLONASS and GPS navigation field in the Arctic region of Russia are investigated for different values of the satellite elevation masks. The possibility of using the obtained information redundancy to form controlled working constellations of satellites in aircraft receiver in emergency situations is evaluated.

Keywords: imitating modeling; satellite navigation systems; information redundancy; emergency situation.

Для улучшения навигационного обслуживания воздушных судов в Арктике в сложных условиях пилотирования и в нештатных ситуациях может быть применён способ, основанный на совместном использовании навигационных полей двух спутниковых систем, ГЛОНАСС + GPS.

В докладе исследуются информационные и структурные характеристики навигационного поля ГЛОНАСС + GPS в зависимости от допустимых углов возвышения спутников; оценивается возможность нештатного использования навигационного поля в сложных условиях пилотирования путём формирования на потребителе управляемых рабочих созвездий спутников с исключением из состава принимаемых ИСЗ тех, сигналы которых искажены либо отраженными сигналами, либо организованными помехами.

Применён методом имитационного математического моделирования. Определяющийся объект располагался в Арктике; баллистические структуры систем ГЛОНАСС и GPS соответствовали 2019 году; число испытаний n = 100000 на временном интервале повторяемости конфигурации ГЛОНАСС + GPS.

В результате моделирования были установлены пределы применимости метода управляемых рабочих созвездий ИСЗ при навигационных определениях по ГЛОНАСС+GPS в сложных условиях пилотирования. Достоинством метода является простота его реализации в используемых в настоящее время авиационных навигационных комплексах.

СПИСОК ЛИТЕРАТУРЫ

1. "Основы государственной политики Российской Федерации в Арктике на период до 2020 года и дальнейшую перспективу" (утв. Президентом РФ 18.09.2008 N Пр-1969).
2. ГЛОНАСС. Принципы построения и функционирования / Под ред. А.И. Перова, В.Н. Харисова. Изд. 4-е, перераб. и доп. – М: Радиотехника, 2010, 800 с.
3. Бабуров В.И., Васильева Н.В., Иванцевич Н.В. Исследование структурных свойств навигационного поля СРНС ГЛОНАСС в Арктическом регионе России //Труды XXIII Санкт-Петербургской Международной конференции по интегрированным навигационным системам. 2016. С. 455-458.
4. Бабуров В.И., Иванцевич Н.В., Васильева Н.В., Панов Э.А. Совместное использование навигационных полей спутниковых радионавигационных систем и сетей псевдоспутников. – СПб, Изд-во «Агентство ”РДК-Принт”», 2005, 264 с.
5. Глобальная навигационная спутниковая система ГЛОНАСС. Интерфейсный контрольный документ. Редакция 5.1. – М.: РНИИ КП, 2008, 74 с.

УДК 004

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ МОРСКОЙ ТЕХНИКИ КЛАССА «СКРУББЕРЫ»

Богданов Евгений Гивиевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: bogdanov.gek01@mail.ru

Аннотация. Настоящее предложение относится к усовершенствованному способу и установке для очистки выхлопных газов морских судов. Установка скрубберов (SCR-технологии), устройство, нейтрализующее вредные вещества выхлопных газов и систем избирательного каталитического восстановления для очистки выхлопных газов от серы и диоксидов азота. При этом используется мокрая очистка выхлопных газов морских судов с целью уменьшения содержания в выхлопных газах веществ, вредных для окружающей среды.

Ключевые слова: очистка выхлопных газов, нейтрализующее вредные вещества, мокрая очистка, окружающая среда.

MODELING THE PROCESSES OF CREATING AND OPERATING AN OMT CLASS “SCRUBBERS”

Bogdanov Evgeny
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: bogdanov.gek01@mail.ru

Abstract. The present invention relates to an improved method and installation for the exhaust gas purification of ships. Installation of scrubbers (SCR-technologies), a device that neutralizes harmful substances from exhaust gases and selective catalytic reduction systems for cleaning exhaust gases from sulfur and nitrogen dioxide. More specifically, this relates to methods and means for purifying the exhaust gases of marine vessels in order to contain substances harmful to the environment in the exhaust gases.

Keywords: cleaning of exhaust gases, neutralizing harmful substances, wet cleaning, environment.

В настоящий момент в мире заказаны или уже установлены скрубберы примерно на 1000 судах. Об этом сообщает seatrade-maritime.com. Крупнейшие судовладельцы Spliethoff, Frontline, DHT и StarBulk выбрали скрубберы для соответствия стандарту Международной морской организации (ИМО) по содержанию серы в топливе (не более 0,5% с января 2020 года).

Скрубберы начали устанавливать и на крупные суда, главным образом из-за того, что они экономически выгодны, и срок окупаемости составляет 12 месяцев.

В основном скрубберная система устанавливается на суда, уже находящиеся в эксплуатации (63%). Новые суда составляют 37%. Основную долю судовладельцев, предпочитающих скрубберы, составляют китайские компании - 60% для б/у судов и 85% - для новостроя.

Моделирование процессов создания и эксплуатации объектов морской техники класса «скрубберы» в части комплексного планирования и обоснования выбора экспериментальных средств проведения исследований по созданию и эксплуатации объекта морской техники заданного класса.

Для комплексного планирования и обоснования выбора экспериментальных средств проведения исследований по созданию и эксплуатации объекта морской техники данного класса был использован программный комплекс «АСОР-14.5», разработанный в СПбГМТУ, реализующий метод количественного оценивания проектного качества.

Сравнение скрубберов по качеству было выполнено методом квалиметрического ранжирования. Выявлен лучший скруббер варианта «4.СВ-Кк» среди своих аналогов, рассмотрены их сильные и слабые стороны.

В результате выполненной работы, была разработана модель оценки конкурентной способности объекта, с качественной и количественной оценкой полученных результатов. Проведен качественный и количественный анализ пяти скрубберов. Выявлен лучший вариант среди аналогов, это скруббер СВ-Кк, также определены их качества, преимущества и недостатки

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В. Моделирование процессов создания и эксплуатации морской техники (МПСЭ МТ). Курс лекций. СПб, 2017.
2. Алексеев А.В. Числовое моделирование процессов стратегического развития ОМТИ / Корабельная энергетика: из прошлого в будущее. – СПб.: СПбГМТУ, 2017, с. 329 – 334.

УДК 656.61

БЕЗОПАСНОЕ МАНЕВРИРОВАНИЕ СУДНА В РАЙОНАХ СО СТЕСНЕННЫМИ УСЛОВИЯМИ ПЛАВАНИЯ С ПРИМЕНЕНИЕМ АППАРАТА ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Биденко Сергей Иванович[1], Храмов Игорь Сергеевич[2]

[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

[2] Государственное казенное учреждение Тверской области «Центр информационных технологий»
Студенческий пер., 28, Тверь, 170100, Россия

e-mails: sibidenko@mail.ru, igorhramov@yahoo.com

Аннотация. Обоснованы направления повышения эффективности информационной поддержки судовождения в условиях со сложной быстроменяющейся навигационной и тактической обстановкой. Представлен алгоритм оперативной выработки рекомендаций по уклонению и расхождению с опасными целями, основанный на аппарате искусственных нейронных сетей. Даны практические рекомендации по реализации метода.

Ключевые слова: информационная система судна, район со стесненными условиями плавания, управление судном, безопасное маневрирование, искусственные нейронные сети, многослойный перцептрон.

SAFE MANEUVERING OF THE VESSEL IN AREAS WITH RESTRICTED NAVIGATION CONDITIONS USING ARTIFICIAL NEURAL NETWORKS

Bidenko Sergey[1], Khramov Igor[2]

[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia

[2] State Treasury Institution of the Tver Region "Information Technology Center"
28, Student lane, Tver, 170100, Russia

e-mails: sibidenko@mail.ru, igorhramov@yahoo.com

Abstract. The directions to improve the efficiency of information support for navigation in conditions with complex fast-changing navigation and tactical conditions are substantiated. Presented algorithm of operational development of recommendations on evasion and divergence with dangerous targets, based on the apparatus of artificial neural networks. Practical recommendations have been given to implement the method.

Keywords: ship information system, area with cramped sailing conditions, ship control, safe maneuvering, artificial neural networks, multi-layered perceptron.

Передвижение судов в акваториях со стесненными условиями (прибрежная зона, подходы к портам, узкости, мелководье) является наиболее сложным в навигационном отношении. Здесь навигационная обстановка является высокодинамической в силу наличия малых глубин, изменения гидрометеорологических условий, сложной конфигурации фарватера, возможного появления малых судов (быстроходные катера и скутеры, яхты, рыбаки) следующих отличающимися от рекомендованных курсами и т.д. При этом постоянно возникает и решается задача изменения курса судна для уклонения (расхождения) от возникающих навигационных опасностей. Известны определенные приемы, подходы и методики поддержки управления судном, маневрирующим в сложных навигационных условиях [1-19]. Это методы и системы искусственного интеллекта [2-4], семантические сети, траекторные подходы [5-7], оценки и прогнозирования навигационной ситуации [8-10], зональная навигация, ситуационное управление [11-16], анализ иерархий [17-18], ключевых индикаторов и др. При использовании этих систем поддержки требуется определенное время для выполнения расчетов для выработки рекомендаций по расхождению с опасными целями, безопасному маневрированию. Меньшее расчетное время требуется при использовании аппарата искусственных нейронных сетей (ИНС), так как они опираются на априорные обучающие выборки [19]. ИНС здесь применяются во вторичной обработке поступающих с радара сигналов для обучения по специальной выборке, состоящей из формальных математических представлений возможных рекомендуемых (безопасных) вариантов маневрирования судна.

Рассмотрим суть метода на следующем примере простейшей ситуации управления судном.

Предположим, что транспортное средство двигается в определенной акватории с помощью управляющего элемента, который имеет определенный радиус «зрения» (наблюдения). Для упрощения используем круг обзора, но можно рассматривать и реальный усеченный шестью пересекающимися плоскостями конус. Стоит отметить, что управляющий элемент в нашей ситуации – функция, которой на вход подаются внешние факторы из радиуса обзора, а на выход – реакцию судна на эти факторы. В связи с тем, что таких факторов может быть несколько, то есть – несколько входов и выходов, будем использовать нейронную сеть обратного распространения, так как она позволяет аппроксимировать такие функции. По сути, такая сеть представляет собой многослойный перцептрон, в котором метод обратного распространения ошибки обучает все слои за один проход.

Преимуществом данной сети также является ее обучаемость, что упростит задачу расстановки весов для нейронов. Для решения поставленной задачи будем рассматривать нейронную сеть, состоящую из 6 слоев. Экспериментальным путем установлено, что достаточная точность достигается при минимуме в 4 слоя, однако при 6 слоях точность вычислений выше, при этом дальнейшее увеличение числа слоев не дает ощутимого прироста точности, при этом значительно увеличивая время работы программы и нагрузку на машинные мощности. Во входном слое для

упрощения модели мы разместим три нейрона, в выходном – два. В промежуточных слоях расположим по 9 нейронов (дальнейшее увеличение их числа не имеет смысла, не давая прироста в точности, но замедляя систему).

В качестве функции активации нейрона применим сигмоидальную функцию.

Данная функция позволяет усиливать слабые сигналы, что делает ее предпочтительной для решения поставленной задачи. Дополнительно, она позволяет существенно сократить вычислительную сложность метода обратного распространения ошибки.

Для того чтобы вычислить положение, необходима позиция (x, y) каждого объекта, положение (x, y) судна и угол транспортного средства (рис. 2). Нам также необходимы r (радиус окружности) и dright, dleft – векторы между автомобилем и линиями Lright и Lleft., параллельными направлению движения автомобиля. Оба вектора перпендикулярны линиям. Для простоты представим, что наша модель двумерная, так как корабль не может двигаться в третьем измерении, поскольку он не взлетает и не ныряет. Таким образом, заметим, что в данной модели не учитываются рифы и подводные объекты. Для учета данных объектов необходимо усложнение модели и введение третьего измерения.

Для каждого объекта в радиусе обзора определяем, находится он в левом поле зрения, правом, или по центру. На вход в нейронную сеть подается массив A. Расстояния до ближайшего препятствия слева, в центре, и справа от транспортного средства будут храниться в A[0], A [1] и A[2]соответственно.

Вычислим уравнения линий Lright и Lleft, которые помогут нам определить, находится препятствие справа, слева или по центру от транспортного средства.

Затем мы проверим, находится ли объект в пределах круга. Для каждого объекта в пределах круга, мы должны проверить, находится он справа, слева или по центру от судна. Теперь сохраняем расстояние в соответствующей части массива (A[0], A[1] или A[2]) при условии, что ранее сохраненное расстояние больше, чем только что вычисленное. Изначально, массив A должен быть инициализирован значениями 2r. После проверки каждого объекта, у нас есть массив A с расстояниями до ближайших объектов справа, по центру и слева от судна. Если не было найдено ни одного объекта в данном поле зрения, элемент массива будет иметь значение по умолчанию 0, что означает отсутствие объектов в радиусе обзора.

Поскольку нейронная сеть использует сигмовидную функцию, входные данные должны лежать в пределах от 0,0 до 1,0. 0,0 будет означать, что объект касается транспортного средства и 1,0 означает, что нет объектов в пределах видимости. Поскольку мы установили максимальное расстояние, на котором может видеть управляющий элемент, мы легко можем привести все расстояния к диапазону от 0,0 до 1,0.

На выходе получаем указания по изменению скорости судна и направления. Это могут быть ускорение, торможение и угол поворота рулевого колеса. Так что нам нужно два выхода; один будет значением ускорения/торможения (торможение - отрицательное ускорение), а другой будет указывать изменение направления.

Результат лежит между 0,0 и 1,0 по той же причине, что и входные данные. Для ускорения 0,0 означает "стоп машина"; 1,0 — "полный вперед" и 0,5 — отсутствие торможения или ускорения. Для рулевого управления, 0,0 означает «лево руля», 1,0 – «право руля» и 0,5 – не изменять направление.

"Отрицательное ускорение" будет означать торможение, если транспортное средство движется вперед, либо движение в обратном направлении, если судно находится в состоянии покое. Кроме того, "положительное ускорение" означает торможение, если транспортное средство движется в обратном направлении.

Стоит также отметить, что данная нейронная сеть нуждается в длительном обучении на большом количестве наборов. Отметим, что в данном случае классические проблемы алгоритма обратного распространения ошибки, связанные с возможностью бесконечного обучения, решаются выбором шага спуска, который вычислялся опытным путем. Также набор обучающих данных был сформирован на основе практических наблюдений за поведением нейронной сети на симуляторе и состоит из 500 обучающих наборов, то есть 500 векторов, состоящих из 5 значений: трех, соответствующих входам и двух, соответствующих выходам.

Кроме того, следует отметить ряд проблем, возникающих при использовании данной модели. Они возникают из-за принятых упрощений в рассматриваемой модели пространства. Судно может оставаться на месте на время, поскольку оно колеблется в решении вопроса – идти вправо или влево. Исправить это не так легко, пытаясь настроить веса нейронной сети. Решением может выступать добавление принудительного действия в случае остановки более, чем на указанное время. Транспортное средство не различает небольшой разрыв между двумя рифами. Поскольку в модель изначально не закладывался высокий уровень точности в зрении (только три позиции: слева, в центре, справа), два объекта, находящиеся близко друг к другу, будут для искусственного интеллекта похожи на стену. Для решения данной проблемы необходимо ввести больше различных позиций положения препятствий. Для ускорения работы данной сети в ситуациях с более сложной областью зрения и большей точностью принятия решения возможно использовать графические процессоры, однако данная оптимизация выходит за рамки рассмотрения данной статьи. Сама по себе данная нейронная сеть не имеет чёткой цели движения, однако при добавлении конкретной цели и присоединении нейронной сети, анализирующей обстановку в ближней зоне, получается полноценный формальный аппарат, отвечающий за передвижение судна либо иного транспортного средства.

СПИСОК ЛИТЕРАТУРЫ

1. Астреин В.В. Разработка технологий выработки решений по предупреждению столкновений судов в море / Автореф. дис. канд. техн. наук: 05.22.19. - Новороссийск - 2011. - 24 с.
2. Васильев С. Н. Интеллектуальное управление динамическими системами / С. Н. Васильев, А. К. Жерлов, Е. А. Федосов [и др.]. — М.: Физматлит, 2000. — 352 с.
3. Смоленцев С. В. Концепция автоматизированной интеллектуальной системы расхождения судов / С. В. Смоленцев, Б. В. Афанасьев, А. Е. Филяков, Д. В. Куниц // Эксплуатация морского транспорта. — 2012. — № 4 (70). — С. 11–14.

4. Zhilenkov, A.A. Intelligent autonomous navigation system for UAV in randomly changing environmental conditions / A. A. Zhilenkov, S. S. Sokolov, S. G. Chernyi, A. P. Nyrkov // Journal of Intelligent and Fuzzy Systems, Vol. 38, No. 5. – 2020. – Pp. 6619 - 6625. https://doi.org/10.3233/JIFS-179741
5. Вагущенко Л.Л., Вагущенко А.Л. Поддержка решений по расхождению с судами. Одесса: Фенікс, 2010. – 229 с.
6. Мальцев А.С. Маневрирование судов при расхождении: Одесса: ЦПАП, 2005. - 208с.
7. Нырков А.П. Алгоритм управления движением судов, идущих пересекающимися курсами / Нырков А.П., Викулин П.В. // Журнал университета водных коммуникаций. – № 1, 2011. – С. 100 – 105.
8. Дмитриев, В.И. Современные навигационные системы и безопасность судовождения / В.И. Дмитриев, В.И. Фарофонов.– М.: Моркнига, 2010. – 160 с.
9. Вайгандт Н.Ю. Повышение точности навигационных систем водного транспорта при помощи технологии референцных станций / Вайгандт Н.Ю., Нырков А.П. // IT: ВЧЕРА, СЕГОДНЯ, ЗАВТРА – 2013: материалы науч.–техн. конференции. – СПб.: ГУМРФ имени адмирала С.О. Макарова, 2013. – С. 64–69.
10. Смоленцев С. В. Проблема оценки навигационной ситуации в море / С. В. Смоленцев // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2015. — № 6 (34). — С. 23–28.
11. Мелихов А.Н., Бернштейн Л.С., Коровин С.Я. Ситуационные советующие системы с нечеткой логикой. - М.: Наука, 1990.
12. Васьков А.С., Мироненко А.А. Система поддержки принятия решений в судовождении. //Сб. научн. тр. – Новороссийск: НГМА, 2003. - Вып.8. С. 5-11.
13. Васьков В.А. Некоторые принципы системы поддержки принятия решения в судовождении //Сб. научн. тр. – Новороссийск: НГМА, 2013. - Вып.3. С. 15-21.
14. Смоленцев С. В. Автоматический синтез решений по расхождению судов в море // Вестник ГУМРФ. - Выпуск 2 (36). - 2016. - С. 7 – 15
15. Нырков А.П. Программно-аппаратная реализация системы предупреждения аварийной ситуации для объектов морского транспорта / А. П. Нырков, А. А. Жиленков, С. С. Соколов, С. Г. Черный // Автоматизация в промышленности. – № 1, 2016. – С. 26 – 30.
16. Родионов А.И. Автоматизация судовождения. – М.: Транспорт,1992. – 192с.
17. Субанов Э.Э. Разработка моделей эффективной оценки опасности столкновения судов при принятии решения методом анализа иерархий./ Автореф. дис. канд. техн. наук: 05.22.19.- Новороссийск - 2012.- 24 с.
18. Субанов Э.Э., Миронов А.В. Использование модифицированной модели метода анализа иерархий для безопасного расхождения морских судов // Эксплуатация морского транспорта. – 2014. - №1 - С. 24 – 28
19. Хайкин, С. Нейронные сети: полный курс, 2-е издание. [Текст]: Пер. с Англ. – М.: Издательский дом «Вильямс», 2006.

УДК 656.61

ОЦЕНКА НАВИГАЦИОННО-ТАКТИЧЕСКОЙ ОБСТАНОВКИ И ВЫРАБОТКИ РЕКОМЕНДАЦИЙ НА ОСНОВАНИИ ПРОЦЕДУРЫ ТОПОЛОГИЗАЦИИ ГЕОГРАФИЧЕСКОЙ РЕАЛЬНОСТИ

Биденко Сергей Иванович[1], Храмов Игорь Сергеевич[2]

[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия

[2] Государственное казенное учреждение Тверской области «Центр информационных технологий»
Студенческий пер., 28, Тверь, 170100, Россия
e-mails: sibidenko@mail.ru, igorhramov@yahoo.com

Аннотация. Обоснована применимость аппарата искусственных нейронных сетей в задачах оперативной оценки обстановки и выработки рекомендаций по управлению судном. Описано представление навигационной и тактической обстановки для использования аппарата ИНС. Определен порядок формирования целевых параметров и диапазон выходных оценок. В качестве архитектуры нейронной сети выбрана рекуррентная нейронная сеть с архитектурой типа многослойный перцептрон. Для обучения нейронной сети использован алгоритм обратного распространения ошибки, представляющийся оптимальным для задачи классификации с применением рекуррентной нейронной сети. Приведены процедуры анаморфирования геоизображения обстановки для обеспечения процедур оценки территориальной ситуации и построения оптимальных маршрутов переходов судна в исследуемой акватории.

Ключевые слова: информационная система судна, территориальная ситуация, оценка обстановки, анаморфоза, искусственная нейронная сеть.

EVALUATION OF NAVIGATION-TACTICAL SITUATION AND MAKE RECOMMENDATIONS BASED ON THE TYPOLOGY OF GEOGRAPHICAL REALITY

Bidenko Sergey[1], Khramov Igor[2]

[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia

[2] State Treasury Institution of the Tver Region "Information Technology Center"
28, Student lane, Tver, 170100, Russia
e-mails: sibidenko@mail.ru, igorhramov@yahoo.com

Abstract. The applicability of the artificial neural network apparatus in the tasks of operational assessment of the situation and recommendations for ship management is substantiated. The presentation of the navigational and tactical environment for the use of the INS apparatus is described. The order of the target parameters and the range of output estimates have been defined. A neural network architecture is chosen as a recurrent neural network with a multi-layered perceptron architecture. To train the neural network, an algorithm of reverse error propagation is used, which is optimal for the task of classification using a recurrent neural network. Procedures for anamorphizing the geo-image of the situation are presented to ensure procedures for assessing the territorial situation and constructing optimal routes of the ship's crossings in the study area.

Keywords: ship information system, territorial situation, situation assessment, anamorphosis, artificial neural network.

Анализ и оценка территориальной ситуации осуществляется во многих научных исследованиях и практических приложениях: геологические изыскания, оборона, гидрометеорологические прогнозы, районная планировка, навигация, и др. Наиболее сложным процесс оценки обстановки является в там, где условия окружающей среды меняются достаточно быстро (гидрометеорология, морские и воздушные перевозки, боевые действия и др.). Актуальным направлением является внедрение искусственного интеллекта в системы территориального анализа и управления. Искусственные нейронные сети [3], являющиеся характерным представителем систем искусственного интеллекта, широко используются во многих научных и технических приложениях (сложные динамические системы, системы диагностики, классификационные системы) [4], но до настоящего времени в системах территориального анализа не применялись. Хотя аппарат ИНС содержат значительный аналитический потенциал по классификации и оценке больших массивов высоко динамических данных. Поэтому цель работы – внедрение аппарата искусственных нейронных сетей (ИНС) в процедуры территориального анализа. Конкретно решается задача оценки обстановки в ближней морской зоне для выбора маршрутов или районов безопасного маневрирования судов с учетом различных территориальных факторов: ледовая обстановка, ветер, течения, экологические ограничения, хозяйственная активность, социальные факторы и др.

Для описания методики построения оптимального маршрута рассмотрим конкретную задачу: построение оптимального и безопасного маршрута перехода судна из пункта А (Бугрино) в пункт В (Варнек) в условиях меняющейся ледовой обстановки с учётом дополнительных параметров территориальной ситуации (течения, ветер, осадки, видимость, экологическая безопасность, навигационные опасности, интенсивность судоходства и др.)

Методика основана на работе искусственных нейронных сетей и оценке обстановки в ближней морской зоне. В связи с этим, необходимо осуществить постановку задачи в условиях модели представления обстановки в ближней морской зоне.

Параметры модели представляют собой совокупность данных, полученных из открытых источников, размещенных на геопорталах map.openseamap.org и gis.adm-nao.ru.

Полученные векторы параметров обобщаются в виде таблицы данных, которая затем будет подана для обучения искусственной нейронной сети.

В качестве входных данных будет выступать модель обстановки в ближней морской зоне, оптимизированная для работы с ИНС, с нанесенными на нее исходной и конечной точками маршрута. Данная модель получается топологическим переходом от географической карты к картоиду, аналогичным подходу, описанному в методике оценки обстановки в ближней морской зоне.

Важным моментом данного этапа является нанесение координатной сетки. От этого зависит точность последующего анаморфирования.

В основе дальнейших преобразований описываемой методики лежит каскад искусственных нейронных сетей одинаковой архитектуры: рекуррентная нейронная сеть. Модель подается на вход только первой нейронной сети. Вторая сеть получает на вход результаты работы первой сети, то есть преобразованный картоид оценки обстановки.

Вторым этапом методики является проведение оценки обстановки, согласно перечисленным входным векторам и условиям задачи. Однако, в отличие от методики оценки обстановки в ближней морской зоне, в целях ускорения работы системы данный этап проводится только в режиме изменения размерности и не имеет этапа финального контроля человеком. Дополнительно следует понизить разрешение графической составляющей, так как на данном этапе она не важна, но ее обработка может занять существенную часть ресурсов и повлечь за собой увеличение времени обработки данных.

Результирующий картоид подается на вход второй нейронной сети. Согласно проведенным экспериментам, нейронная сеть имеет архитектуру многослойного перцептрона с обратной связью, т.е. рекуррентной нейронной сети. Данная нейронная сеть является второй частью каскада нейронных сетей, лежащего в основе данной методики. На вход сети подаются результаты работы первой нейронной сети, то есть анаморфированный картоид оценки обстановки в ближней морской зоне.

Обучение второй нейронной сети также осуществляется с помощью алгоритма обратного распространения ошибки, однако существенно изменена структура обучающего набора. В данной ситуации оцениваются не каждая область по отдельности, а все области целиком. То есть обучающее множество состоит из матрицы, строками которой являются соответствующие области, на которые разбит картоид, а столбцами входные значения: удаленность от кратчайшего маршрута и оценка обстановки в данном регионе, а также выходное значение, принимающее значения 0 и 1 – соответственно маршрут не проходит либо проходит через рассматриваемую область.

Затем с учетом заданной ранее координатной сетки осуществляется процесс детопологизации, то есть перехода от графического картоида к географической карте. Стоит отметить, что при использовании классических моделей на основе shape-файлов подобный переход не является возможным. При этом он составляет важный шаг методики, позволяя выстроить маршрут в условиях реальной карты.

Результатом работы методики является карта с выделенными исходным и конечным пунктами и построенным между ними маршрутом.

Оптимальность построенного маршрута во многом зависит от количества обучающих наборов, и соответственно этапа обучения нейронной сети. На рисунке ниже приведены маршруты, построенные нейронной сетью на различных этапах ее обучения в условиях поставленной задачи.

Дополнительно был проведен эксперимент с переносом полностью обученной нейронной сети в иные условия. Был рассмотрен вариант построения оптимального маршрута с переносом на реалии Карского моря, с сохранением начальных условий – рассматривается ледовая обстановка в ближней морской зоне. При первом запуске нейронной сети точность маршрута соответствовала примерно обучению приблизительно на половине наборов. Однако процент ошибки падал значительно быстрее, чем при первичном обучении.

Предложенная методика построения маршрута на основании оценки обстановки в ближней морской зоне отличается наличием дополнительных процедур топологизации для поиска решений в географически абстрактной среде и детопологизации первичного решения для адаптации его в географически конкретной обстановке с применением аппарата ИНС.

СПИСОК ЛИТЕРАТУРЫ

1. Биденко С.И., Панамарев Г.Е. Геоинформационная поддержка управления сложными территориальными объектами и системами. - Новороссийск: Изд-во МГА, 2011. – 202 с.
2. Гусейн-Заде С.М., Тикунов В.С. Анаморфозы: что это такое? - М.: Эдиториал УРСС, 1999. – 168 с.
3. Храмов И.С. Перспективы развития искусственного интеллекта // Актуальные направления научных исследований XXI века: теория и практика. 2015. Т. 3. № 8-1 (19-1). С. 375-377.
4. Храмов И.С. Интеграция искусственных нейронных сетей с геоинформационными системами // Вестник ТвГУ. – Серия «Математические методы управления». – 2017. – С. 118-120.
5. Шилин М.Б., Биденко С.И., Кравченко П.Н. Концепция моделирования геоэкологической ситуации // Ученые записки РГГМУ. – 2015. – № 39. – С. 157 – 164.
6. Хайкин, С. Нейронные сети: полный курс, 2-е издание. [Текст]: Пер. с Англ. – М.: Издательский дом «Вильямс», 2006. – 1104 с.
7. Сигеру Омату. Нейроуправление и его приложения. Neuro-Control and its Applications. [Текст]: монография: 2-е изд. / Сигеру Омату, Марзуки Халид, Рубия Юсоф — М.: ИПРЖР, 2000. — 272 с.
8. Апальков Ю. В. Противолодочные корабли. — Моркнига. — М., 2010. — С. 148.
9. Ведерников Ю.В. Красный дракон: современные военно-морские силы Китая. — Флот Тихого океана. — Владивосток., 2007. — С.140
10. Michael T. Gastner and M. E. J. Newman. Density-equalizing map projections:Diffusion-based algorithm and applications. PNAS May 18, 2004 101 (20) 7499-7504.

УДК 004.056

5G СЕТЬ НОВОГО ПОКОЛЕНИЯ

Белова Мария Александровна, Рыськина Василиса Игоревна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, г. Санкт-Петербург, 198035, Россия
e-mails: m-belova123@mail.ru, vasilisa.rys@mail.ru

Аннотация. Рассмотрим сеть 5G, концепцию ее безопасности, основные процедуры и места особой уязвимости.

Ключевые слова: Сети 5G; SIM-карта; защита; шифрование; контроль целостности; безопасность сети; аутентификация.

5G NEW GENERATION NETWORK

Belova Maria, Ryskina Vasilisa
Admiral Makarov State University Of Maritime And Inland Shipping
5/7, Dvinskaya St., St. Petersburg, 198035, Russia
e-mails: m-belova123@mail.ru , vasilisa.rys@mail.ru

Abstract. Consider the 5G network, its security concept, basic procedures, and places of special vulnerability.

Keywords: 5G networks; SIM card; protection; encryption; integrity control; network security; authentication.

Общение является неотъемлемой частью нашего общества. Уже сегодня большая часть нашего общения является цифровой и включает в себя связь человека с машиной и машины с машиной. За предыдущие десятилетия мы также испытали резкое увеличение трафика связи (осуществляется в стандартных коммерческих телекоммуникационных сетях). На транспорте это также актуально, т.к. оказывает значительное влияние на транспортную безопасность [1-3]. Ожидается, что эти тенденции сохранятся, и предстоящее поколение телекоммуникационных сетей, а именно сетей 5G, призвано обеспечить это увеличение.

Сети 5G также должны предлагать решения для эффективного и экономически эффективного запуска множества новых услуг, адаптированных для различных вертикальных рынков с различными требованиями к обслуживанию и с участием большого числа участников. Возможности 5G существенно увеличивают стабильность и скорость обновления электронного оборудования на водном транспорте.

Но с мощным функционалом и огромным количеством возможностей 5G-технология также преподносит множество вопросов в плане безопасности таких сетей.

Но для начала стоит рассмотреть архитектуру сети 5G.

1. Архитектура 5G. Архитектура безопасности 5G — совокупность механизмов и процедур безопасности, реализованных в сетях 5-го поколения и охватывающих все компоненты сети, начиная от ядра и заканчивая радиоинтерфейсами.

Для начала обратимся к ключевым принципам архитектуры 5G-сетей, которые позволят далее в полной мере раскрыть смысл и зоны ответственности каждого программного модуля и каждой функции безопасности 5G.

Разделение сетевых узлов на элементы, обеспечивающие работу протоколов пользовательской плоскости (для передачи абонентской информации) и элементы, обеспечивающие работу протоколов плоскости управления (отвечает за логику работы сетевого устройства).

Поддержка механизма network slicing (разделение одной физической среды на несколько логических), основываясь на услугах, предоставляемых конкретным группам конечных пользователей.

Реализация сетевых элементов в виде NFV (виртуальных сетевых функций).

Поддержка одновременного доступа к централизованным и локальным службам, т. е. реализация концепций облачных и пограничных вычислений.

Реализация конвергентной (объединение, бывших ранее раздельными) архитектуры, объединяющей различные типы сетей доступа — 3GPP 5G New Radio и non-3GPP (Wi-Fi и т. п.) — с единым ядром сети.

Поддержка единых алгоритмов и процедур аутентификации вне зависимости от типа сети доступа.

Поддержка сетевых функций без сохранения состояния, в которых вычисляемый ресурс отделен от хранилища ресурсов.

Взаимодействие между сетевыми функциями представлено двумя способами: сервис-ориентированное и интерфейсное.

2. Концепция безопасности сетей 5G и ее основные процедуры:

А. Непосредственно то, что включает концепция:

Аутентификацию пользователя со стороны сети.

Аутентификацию сети со стороны пользователя.

Согласование криптографических ключей между сетью и пользовательским оборудованием.

Шифрование и контроль целостности сигнального трафика.

Шифрование и контроль целостности пользовательского трафика.

Защиту идентификатора пользователя.

Защиту интерфейсов между различными элементами сети в соответствии с концепцией сетевого домена безопасности.

Изоляцию различных слоев механизма network slicing и определение для каждого слоя собственных уровней безопасности.

Аутентификацию пользователя и защиту трафика на уровне конечных сервисов (IMS, IoT и других) [4].

В. Процедуры:

1) Домены доверия. В сетях 5-ого поколения доверие к элементам сети снижается по мере удаления элементов от ядра сети. Эта концепция влияет на решения, реализованные в архитектуре безопасности 5G. Таким образом, можно говорить о модели доверия 5G-сетей, определяющей поведение механизмов безопасности сети. Со стороны пользователя домен доверия образуют UICC и USIM. На стороне сети домен доверия имеет более сложную структуру.

Сеть радиодоступа подразделяется на две составляющие — DU (от англ. Distributed Units — распределенные единицы сети) и CU (от англ. Central Units — центральные единицы сети).

Вместе они формируют gNB — радиоинтерфейс базовой станции сети 5G. В ядре сети располагается AMF (от англ. Access & Mobility Management Function — функция управления доступом и мобильностью), терминирующая трафик механизмов безопасности NAS(функциональный уровень в стеках протоколов беспроводной связи между базовой сетью и пользовательским оборудованием). В текущей спецификации 3GPP 5G Phase 1 описано совмещение AMF с функцией безопасности SEAF (обеспечивает аутентификацию пользователей при их регистрации в сети с любой технологией доступа), содержащей корневой ключ (также известный как «якорный ключ») посещаемой (обслуживающей) сети. AUSF отвечает за хранение ключа, полученного после успешной аутентификации. Он необходим для повторного использования в случаях с одновременным подключением пользователя к нескольким сетям радиодоступа. ARPF (Authentication Credential Repository and Processing Function — функция хранилища и обработки учетных данных аутентификации) хранит учетные данные пользователей и является аналогом USIM у абонентов. UDR (является, по сути, базой данных всех абонентов сети) и UDM (англ. Unified Data Management — унифицированная база данных) хранят пользовательскую информацию, которую используют для определения логики генерации учетных данных, идентификаторов пользователей, обеспечения непрерывности сессии и др.

2) Иерархия ключей и схемы их распределения. В сетях 5-ого поколения, в отличие от сетей 4G-LTE, процедура аутентификации имеет две составляющие: первичную и вторичную аутентификацию. Первичная аутентификация обязательна для всех пользовательских устройств, подключающихся к сети. Вторичная аутентификация может производиться по запросу от внешних сетей, если абонент к таковым подключается [5].

3. Уязвимости сети 5G:

А. Уязвимости, связанные с SIM-картами:

1) Уязвимости непосредственно самих SIM-карт. SIM-карта представляет собой сложное устройство, на котором имеется даже целый набор встроенных приложений — SIM Toolkit, STK. Одна из таких программ — S@T Browser — теоретически может использоваться для просмотра внутренних сайтов оператора, но на практике давно забыта и не обновлялась с 2009 года, поскольку сейчас эти функции выполняют другие программы.

Проблема в том, что S@T Browser оказался уязвимым: специально подготовленная служебная SMS взламывает SIM-карту и заставляет её выполнить нужные хакеру команды, причём пользователь телефона или устройства не заметит ничего необычного. Атака получила название Simjaker и даёт массу возможностей злоумышленникам.

В частности, она позволяет передать злоумышленнику данные о местоположении абонента, идентификатор его устройства (IMEI) и сотовой вышки (Cell ID), а также заставить телефон набрать номер, отправить SMS, открыть ссылку в браузере и даже отключить SIM-карту.

В условиях сетей 5G эта уязвимость SIM-карт становится серьёзной проблемой, учитывая количество подключённых устройств. Хотя SIMAlliance и разработал новые стандарты SIM-карт для 5G с повышенной безопасностью, в сетях пятого поколения по-прежнему возможно использование «старых» SIM-карт. А раз всё и так работает, ожидать быстрой замены имеющихся SIM-карт не приходится.

Использование Simjacking позволяет принудительно переключить SIM-карту в режим роуминга и заставить её подключиться к сотовой вышке, которую контролирует злоумышленник. При этом атакующий получит возможность модифицировать настройки SIM-карты, чтобы прослушивать телефонные разговоры, внедрять вредоносное ПО и проводить различные виды атак с использованием устройства, содержащего взломанную SIM-карту. Сделать это ему позволит тот факт, что взаимодействие с устройствами в роуминге происходит в обход процедур безопасности, принятых для устройств в «домашней» сети.

2) Уязвимости сети через SIM-карту. Злоумышленники могут менять настройки скомпрометированной SIM-карты для решения своих задач. Относительная лёгкость и скрытность атаки Simjaking позволяют проводить её на постоянной основе, захватывая контроль над всё новыми и новыми устройствами, медленно и терпеливо (low and slow attack) [6] отрезая кусочки сети подобно ломтикам салями (salami attack) [7]. Отследить такое воздействие крайне сложно, а в условиях сложной распределённой сети 5G — практически нереально.

А поскольку сети 5G не имеют встроенных механизмов контроля безопасности SIM-карт, постепенно злоумышленники получат возможность установить внутри коммуникационного домена 5G свои правила, используя захваченные SIM-карты для кражи средств, авторизации на сетевом уровне, установки вредоносного ПО и другой незаконной деятельности.

3)Уязвимости идентификации через SIM-карту. SIM-карта используется для идентификации устройства в сети. Если SIM-карта активна и имеет положительный баланс, устройство автоматически считается легитимным и не вызывает подозрений на уровне систем обнаружения. Между тем уязвимость самой SIM-карты делает уязвимой всю систему идентификации. ИТ-системы безопасности просто не смогут отследить незаконно подключённое устройство, если оно зарегистрируется в сети с помощью похищенных через Simjaking идентификационных данных.

Получается, что подключившийся к сети через взломанную SIM-карту хакер получает доступ на уровне настоящего владельца, поскольку ИТ-системы уже не проверяют устройства, прошедшие идентификацию на сетевом уровне.

5G-технология безусловно дает огромное количество новых возможностей и расширяет границы доступного, но и открывает новые возможности для преступности в сфере информационных технологий, которые ранее были недоступны. Также хочется отметить, что часть уязвимостей 5G унаследовала от своего предшественника (яркий пример SIM-карты), поскольку за основу, конечно же, была взята архитектура сети прошлого поколения мобильной связи.

Учитывая это, к сожалению не создано кардинально новых механизмов защиты такой сети, а скорей собран огромный ком всевозможных защитных алгоритмов и технологий, которые взаимодействуют друг с другом, но опять, же каждый из которых имеет свои уязвимости и не способен в полной мере защитить такую сеть.

СПИСОК ЛИТЕРАТУРЫ

1. Kardakova M. Cyber Security on Sea Transport / M. Kardakova, I. Shipunov, A. Nyrkov, T. Knysh // Advances in Intelligent Systems and Computing, Vol. 982. – 2020. – Pp. 481 - 490. https://doi.org/10.1007/978-3-030-19756-8_46.
2. Соколов, А. П. Ныркov, Т. П. Кныш // XXI век: итоги прошлого и проблемы настоящего плюс. – Т. 9. №2 (50). – 2020. – С. 158–163. https://doi.org/10.46548/21vek-2020-0950-0028.
3. Соколов С.С. Кибербезопасность на водном транспорте / С. С. Соколов, А. П. Ныркov, Н. Б. Глебов // Сборник тезисов докладов национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ «ГУМРФ имени адмирала С. О. Макарова». — СПб: Изд-во ГУМРФ им. адм. С.О. Макарова, 2018. – С. 177–178.
4. 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.6.0 Release 15). URL: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf (дата обращения: 10.07.2020).
5. Anand R. Prasad, Sivabalan Arumugam, Sheeba B and Alf Zugenmaier “3GPP 5G Security”, 3 May 2018.
6. What is a low and slow attack? Low and slow DDoS attack definition | Cloudflare. URL: https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/ (дата обращения: 12.07.2020).
2. What is a Salami Attack? - Aj Maurya. An Engineer. URL: https://ajmaurya.wordpress.com/2014/03/27/what-is-a-salami-attack/ (дата обращения: 13.07.2020).

УДК 681,3.067

АНАЛИЗ И ОЦЕНКА РИСКОВ В ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Голоскоков Константин Петрович, Коротков Виталий Валерьевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: goloskokovkp@gumrf.ru, korotkovvv@gumrf.ru

Аннотация. Показана необходимость проведения мероприятий для повышения надежности телекоммуникационных систем на транспорте с целью повышения точности и достоверности систем спутниковой навигации. Приведенная методика может быть рекомендована для применения при проектировании транспортных спутниковых систем связи.

Ключевые слова: телекоммуникационная система, транспорт, риски, ГЛОНАСС, функционирование, спутниковые системы, информационные ресурсы.

ANALYSIS AND ASSESSMENT OF RISKS IN THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Goloskokov Konstantin, Korotkov Vitaliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: goloskokovkp@gumrf.ru, korotkovvv@gumrf.ru

Abstract. It is shown that a number of measures should be taken to improve the reliability of telecommunications systems in transport in order to improve the accuracy and reliability of satellite navigation systems. This methods can be recommended for use in the design of transport satellite communication systems.

Keywords: telecommunications system, transport, risks, GLONASS, operation, satellite systems, information resources.

Внедрение на предприятии системы диспетчеризации и мониторинга транспорта позволяет коммерческим компаниям ускорять бизнес-процессы, бороться с халатностью и воровством сотрудников, пресекать случаи нецелевого использования служебных транспортных средств [1]. В результате эксплуатации системы спутникового мониторинга транспорта ГЛОНАСС/GPS происходит экономия средств. Максимальная экономическая эффективность достигается при использовании в системе контроля транспорта сертифицированных датчиков расхода топлива. Мониторинг транспорта (ГЛОНАСС/GPS слежение) является действенным инструментом для принятия оперативных управленческих решений. Отметим, что существуют и негативные последствия внедрения информационных и телекоммуникационных технологий.

Сдерживают рост чрезвычайно запутанная нормативная база по геодезии, картографии, секретности и прочим ключевым вопросам для навигации [2]. Жёсткость и запутанность законов, как обычно, компенсируется необязательностью их исполнения, и Россия на сегодня – рай для пиратов от картографии. Законопослушным компаниям в такой ситуации работать крайне сложно. Пользователи предпочитают приобретать именно те приборы и программное обеспечение, которое позволяет им использовать пиратское обеспечение.

Потребность в нововведениях сейчас ощущают все участники процесса грузоперевозки, не только транспортные компании [3]. В мониторинге своих машин нуждаются заводы, с/х предприятия, строительные компании и в организации общественного транспорта. Также ощущается потребность в мониторинге речных и морских судов, паромов и яхт.

Но, несмотря на преимущества данной системы, существует ряд проблем. Одной из таких проблем можно назвать недолговечность работы основы этой системы, а именно, это GPS-навигатора. По причине того, что производители навигационных приборов стараются снизить цену на свою продукцию за счет использования материалов низкого качества и происходит быстрый выход таких приборов из строя.

Также одной из составляющих GPS-навигации является программное обеспечение. Программное обеспечение для навигатора является, по сути, интерфейсом систем спутниковой навигации. И здесь возникают свои проблемы. В частности, дешевые экземпляры данных устройств не позволяют в полной мере использовать все преимущества, предоставляемые данной технологией.

СПИСОК ЛИТЕРАТУРЫ

1. Брусакова И.А., Власов М.П., Соколов Р.В., Голоскоков К.П., Цветков Э.И., Андреевский И.Л. Управление корпоративными ресурсами в информационных системах. Монография /Федеральное агентство по образованию. Санкт-Петербург, 2010
2. Гаскаров Д.В., Голоскоков К.П., Шкабардня А.В. Применение математического программирования в дискриминантом анализе для решения задачи прогнозирования. Автоматика и телемеханика. 1988. № 7. С. 174-181.
3. Власов М.П., Голоскоков К.П., Панова Е.Н. Оценка экономической эффективности нововведений //Экономическое возрождение России. 2011. № 4 (30). С. 25-38.

УДК 004.413

К ВОПРОСУ О ЯДЕРНОЙ И РАДИАЦИОННОЙ БЕЗОПАСНОСТИ НА ТРАНСПОРТЕ

Грудина Эвелина Владимировна, Шапаренко Никита Витальевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: evelina.grudina.80@gmail.com, nikita4shap@gmail.com

Аннотация. Рассматриваются вопросы ядерной и радиационной безопасности, возможные угрозы от неё на транспорте, исторические разработки в области атомной энергетики, их безопасность и эффективность, а также полный цикл разработки нового умного дозиметра.

Ключевые слова: дозиметр, радиометр, счётчик Гейгера, ядерная энергетика, атомная энергетика, радиационная безопасность, ядерная безопасность, МАГАТЭ.

ABOUT NUCLEAR AND RADIATION SAFETY ON TRANSPORT

Grudina Evelina, Shaparenko Nikita
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: evelina.grudina.80@gmail.com, nikita4shap@gmail.com

Abstract. The article discusses the issues of nuclear and radiation safety, possible threats from it in transport., historical developments in the field of nuclear power, their safety and efficiency, as well as the full development cycle of a new smart dosimeter.

Keywords: dosimeter, radiometer, Geiger counter, nuclear power, nuclear power, radiation safety, nuclear safety, IAEA.

Введение. Открытие мирного атома – это величайшее достижение человечества, а ядерная энергетика последние несколько десятилетий остается одним из самых перспективных видов получения энергии в мире. Атомные электростанции неотделимы от углеродной энергетики: они генерируют огромное количество энергии при меньших затратах исходного материала по сравнению с традиционной энергетикой и оказывают меньшее негативное воздействие на окружающую среду [1]. Строительство АЭС вместо ТЭС позволяет снижать уровень выделяемого углекислого газа в атмосферу, а сами АЭС обладают высокой энергоёмкостью, возможностью повторного использования сырья, а также снижают парниковый эффект и обеспечивают интенсивное развитие экономики [2]. В нормально функционирующей АЭС выделяется меньше радиации в окружающую среду, чем в любой ТЭС (за счёт выделения золы, в составе которой присутствует уран, который изначально содержится в угле). Однако в истории развития атомной энергетики было много чёрных страниц [3-11].

Авария на Чернобыльской АЭС. Катастрофа на 4-ом энергоблоке Чернобыльской Атомной Электростанции произошла 26 апреля 1986-го года в 1:23:45 ночи, в ходе проведения проектного испытания турбогенератора № 8 на энергоблоке № 4. Произошёл гидротермический взрыв, который полностью разрушил реактор, крышу энергоблока и большую часть здания энергоблока. В атмосферу было выброшено примерно 380 миллионов кюри радиоактивных веществ, в том числе изотопов урана, плутония, иода-131, цезия-134, цезия-137, стронция-90 [1, 5].

Авария на АЭС Фукусима – 1. Произошла 11 марта 2011 года в результате землетрясения и последующего за ним удара цунами, которые привели к полному обесточиванию станции, а следовательно и к отказу резервных источников электроснабжения, что явилось причиной неработоспособности всех систем нормального и аварийного охлаждения и привело к расплавлению активной зоны реакторов на энергоблоках 1—3 и взрывам водорода на энергоблоках 1, 3 и 4 [6].

Авария на ЛАЭС. 30 ноября 1975 года на энергоблоке № 1 Ленинградской АЭС произошла авария с разрушением (расплавлением) топливного канала, приведшая к радиоактивным выбросам (1,5 млн Кюри активности). Эту аварию, высветившую конструктивные недостатки реактора РБМК, специалисты считают предтечей катастрофы в Чернобыле [7-9].

Обоснование актуальности исследования. Радиация опасна в виду нескольких причин:

Её невозможно обнаружить, не располагая специальными дозиметрами или трубками Мюллера-Гейгера пока радиационный фон не превышает запредельные значения.

Так как радиация неосязаема, то расчёт дозы, которую может получить человек при облучении производится уже после обнаружения самой опасности путём серьёзного анализа всех произошедших событий за долгий период времени, связанных с радиоактивным компонентом и действиями пострадавших.

Что нового мы предлагаем в собственном дозиметре?

Мы предлагаем надёжный дозиметр\радиометр, который возможно интегрировать в автоматизированную среду, а также удаленно контролировать и использовать как статично, так и мобильно. В случае статичного использования, он представляет собой датчик, который можно интегрировать в системы автоматизации (например, SCADA системы) как с подключением проводов, так и беспроводным путём. Возможно подключить дозиметр к сетям Интернета Вещей, параллельно многим другим датчикам, например, в сеть LoRaWAN, чтобы радио дозиметрический контроль был автоматизирован. Также, благодаря унификации интерфейсов и использованию стандартных протоколов можно использовать изобретение в профессиональных системах, к примеру, AdAstra Trace Mode без

каких-либо доработок: дозиметр поддерживает протокол Modbus поверх RS-232 и RS-485, что допускает удобное промышленное использование. Может использоваться группами дозиметрического контроля на местности, а данные о радиационном фоне могут, как передаваться автоматически, так и вручную при обнаружении сети.

Предполагается интегрировать интерфейсы связей: Bluetooth, Wi-Fi, Аналоговая передача на частоте 433 мгц, LoRaWAN (868 мгц), RS-232, RS-485, IR, GSM/2G GPRS, USB. Интерфейсы могут использоваться как одновременно, так и по надобности (по обращению к дозиметру извне).

Цели и задачи работ. Целями работы является анализ состояния радиационной безопасности на транспорте, а также разработка инновационного дозиметра, который имеет возможность интеграции в автоматизированные системы управления технологическими процессами, удалённой передачи данных о радиационном фоне в исследуемой зоне.

Задачи работы:

Исследование радиационной обстановки в мире и регионе, в частности, опираясь на открытые источники в сети Internet.

Теоретическая разработка принципиальной электрической схемы умного дозиметра

Практическая разработка печатной платы (изготовление заготовки, обработка её, трассировка, сверление, монтаж компонентов, испытания и контроль)

Разработка встроенного программного обеспечения

Технологические испытания готового устройства

Описание методов и методик, применённых авторами.

В основе нашей работы лежат мировые исследования МАГАТЭ и советско-российской атомной энергетики. Проектируя наш дозиметр, мы опирались на электрические схемы дозиметров, основанные на распространённых бытовых счётчиках Гейгера – такие как СТС-5, СБМ-20, СБМ-21. В свою очередь, автоматизация строилась на готовых решениях и сертифицированных микросхемах и микроконтроллерах различных интерфейсов, что гарантирует их совместимость с реальными системами автоматизации.

Приведение результатов исследования. В качестве конечных результатов исследования планируется производство печатной платы дозиметра, программирование и прошивка микроконтроллеров – центрального процессора и со-процессора, а также опытные испытания дозиметра – измерение радиационного фона здания корпуса ФГБОУ ВО «ГУМРФ им. Адмирала Макарова» (Учебный городок – 7), расположенного по адресу: г. Санкт-Петербург, улица Двинская, 5/7.

Заключение. В ходе работы мы изучили тему ядерной безопасности, проанализировали её с точки зрения обеспечения безопасности транспорта, изобрели инновационный дозиметр и запускаем производство опытного экземпляра для практического тестирования в рамках учебного города нашего университета.

СПИСОК ЛИТЕРАТУРЫ

1. Ядерной науке и технике России 50 лет: Сб. докладов юбилейной конференции. 29–30 августа 1995 г. М.: Минатом, 1996.
2. История советского атомного проекта: Труды международного симпозиума ИСАП-96. М.: ИздАТ, 1999.
3. https://www.rusatom-overseas.com/ru/integrated-offer/energy-solution/ (дата обращения: 06.09.2020).
4. Официальный сайт компании «Русатом Оверсиз» - компании госкорпорации Росатом, ответственной за продвижение проектов АЭС и ЦЯНТ // [Электронный ресурс]: Раздел «Энергетические решения».
5. Официальный сайт электронного музея истории Мосэнерго : [Электронный ресурс] : ВВЭР – 1000, история и перспектива развития атомной энергетикию
6. http://elib.biblioatom.ru/text/byulleten-atomnoy-energii_2006_v4/go,54/ (дата обращения 06.09.2020).
7. http://www.mosenergo-museum.ru/Museum/Cooperation/materialy-nashikh-chitateley/material/reaktor-vver.php (дата обращения 06.09.2020).
8. Борис Горбачёв – [Электронный ресурс] : Статья в периодическом издании, «В чём она, главная причина Чернобыльской Аварии?» - Электронная библиотека Росатома, история Росатома, периодическое издание «Бюллетень по атомной энергии. — 2006. — № 4», стр. 54.
9. http://nuclphys.sinp.msu.ru/mrrs/mrrsa/ (дата обращения – 06.09.2020).
10. Проект кафедры общей ядерной физики физического факультета МГУ (при поддержке НИИЯФ МГУ) – [Электронный ресурс] : Р.В. Арутюнян, Л.А. Большов, И.И. Линге, Е.М. Мелихова, С.В. Панченко – «Уроки Чернобыля и Фукусимы и актуальные проблемы совершенствования системы защиты населения и территорий при авариях на АЭС» - журнал «Медицинская радиология и радиационная безопасность» 2016. Том 61. № 3.
11. Международное агентство по атомной энергии – Серия изданий по безопасности №. 75-INSAG-7. Чернобыльская авария: дополнение к INSAG-1. Доклад Международной консультативной группы по ядерной безопасности INSAG-7. [Электронный ресурс] :https://www-pub.iaea.org/MTCD/publications/PDF/Pub913r_web.pdf (дата обращения - 06.09.2020).

УДК 004.05

О ПРИМЕНЕНИИ ЦИФРОВЫХ СЕРТИФИКАТОВ КАК СРЕДСТВА АУТЕНТИФИКАЦИИ В ТРАНСПОРТНО-ЛОГИСТИЧЕСКИХ КОМПАНИЯХ

Ерисова Анастасия Дмитриевна, Ныркov Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: xoytlo@ya.ru, apnyrkow@mail.ru

Аннотация. Рассмотрен метод аутентификации с использованием цифровых сертификатов, его преимущества, недостатки, возможности применения на транспорте, в том числе в морских компаниях.

Ключевые слова: методы аутентификации; цифровые сертификаты; безопасность информации.

ON THE APPLICATION OF DIGITAL CERTIFICATES AS A MEANS OF AUTHENTICATION IN TRANSPORTATION AND LOGISTICS COMPANIES

Erisova Anastasiya, Nyrkov Anatoliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: xoytlo@ya.ru, apnyrkow@mail.ru

Abstract. An authentication method using digital certificates is considered, its advantages, disadvantages, and possible applications in transport, including in maritime companies.

Keywords: authentication methods; digital certificates; information security.

Увеличение объемов потерь: финансовых, материальных, имиджевых и др. - при передаче и обработке информации в компаниях и организациях разного уровня и принадлежности в значительной степени связаны с неправомерным доступом к информации. Различные аспекты безопасного и правомерного получения доступа рассматривались авторами в работах [1, 2], с применением биометрических методов [3, 4], электронной цифровой подписи [5 – 7], логин+пароль [1, 8]. Сегодня существуют и развиваются методы, которые считаются наиболее актуальными в сфере проверки прав пользователей, и постепенно вводятся в работу в большинстве компаний. Рассмотрим подробнее метод аутентификации при помощи цифровых сертификатов, который на данный момент считается одним из самых безопасных и универсальных.

О цифровых сертификатах стало известно в 1976 году, но активное использование началось только в последние годы. Даже сейчас организации используют аутентификацию при помощи ввода логина и пароля. Хотя по активному внедрению SSL-протокола в интернете становится понятно, что цифровые сертификаты являются наиболее развитым методом подтверждения прав. Преимуществом использования цифровых сертификатов является не только безопасность. При использовании сертификатов от аккредитованных удостоверяющих центров остается возможность вменения юридической ответственности, так как при этом проверяется и личность пользователя системы, и сервер, на котором будет производиться дальнейшая работа.

Проблемы использования цифровых сертификатов в основном совпадают с проблемами, описанными в [5, 9]. Цифровые сертификаты могут храниться в реестре на жестком диске компьютера или сервера, а соответственно их оттуда можно украсть. Получив доступ к рабочему месту, можно использовать полномочия пользователя. Для решения этой проблемы используются аппаратные носители, на которые, в свою очередь, ставится надежный PIN-код, таким образом, образуется система двухфакторной аутентификации.

Цифровой сертификат (сертификат открытого ключа) - это электронный документ, который использует цифровую подпись для связывания открытого ключа с удостоверением личности.

Основной задачей цифровых сертификатов является обеспечение безопасности информационных потоков, проходящих как внутри организации, так и извне. Так как сертификат гарантирует подлинность и целостность информации, получатель будет точно знать, что информация достоверна и пришла от доверенного источника.

Достоверность информации подтверждается сертификационным центром, который выдает сертификат. На различных уровнях применения сертификатов, надежность будет разная. Такую систему можно организовать внутри организации, тогда надежность будет характеризоваться защитой самой организации, ее серверов, и ответственность все равно будет определяться внутри организации. А может быть организована выдача сертификатов от аккредитованных центров, тогда каждый сертификат будет иметь юридическую силу.

В любом случае, основным фактором является определение пользователя или системы, использующих сертификат, как на уровне внутренних распорядков организации, так и юридически. Сертификат может быть выдан как пользователю, так и любому объекту (рабочей станции, серверу и т. д.). Стандартный формат сертификатов, использующийся в большинстве систем это - X.509. Он описывает сведения, которые должен содержать сертификат. Это – информация о сертификате, о центре сертификации, о субъекте, владеющем сертификатом. В сертификат включается информация, связывающая его открытый ключ с пользователем, рабочей станцией, сервером или службой, у которых находится парный закрытый ключ. Сертификат подписывается центром сертификации и таким образом подтверждается его подлинность. Все выданные сертификаты хранятся в базе центра, в которой учитываются действующие и отозванные. При проверке система подтверждает действие сертификата или отказывает в доступе, так как сертификат является недействительным.

Аутентификацию с использованием сертификатов поддерживают несколько протоколов, наиболее распространенный протокол SSL (используется в веб-браузерах), также применяются протоколы Transport Layer Security (TLS), Internet Key Exchange (IKE), S/MIME, PGP и Open PGP.

Рассмотрим преимущества использования цифровых сертификатов:

– Если в компании нет необходимости применять ЭП, то использование цифровых сертификатов обеспечит авторизацию пользователей в системе, авторизацию сервера или приложения, при этом такую систему можно развернуть, не получая дополнительных затрат, существуют бесплатные аналоги подобных систем. Также можно развернуть собственный центр сертификации на сервере. А носителем сертификата может являться обычная флэш-карта.
– Надежность передачи информации (целостность, конфиденциальность).
– Аутентификация (доступ к серверу, приложениям, интернет-ресурсам, почте, финансам).
– Удаленная работа через VPN.
– Возможность юридической ответственности.

К недостаткам использования цифровых сертификатов можно отнести:

– Сложность настройки (при неправильной настройке будет организовано обычное незащищенное соединение).
– Совместимость (не все субъекты корректно работают с цифровыми сертификатами).
– При утрате сертификата возможна подмена сертификатов через сервер-злоумышленника.
– Основой корректной работы является защита секретного ключа, который в большинстве случаев хранится в реестре на жестком диске компьютера, что не обеспечивает его полную защиту.

Сравнивая парольную защиту и защиту при использовании цифровых сертификатов, становится понятно, что последний метод надежнее, он увеличивает сложность получения доступа к информации в системе, таким образом, укрепляя защиту. Данный метод помимо увеличения сложности позволяет определить пользователя, систему, объект, который имеет цифровой сертификат, что позволяет четко разграничить доступ и определить, кем и какие действия были произведены. Несмотря на то, что из-за сложности настройки цифровых сертификатов, такой метод аутентификации не является популярным, он продолжает развиваться, находятся новые направления применения данного метода, в частности, на морском транспорте [10, 11]. В будущем, когда приложения будут более доступны для работы с сертификатами, а настройка упроститься, этот метод наберет популярность среди специалистов по защите информации.

СПИСОК ЛИТЕРАТУРЫ

1. Нырков А.П. Основные принципы построения защищенных информационных систем автоматизированного управления транспортно–логистическим комплексом / А. П. Нырков, Ю. Ф. Каторин, С. С. Соколов, В. Н. Ежгуров // Проблемы информационной безопасности. Компьютерные системы. – № 2, 2013. – С. 54 – 58.
2. Ерисова А.Д. История и методы аутентификации // Материалы конференции «Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». – СПб.: СПОИСУ, 2016. – С. 159–160.
3. Boriev Z. Software and hardware user authentication methods in the information and control systems based on biometrics / Z. Boriev, A. Nyrkov, S. Sokolov, S. Chernyi // IOP Conf. Series: Materials Science and Engineering 124 (1) 2016. – № 012006 https://doi.org/10.1088/1757-899X/124/1/012006.
4. Boriev Z. V. Review of modern biometric user authentication and their development prospects / Z. V. Boriev, S. S. Sokolov, A. P. Nyrkov // IOP Conf. Series: Materials Science and Engineering 91 (2015) 012063, 2015. https://doi.org/10.1088/1757-899X/91/1/012063.
5. Ерисова А.Д., Васильева А.Е. Тенденции использования электронной подписи // Материалы Молодежного научного форума студентов и аспирантов транспортных вузов с международным участием «Актуальные аспекты и приоритетные направления развития транспортной отрасли». – М.: Изд-во «Перо», 2019. – С. 169–172.
6. Нырков А.П. Программный комплекс аутентификации с использованием электронной цифровой подписи / Нырков А.П., Янюшкин К.А. // «Информационные управляющие системы и технологии» (ИУСТ–Одесса–2015). Материалы международной научно-практической конференции, 22 – 24 сентября 2015 г. – Одесса, 2015. – С. 151–153.
7. Гаскаров В.Д. Структура программного обеспечения для аутентификации с использованием электронной цифровой подписи / В. Д. Гаскаров, А. П. Нырков, А. А. Нырков // Сборник тезисов докладов национальной ежегодной научно-практической конференции профессорско-преподавательского состава ГУМРФ имени адмирала С. О. Макарова. — СПб: Изд-во ГУМРФ им. адм. С.О. Макарова, 2017. – С. 25–26.
8. Kovalnogova, N.M. Model of user identification of electronic informational-educational environment / N. M. Kovalnogova, S. S. Sokolov, A. P. Nyrkov // IOP Conf. Series: Materials Science and Engineering 124(1) 2016. – № 012066 https://doi.org/10.1088/1757-899X/124/1/012066
9. Nyrkov A., Goloskokov K., Koroleva E., Sokolov S., Zhilenkov A., Chernyi S. Mathematical Models for Solving Problems of Reliability Maritime System. In: Advances in Systems, Control and Automation. Lecture Notes in Electrical Engineering, vol 442, 2018. – Pp. 387-394. https://doi.org/10.1007/978-981-10-4762-6_37.
10. S. G. Chernyi, V. E. Marley, S. S. Lopyrev, A. A. Bulov and A. S. Bordug, "Systems of identification authentication and encoding in maritime industry,"2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 37-39, doi: 10.1109/EIConRus.2018.8317023.
11. Kardakova M. Cyber Security on Sea Transport / M. Kardakova, I. Shipunov, A. Nyrkov, T. Knysh // Advances in Intelligent Systems and Computing, Vol. 982. – 2020. – Pp. 481–490. https://doi.org/10.1007/978-3-030-19756-8_46

УДК 004.3

О ВОЗМОЖНОСТЯХ ПРИМЕНЕНИЯ ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ КОНТРОЛЛЕРОВ ДЛЯ ЦЕЛЕЙ МОНИТОРИНГА СОСТОЯНИЯ СУДОВОГО ОБОРУДОВАНИЯ

Зубанова Анастасия Александровна, Шипунов Илья Сергеевич, Нырков Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: mr-shis@yandex.ru, kaf.koib@gmail.com

Аннотация. Рассматриваются возможности применения программируемых логических контроллеров для целей мониторинга состояния судового оборудования. Приводятся проблемы, которые можно решить с помощью контроллера.

Ключевые слова: современное судоходство, судовое оборудование, системы мониторинга, программируемые логические контроллеры.

ON THE POSSIBILITIES OF USING PROGRAMMABLE LOGIC CONTROLLERS FOR MONITORING THE STATE OF SHIPBOARD EQUIPMENT

Zubanova Anastasia, Shipunov Ilya, Nyrkov Anatoly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: mr-shis@yandex.ru, kaf.koib@gmail.com

Abstract. The possibilities of application of programmable logic controllers for the purpose of ship equipment condition monitoring are considered. The problems that can be solved with the help of the controller are given.

Keywords: modern shipping, shipboard equipment, monitoring systems, programmable logic controllers.

Диагностика работающих машин и механизмов – это естественное развитие технологий контроля протекающих в них процессов, без которого невозможна безаварийная эксплуатация технических систем. Технологии диагностики, как и контроля, развиваются по двум постепенно сближающимся направлениям, первое из которых нацелено на развитие автоматических систем безопасного управления контролируемыми объектами, а второе – на совершенствование процессов обслуживания и ремонта [1].

Первое направление диагностики ориентировано, в основном, на измерение и анализ протекающих в объектах рабочих процессов, причем глубина анализа ограничена высокими требованиями к скорости принятия решений, используемых в системах автоматического управления машинами и оборудованием. Соответственно, эти решения должны приниматься за доли секунды и без участия человека.

К превентивной (глубокой) диагностике, используемой для планирования работ по обслуживанию и ремонту, предъявляются другие требования, как по скорости принятия решений, так по глубине диагностирования и по участию экспертов в постановке диагноза и прогноза. Назначение глубокой диагностики – долгосрочный прогноз безотказной работы машин и оборудования, который возможен только при отсутствии в них дефектов, имеющих высокую скорость развития. Поэтому основной задачей такой диагностики является идентификация всех типовых дефектов на стадии зарождения и мониторинг развития каждого из них с прогнозом остаточного ресурса [2]. А дополнительной задачей является общий мониторинг состояния объектов диагностики, который исключает пропуск опасных дефектов, не относящихся к типовым и обычно являющихся результатом ошибок управления объектами диагностики.

Как правило, глубокая диагностика проводится по вторичным процессам, протекающим в машинах и оборудовании, с применением средств измерения без встраивания датчиков в объект диагностики. Возможно использование и штатных датчиков рабочих процессов, если есть доступ к снимаемым с них сигналам, а их характеристики обеспечивают получение необходимой диагностической информации. Достаточно часто измерения для глубокой диагностики выполняются переносными (портативными) средствами измерения. В диагностике машин и механизмов с узлами вращения чаще всего используются средства измерения и анализа вибрации, тока в силовых цепях электрических машин, а также средства контроля температуры и состава смазки. Время для принятия решения в глубокой диагностике ограничено лишь типовым интервалом между диагностическими измерениями, которого даже при наличии развитого дефекта достаточно для анализа всей имеющейся информации удаленным экспертом, включая проведение дополнительных измерений, необходимых для уточнения диагноза.

Ключевым моментом в сближении двух направлений диагностики является реальная потребность устанавливать на наиболее ответственные агрегаты стационарные системы общего мониторинга состояния для решения проблем предупреждения аварийных ситуаций, возникающих из-за ошибок управления, без преждевременной остановки агрегата. Время, отводимое на принятие решений в таких системах, в несколько раз больше, чем в системах аварийной защиты, что позволяет дополнить ее многими алгоритмами глубокой диагностики, многократно увеличивая объем используемой диагностической информации и формируя оперативный диагноз, включая краткосрочный прогноз и рекомендации обслуживающему персоналу, в режиме он-лайн.

Применение логических контроллеров возможно на судне для повышения безопасности таких элементов, как двигатель внутреннего сгорания, воздушный компрессор, пожарный насос, система охлаждения, трансформаторы, генераторы и другие [3]. Областями повышения безопасности были изначально выбраны температурные режимы, поскольку выход из температурного режима каждого вида вышеперечисленного оборудования может привести к пожру на судне, который в свою очередь может привести к человеческим жертвам.

Рассмотрим проблемы судового оборудования, перечисленного выше.

Начнем с воздушного компрессора.

Данный тип судового оборудования может столкнуться со следующими проблемами:

1. Низкая мощность компрессора. Основными причинами этой проблемы являются:
   - Утечка в нагнетательных и всасывающих клапанах
   - Неисправность или утечка в разгрузчике
   - Утечка из предохранительного клапана
   - Неправильная настройка автоматического включения и выключения компрессора (слишком близко)
2. Перенос масла в воздух.
3. Чрезмерная вибрация и шум.
4. Перегрев выпускаемого воздуха. Если температура выпускаемого сжатого воздуха высокая, это может быть связано с перегревом, вызванным следующими причинами:
   - Засоренный или грязный интеркулер
   - Производительность насоса охлаждающей воды уменьшена или недостаточна
   - Атмосфера при всасывании воздуха компрессора горячая
   - Нет принудительной вентиляции для свежего воздуха возле компрессора
   - Повреждение прокладки головки
   - Фильтр всасывания засоренного воздуха
   - Клапаны 1 или 2 ступени протекают

5. Молочное масло в картере.

Далее рассмотрим проблемы, возникающие при работе пожарного насоса.

1. Отказ при доставке - насос не может подать необходимое давление. Причинами могут являться:
- Неправильное заполнение насоса
- Недостаточная скорость работы
- Утечка воздуха
- Повреждение механизма (рабочее колесо/шестерня/винт)
- Не правильное направление движения вала
- Высота всплывания превышает требуемую
- Температура жидкости ниже предела прокачки насоса

2. Отказ при заправке - заправка необходима для запуска большинства насосов.

3. Неспособность создать давление - если насос не может создать достаточное давление для обеспечения плавного потока жидкости.

4. Чрезмерная вибрация.

5. Уменьшенная производительность. Из-за непрерывной работы производительность насоса резко снижается в несколько раз.

6. Перегрузка двигателя. Это очень распространенная проблема с насосами на борту судов.

7. Потеря жидкости. Насос теряет жидкость после запуска или во время работы. Причины:
- Всасывающий лифт не соответствует необходимому
- Утечки в линии всасывания.
- Температура жидкости
- Предохранительный клапан насоса установлен на неправильное значение

Выход пожарного насоса из строя грозит уменьшению вероятности потушить пожар на судне при его возникновении, что может привести к серьезным его последствиям, при которых могут пострадать документы, груз, оборудования и экипаж. Проблемы, которые могут возникнуть при работе судового дизельного двигателя:

1. Неисправность топливного клапана / утечка топлива
2. Утечка воздуха
3. Выход из строя установленных датчиков
4. Неисправные датчики и сигнализации
5. Перегрев

Выход из строя дизельного двигателя грозит серьезными последствиями, такими как: невозможность продолжать маршрут, сбой с курса, а в некоторых случаях и взрыв, влекущий за собой пожар и самые плохие последствия.

Далее рассмотрим проблемы системы охлаждения, использующейся на множестве судов:

1. возможность засорения зарубашечного пространства дизеля илом и другими взвешенными частицами, содержащимися в морской воде;

2. интенсивное отложение солей в зарубашечном пространстве и образование накипи, плохо проводящей тепло и резко ухудшающей теплообмен, в результате чего происходит перегрев деталей и даже их разрушение;

3. нарушение температурного режима в следствии поступления на вход забортной воды с пониженной температурой.

При использовании трансформаторов необходимо периодически контролировать:

1. Напряжение и токовую нагрузку по штатным приборам;
2. Температуру нагрева кожуха;
3. Отсутствие повышенного шума (гудения);
4. Исправность защитных заземлений.

При использовании генераторов необходимо контролировать:

1. Основные параметры генераторов (напряжение, частоту тока, ток, мощность и др.) По штатным щитовым измерительным приборам;
2. Сопротивление изоляции генераторов и судовой сети по штатным приборам на ГРЩ;
3. Работу щеточного аппарата, контактных колец (коллектора);
4. Температуру нагрева генераторов;
5. Работу подшипников, их температуру нагрева, подачу и давление масла в подшипниках с принудительной смазкой;
6. Отсутствие постороннего шума и вибрации;
7. Действие средств АПС (сигнальных ламп, световых табло, звуковых сигналов);
8. Температуру воздуха в помещении;
9. Состояние воздушных фильтров;
10. Исправность защитных заземлений.

Поломки генераторов грозят обесточиванием всего корабля, что в свою очередь может привести к временному выходу из строя систем навигации, систем жизнеобеспечения, контроля за работой судового оборудования, да и к общему отключение судового оборудования [4].

Итак, рассмотрев проблемы судового оборудования и причины их возникновения, можно прийти к выводу, что множество проблем может возникать из-за физических неполадок (износа), но не малая часть проблем также может

возникать из-за превышения или понижения допустимых температур. Именно такие проблемы можно контролировать с помощью программируемого логического контроллера.

С помощью ПЛК можно проводить мониторинг температур жидкостей в оборудовании, состояния систем, а также непосредственно управлять работой рассмотренного в данной работе судового оборудования [5].

Остановимся на некоторых проблемах судового оборудования, которые можно решить с помощью ПЛК. К таким проблемам относятся:

1. У воздушного компрессора – перегрев выпускаемого воздуха
2. У пожарного насоса – отказ при доставке
3. У судового дизельного двигателя – перегрев
4. У системы охлаждения – нарушение температурного режима
5. У трансформаторов – температура нагрева кожуха
6. У генераторов – температура нагрева генераторов и воздуха в помещении.

Использование ПЛК для мониторинга состояния также возможно при этих проблемах, однако при правильной разработке программного комплекса, мониторинг и устранение проблем можно объединить в одной программе.

ПЛК также можно использовать для устранения других проблем, возникающих при работе судового оборудования, это возможно осуществить подсоединением к ПЛК необходимых датчиков, способных передавать требуемые параметры для оценки состояния судового оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. “The Safety Assessment of Critical Infrastructure Control System” 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 5 November 2018, pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948
2. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “About the Problems of Ensuring Information Security on Unmanned Ships” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 339-343. https://doi.org/10.1109/EIConRus.2019.8657219
3. S. Shipunov, A. P. Nyrkov, M. V. Kardakova, Y. F. Katorin and V. V. Vychuzhanin, "Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 497-500, doi: 10.1109/EIConRus49466.2020.9039181.
4. Kardakova, M., Shipunov, I., Nyrkov, A., Knysh, T. “Cyber Security on Sea Transport” Advances in Intelligent Systems and Computing, vol. 982, (2020), pp.481-490. https://doi.org/10.1007/978-3-030-19756-8_46
5. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “Trusted transport telemetry by using distributed databases” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 344-347. https://doi.org/10.1109/EIConRus. 2019.8657215

УДК 004.05

О ПРАВОВОМ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ ТРАНСПОРТА

Кириков Антон Викторович, Ныркov Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: kav@niti.ru, apnyrkow@mail.ru

Аннотация. Рассмотрены проблемные вопросы, возникающих при проведении категорирования объектов критической информационной инфраструктуры на транспорте, в том числе в морских компаниях, в соответствии с ФЗ-187.

Ключевые слова: безопасность информации, менеджмент безопасности, критическая информационная инфраструктура, транспортные объекты.

ON THE LEGAL SUPPORT OF INFORMATION SECURITY AT TRANSPORT FACILITIES

Kirikov Anton, Nyrkov Anatoliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: kav@niti.ru, apnyrkow@mail.ru

Abstract. The problematic issues arising during the categorization of objects of critical information infrastructure in transport, including in maritime companies, in accordance with FL-187 are considered.

Keywords: information security, security management, critical information infrastructure, transport facilities.

Говоря об обеспечении информационной безопасности на объектах транспорта, необходимо, прежде всего, обратить внимание на изменения в подходах, связанные с нормативным закреплением в Российской Федерации такого понятия, как «критическая информационная инфраструктура».

В соответствии с ФЗ-149 "Об информации, информационных технологиях и о защите информации", информация – это сведения (сообщения, данные) независимо от формы их представления [1]. Этим же нормативным актом определяются основные категории защиты (свойства) информации – конфиденциальность, целостность, доступность.

Другими, равновесными с ФЗ-149 с юридической точки зрения, нормативными актами (кроме Постановления Правительства РФ от 3 ноября 1994 г. N 1233) являются нормативные акты, законодательно описывающие и закрепляющие принципы защиты конкретных видов информации ограниченного распространения, а именно:

- Закон РФ № 5485-1 от 21.07.1993 года «О государственной тайне» [2];
- Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне"[3];
- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"[4];

Постановление Правительства РФ от 3 ноября 1994 г. N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности".

При этом необходимо отметить, что вышеуказанные нормативные акты, с точки зрения информационной безопасности концентрируют внимание на защите основного свойства информации – конфиденциальности, в пику актуальности защиты таких же неотделимо важных свойств информации, как целостность и доступность.

Применительно к объектам транспортной инфраструктуры данный подход носил локальный характер, так как число автоматизированных систем, обрабатывающих сведения ограниченного распространения (за исключением обработки персональных данных пассажиров) в данной сфере было невелико.

Такие важнейшие системы транспортной инфраструктуры, как системы управления водным, наземным, воздушным и железнодорожным транспортом в принципе не подпадали под действие данных законодательных актов, а говорить об их защищенности можно было весьма приблизительно.

Стоит отметить, что все попытки приведения в соответствие данных систем реализовывались в рамках ведомственных подходов и не носили взаимоувязанной по цели задачи обеспечения безопасности информации в рамках государства, а главное, не давали возможности осуществлять финансирование данных задач на полностью законных основаниях.

Для понимания и реальной оценки защищенности данных информационных инфраструктур требовался иной законодательный подход, позволяющий владельцам информационных инфраструктур осуществлять финансирование задач обеспечения безопасности информации на полностью законных основаниях.

К тому же, выбрав в качестве объектов защиты именно информацию, все равно оставалась необходимость защиты информационных технологий, посредством которых обрабатывалась данная защищаемая информация. То есть при анализе технологического процесса основное внимание уделялось защите выделенных сегментов информационной (автоматизированной) системы, где именно обрабатывалась (хранилась, передавалась) защищаемая информация, а сегменты, где отсутствовал признак конфиденциальности, почему-то считались не подлежащими защите. При этом эта информация не считалась общедоступной, так как все равно должны были применяться меры по недоступности этих информационной (автоматизированной) системы для внешних воздействий.

С целью реализации требований к таким системам вышел в свет, в частности, документ «Требования к АСУ ТП …» (приказ ФСТЭК России №31 от 14 марта 2014 г.) [5], но практика его применения тоже стала носить ведомственный характер.

Впервые в документе такого уровня появилось понятие «технологическая» информация, подлежащая защите, которая не является общедоступной. Позже появился нормативный акт - Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", вступивший в действие с 01.01.2018 года, который существенным образом изменил подход к обеспечению информационной безопасности объектов транспортной инфраструктуры [1].

Положения ФЗ-187 ставят во главу угла обеспечение защиты не только конфиденциальности информации, но также и ее целостности и доступности, так как компьютерные атаки, включая деструктивное воздействие компьютерных вирусов, нацелены в основном на воздействие именно по линии целостности и доступности информации, что при условии проведения успешной компьютерной атаки, фактически делает бессмысленным защиту конфиденциальности информации, но вносит необходимость защиты именно «технологической» информации объектов критической информационной инфраструктуры.

При этом, в некоторых случаях, к данным объектам могут относиться объекты критической информационной инфраструктуры, обрабатывающие общедоступную информацию. Из этого следует, прежде всего, то, что защите должна подлежать не только информация ограниченного распространения, технологическая информация, но и общедоступная.

В 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", главным критерием считается ущерб, который может быть нанесен собственнику при утрате той или иной информации, также и устанавливает сферы деятельности в РФ, в которых осуществляют свою деятельность объекты критической информационной инфраструктуры. К одной из таких сфер деятельности отнесена сфера транспорта (п.8 ст. 2 ФЗ-187) [1].

Уже имеющаяся статистика по категорированию объектов критической информационной инфраструктуры и вводу в действие систем защиты информации данных объектов показывает, что из заявленных для внесения в реестр ФСТЭК России, как объекты КИИ, принято 80 % заявленных объектов, отклонено 20%. Из общего числа объектов КИИ, находящихся в реестре ФСТЭК России, на долю объектов транспорта приходится 2%. [6, 7]

Вопросы категорирования объектов КИИ являются очень сложными и требующими наличия квалифицированных экспертов, входящих в состав постоянно действующих комиссий по категорированию КИИ в области информационной безопасности.

Объективной причиной этого является новизна предмета, во многом размытость и неопределенность критериев категорирования, установленных подзаконным актом - постановлением Правительства РФ от 8 февраля 2018 г. N 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений".

Но существуют и субъективные причины при определении категорий объектов КИИ, которые можно уже выделить в отдельные группы;

– сознательное занижение значимости объектов КИИ;

– попытка игнорирования сроков реализации 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации";

– сокрытие объектов КИИ;

– привлечение к категорированию сторонних организаций.

Какими представляются пути повышения защищенности информационных систем на объектах транспорта:

1. Окончание категорирования уже имеющихся информационных систем и обеспечение непрерывности и обязательности категорирования вновь создаваемых ИС.

2. Принятие локальных нормативных актов на уровне Министерства транспорта РФ (несмотря на то, что ФЗ-187 является законом прямого действия), что позволило бы контролировать действия руководителей субъектов КИИ – предприятий транспортной инфраструктуры.

3. Критическое осмысление уже полученных результатов категорирования объектов КИИ – то есть уменьшение неопределенности. Решение данного вопроса потребует разработки методик, отдельные примеры уже находят отражение в научных изданиях.

4. В том случае, когда ИС АСУ ТП является важной (значимой) для предприятия транспорта, но присвоить ей категорию значимости не представляется возможным, в обязательном порядке осуществлять ее защиту по требованиям Приказа ФСТЭК России от 14 марта 2014 г. N 31 г. [5] (что коррелируется с п.2).

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Система ГАРАНТ: интернет портал правовой информации. – М., 1998–2019. URL: http://ivo.garant.ru/#/document/12148555 (дата обращения: 23.04.2019).
2. Закон Российской Федерации от 21 июля 1993 г. № 5485-I «О государственной тайне» [Электронный ресурс] // Система ГАРАНТ: интернет портал правовой информации. М., 1998-2015. URL: http://ivo.garant.ru/document?id=10002673&byPara=1&sub=51952 (дата обращения: 23.04.2019).
3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [Электронный ресурс] // Система ГАРАНТ: интернет портал правовой информации. – М., 1998–2015. URL: http://ivo.garant.ru/#/document/12136454 (дата обращения: 23.04.2019).
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс] // Система ГАРАНТ: интернет портал правовой информации. М., 1998–2015. URL: http://ivo.garant.ru/#/document/12148567 (дата обращения: 23.04.2019).
5. Приказ ФСТЭК России от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 23.04.2019).
6. Ныркov А.П. К вопросу о категорировании объектов критической информационной инфраструктуры водного транспорта / А. П. Ныркov, Р. И. Кислов, А. В. Белов // Материалы конференции «XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018. - СПб.: СПОИСУ, 2018. – С. 316–318.
7. Наташова К.В. К вопросу о категорировании объектов критической информационной инфраструктуры морских портов / К. В. Наташова, С. С. Соколов, О. Н. Губернаторов, А. П. Ныркov, А. В. Кириков // Безопасность информационных технологий. – Т. 27. №2. – 2020. – С. 35–46. http://dx.doi.org/10.26583/bit.2020.2.03

УДК 004.056

ИДЕНТИФИКАЦИЯ СУБЪЕКТА И МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Костенкова Анастасия Владимировна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: anvlkostenkova@gmail.com

Аннотация. В данной работе были рассмотрены основные факторы идентификации при использовании многофакторной аутентификации субъекта, а также показана необходимость использования более комплексного уровня аутентификации. В настоящее время защита информации является одним из основополагающих принципов современного мира, построенного на взаимосвязи множества информационных систем из разных сфер жизни. На различных сервисах происходит онлайн-оплата, общение, управление [1], изменение различных данных, и именно поэтому требуется все больше уделять внимание аутентификации пользователей.

Ключевые слова: аутентификация; многофакторная аутентификация; биометрия; доверенные устройства; идентификация.

SUBJECT IDENTIFICATION AND MULTI-FACTOR AUTHENTICATION

Kostenkova Anastasia
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: anvlkostenkova@gmail.com

Abstract. This paper examines the main identification factors of using multi-factor authentication of the subject and shows the need for a more comprehensive authentication level. Currently, information protection is one of the fundamental principles of the modern world, built on the interconnection of many information systems from different spheres of life. Online payment, communication, management [1], and various data changes occur on various services, which is why we need to pay more and more attention to user authentication.

Keywords: authentication; multi-factor authentication; biometrics; trusted devices; identification.

Введение. Многофакторная аутентификация позволяет эффективно поднять уровень защищенности данных, значительно повышая сложность получения доступа к данным злоумышленнику. Многофакторная аутентификация реализуется таким образом, что к привычным пользователю логину и паролю запрашиваются дополнительные данные, позволяющие идентифицировать субъект [1]. Их разделяют на 3 основных категории: факторы на основе знаний, к которым относятся логины, пароли [2], пин-коды, факторы на основе владения собственности: доверенные устройства, на которые отправляется одноразовый код, токены[3] и смарт-карты[4], а так же факторы на основе биометрических данных: отпечатки пальцев, голос и другие [5].

Актуальность. Однофазовая аутентификация на основе знания простейших идентификаторов как логин и пароль является крайне уязвимой [2]. Даже алгоритмически сложный пароль можно узнать, в интернете существуют огромные базы данных, в которых хранятся данные пользователей взломанных сервисов. Именно поэтому рекомендуется внедрять многофакторную аутентификацию, которая значительно повышает уровень защищенности безопасности, так как взлом подобного механизма крайне ресурсозатратен и трудноосуществим для злоумышленника. Многофакторную аутентификацию требуется внедрять во все сферы, так как сейчас это один из наиболее эффективных способов повышение информационной безопасности при авторизации. Это касается не только пользовательских приложений, но и больших инфраструктур. Например, транспортная сфера, использующая «интернет вещей» для сбора и управления всей информацией и системами в одном месте. Подобное решение позволяет значительно проще пользоваться подобной экосистемой, но и значительно повышает риски, в случае несанкционированного доступа [6].

Заключение. В данной работе была рассмотрена актуальность такого решения для защиты информации как многофазовая аутентификация. Оптимальным на данный момент решением будет являться строгая аутентификация, сочетающая в себе запрос логина и пароля, а также использование криптографического токена на основе открытых ключей.

СПИСОК ЛИТЕРАТУРЫ

1. Aleksandr Ometov; Sergey Bezzateev; Niko Mäkitalo; Sergey Andreev; Tommi Mikkonen; Yevgeni Koucheryavy. Multi-Factor Authentication: A Survey. 2018. Доступно онлайн: mdpi.com/2410-387X/2/1/1
2. Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the evolution of imperfect authentication. 2015. Доступно онлайн: jbonneau.com/doc/BHOS15-CACM-imperfect_authentication.pdf
3. Draft NIST Interagency Report 7981, Mobile, PIV, and Authentication. URL: http://csrc.nist.gov/publications/drafts/nistir7981/nistir7981_draft.pdf
4. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices. 2014. Доступно онлайн: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
5. Dasgupta, D.; Roy, A.; Nag, A. Toward the design of adaptive selection strategies for multi-factor authentication. 2016. Доступно онлайн: sciencedirect.com/science/article/pii/S016740481630102X
6. Arti loftus. How industrial IoT will disrupt the shipping industry. 2019. Доступно онлайн: https://www.iotevolutionworld.com/smart-transport/articles/442702-how-industrial-iot-will-disrupt-shipping-industry.htm

УДК 514.18

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ В СОВРЕМЕННОЙ КРИПТОГРАФИИ

Ольшанский Владислав Константинович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: softelele2@mail.ru

Аннотация. В работе рассматриваются вопросы использования криптографии на основе эллиптических кривых, осуществлен сравнительный анализ с другими криптосистемами, основанными на модулярной арифметике. На основе анализа выведены аргументы в пользу использования криптографии на основе эллиптических кривых.

Ключевые слова: эллиптические кривые, криптосистемы модулярной арифметики.

ELLIPTIC CURVES IN MODERN CRYPTOGRAPHY

Olshansky Vladislav
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: softelele2@mail.ru

Abstract. This paper discusses the use of elliptic curve-based cryptography and compares it with other cryptosystems based on modular arithmetic. Based on the analysis, arguments in favor of using elliptic curve-based cryptography are derived.

Keywords: elliptic curves, cryptosystems of modular arithmetic.

Введение. От современных технологий требуется скорость и безопасность при обработки больших объёмов данных. Без нововведений в криптографию не обойтись, она должна идти в шаг вместе с развитием в информационной сферой. Старые методы шифрования находятся под угрозой взлома, ведь с каждым годом вычислительная мощность современных ЭВМ сильнее и сильнее. Основные принципы информационной безопасности [1] должны быть в приоритете и достигаться, путём создания новых криптосистем. В данном направлении была изучена криптография на основы эллиптических кривых (далее - ECC) и проведён сравнительный анализ с текущей используемой криптосистемой RSA.

Актуальность и использование в ИТ. ECC – это раздел криптографии, вида ассиметричной криптосистемы, основанная на эллиптических кривых над конечными полями. Которая на данный момент используется в SSH [2], TLS [3], PGP [4], различных криптовалютах – важнейших технологиях, благодаря которым основано большое количество сервисов и проектов. Конечно, её использование обусловлено многими преимуществами в сравнении с RSA. Если они выполняют одинаковые функции, то ECC более «легкая» криптосистема при этом без потери требуемого уровня защиты данных, что и ставит её на первый план.

Заключение. На основе данных исследований, можно сделать вывод о важности нововведений в криптографию, слабости старых криптосистем и сравнение, актуальной на данный момент, криптосистемы ECC с текущей используемой криптосистемой RSA.

СПИСОК ЛИТЕРАТУРЫ

1. Фаткулин А.Р., д.т.н. Ныркова А.П., Тяпкин Д.А. Основные проблемы в области защиты интернета вещей / ред. В. В. Вычужанин; Одес. нц. политех. ун-т. —Одесса : Экология, 2019. — 340 с.
2. Douglas Stebila Jon Green Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer // 2009 doi: 10.17487/RFC5656 – 20c
3. S. Blake-Wilson, N. Bolyard, Vipul Gupta, C. Hawk, B. Möller Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) // 2018 doi: 10.17487/RFC4492 – 30c.
4. A. Jivs Elliptic Curve Cryptography (ECC) in OpenPGP // 2012 doi: 10.17487/RFC6637 – 15c.

УДК 004.4

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ - ВАЖНАЯ СОСТАВЛЯЮЩАЯ В ВОПРОСАХ БЕЗОПАСНОСТИ МОРСКИХ ПЕРЕВОЗОК

Рябенков Максим Юрьевич
Государственный университет морского и речного флота им. адм. С.О. Макарова
ул. Двинская, д 5/7, Санкт-Петербург, 198035, Россия
e-mails: hatememore33@gmail.com

Аннотация: рассматривается система проведения расследований компьютерных инцидентов на морском транспорте. Приводится возможная схема расследования инцидента с использованием инструментов forensic science.

Ключевые слова: современное судоходство, компьютерный инцидент, forensic science.

INVESTIGATION OF COMPUTER INCIDENTS ARE AN IMPORTANT COMPONENT IN THE SECURITY OF MARITIME TRANSPORTATION

Ryabenkov Maksim
Admiral Makarov state university of maritime and inland shipping
st. 5/7, Dvinskaya St. Petersburg, 198035, Russia
e-mails: hatememore33@gmail.com

Abstract: the possibilities of investigation of computer incidents on modern ships using computer forensics tools. The possible scheme of investigation of computer incidents using computer forensics tools.

Keywords: modern shipping, computer incident, forensic science.

Расследование компьютерных инцидентов информационной безопасности является важнейшей частью обеспечения безопасности морских перевозок. В 2017 году компания Maersk подверглась кибератаке, в результате которой понесла потери в размере 250$ миллионов. В 2018 году одна из крупнейших морских линий China Ocean Shipping Company (COSCO) стала жертвой кибератаки. В 2019 году Береговая охрана США

подтвердила кибератаку с помощью вредоносного ПО. Благодаря расследованию этих атак системы безопасности продолжают эволюционировать и развиваться. Система расследования инцидентов позволяет определить, как была произведена атака, построить алгоритм взлома, восстановить хронологию, а также собрать артефакты. Кроме того, расследование такого рода дает возможность усовершенствовать систему безопасности.

Данная система должна функционировать в паре с системой мониторинга инфраструктуры от несанкционированного доступа. И включает в себя:

Различные средства снятия дампов оперативной памяти и HDD устройства;

Средство анализа дампа памяти;

Средство проведения обратной инженерии для анализа вредоносного ПО;

Средство поиска артефактов в системе, подвергшейся атаке;

Отчет о проведенном расследовании;

Предложение превентивных защитных мер.

Одной из возможных функций такой системы является организация эффективной системы защиты инфраструктуры судна. Система может функционировать в двух режимах: пост-безопасности и внутренних инцидентов. Первый режим предназначен для анализа произведенной атаки, построения хронологии взлома и заражения, а также проверки целостности информации, хранящейся в АИС. Второй – для расследования неправомерных действий членов команды, имеющих доступ к АИС, в том числе, если атака производилась с инсайдером.

Кроме того, второй режим работы системы предполагает регулярный анализ. Дампы снимаются автоматически через определенный промежуток времени и поступают в систему анализа. По результатам отчета система делает вывод о процессе функционирования АИС судна. Отмечает подозрительную активность со стороны системы и пользователей. При необходимости АИС может быть выведена из эксплуатации, когда это возможно, для выполнения мер по обеспечению информационной безопасности [1].

Если АИС судна подверглась заражению, то с данной системы снимается образ оперативной памяти и HDD. Данный образ поступает в систему анализа, которая определяет вектор атаки, что дает возможность своевременно обезопасить инфраструктуру судна. Поиск артефактов атаки позволяет определить виновника и собрать доказательную базу для судебной экспертизы. По результатам анализа специалист предлагает защитные меры, чтобы обезопасить систему от подобных инцидентов в дальнейшем.

Сама по себе система не может защитить АИС от атаки, но она позволяет повысить эффективность ответных мер на инциденты. Своевременное расследование и анализ системы позволит обезопасить целую группу объектов, которые используют схожую АИС и систему безопасности.

Важным преимуществом использование такой системы может быть диагностика системных сбоев и определение несанкционированных источников приема и передачи информации. В дополнение к этому, система позволяет зафиксировать неправомерные действия членов экипажа, даже если они не несут в себе злого умысла для инфраструктуры в целом [2].

Рассмотрим следующий пример. Судно подверглось атаке, и АИС не функционирует в штатном режиме. Система мониторинга зафиксировала этот факт. С устройства, на которое была произведена атака, снимается дамп оперативной памяти. Он поступает в систему расследования инцидентов. В полученном отчете будет представлена информация о затронутых процессах, а также об измененной информации в АИС. На основании полученных данных специалист может принять своевременные решения по обеспечению безопасности судна и экипажа. После восстановления штатного функционирования судна дампы и результаты анализа должны быть переданы в службу безопасности для подробного изучения. Полученные отчеты предоставят информацию о сторонних воздействиях на АИС. Эта информация крайне ценна при поиске субъекта атаки, а также может быть представлена для судебной экспертизы в качестве доказательной базы [3].

Одной из проблем кибербезопасности при использовании системы анализа на судах может стать информация, которая хранится в дампах оперативной памяти. Если злоумышленник получит к ним доступ, то в его ведении окажется уникальная информация о всех устройствах, входящих в состав АИС судна, а также определенный перечень конфиденциальной информации (путевой лист, отгрузочная документация и т.д.).

При создании такой системы необходимо обеспечить высокий уровень безопасности. Система не должна хранить данные о тех дампах, которые не представляют ценность в рамках обеспечения ИБ. В ином случае, дамп должен быть отправлен в службу безопасности по безопасному каналу передачи.

Система расследования компьютерных инцидентов может быть реализована на базе The Volatility Framework – это проект с открытым исходным кодом, написанный на языке программирования Python, является самой широко используемой платформой для криминалистической экспертизы памяти Этот фреймворк позволяет исследовать дампы оперативной памяти с различных операционных систем. Он имеет широкие возможности анализа:

- Анализ процессов;
- Обнаружение API hooks в процессах и памяти ядра;
- Выгрузка процессов для обратной инженерии;
- Создание временных шкал из артефактов в памяти;
- Поиск скрытого и внедренного кода.

Это лишь основной список возможностей данного фреймворка. При более глубоком погружении он открывает широкие возможности анализа оперативной памяти. Система будет использовать алгоритмы из

Volatility и в автоматическом режиме анализировать отчеты. В этом случае на обработку отдельного дампа оперативной памяти уйдет меньше времени, кроме того, автоматический анализ поможет минимизировать человеческий фактор при просмотре отчетов. С ситуациями, где человек не заметил внедренный код или опасный процесс, система автоматического анализа обратит внимание специалистов на них. К преимуществам Volatility так же можно отнести широкий спектр поддерживаемых ОС, а также поддерживаемых форматов памяти.

Для проведения работ по исследованию и сбору цифровых доказательств необходимо придерживаться принципов неизменности, целостности, полноты информации и ее надежности. Поэтому одним из основных этапов расследования компьютерных инцидентов является определение перечня похищенной, модифицированной и удаленной информации. В этом безусловно помогут снятые дампы памяти для определения последовательности действий атакующего и дампы жестких дисков для восстановления утраченных данных. Для защиты системы анализа необходимо обеспечить резервное питание оборудования, а также настроить систему резервного копирования во избежание непреднамеренной утраты данных [4].

Применение такой системы в разы облегчит расследование инцидентов кибербезопасности и автоматизирует процесс сбора цифровых доказательств. Это поможет не только специалистам, но и компаниям, которые заинтересованы в скорости разрешения инцидентов, произошедших в их АИС.

СПИСОК ЛИТЕРАТУРЫ

1. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. “The Safety Assessment of Critical Infrastructure Control System” 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 5 November 2018, pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948
2. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “About the Problems of Ensuring Information Security on Unmanned Ships” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 339-343. https://doi.org/10.1109/EIConRus.2019.8657219
3. S. Shipunov, A. P. Nyrkov, M. V. Kardakova, Y. F. Katorin and V. V. Vychuzhanin, "Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 497-500, doi: 10.1109/EIConRus49466.2020.9039181.
4. Kardakova, M., Shipunov, I., Nyrkov, A., Knysh, T. “Cyber Security on Sea Transport” Advances in Intelligent Systems and Computing, vol. 982, (2020), pp.481-490. https://doi.org/10.1007/978-3-030-19756-8_46

УДК 004.8

СОВРЕМЕННЫЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Рыськина Василиса Игоревна, Белова Мария Александровна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, г. Санкт-Петербург, 198035, Россия
e-mails: vasilisa.rys@mail.ru, m-belova123@mail.ru

Аннотация. Рассмотрены методы биометрической идентификации их преимущества и недостатки, а также области применения этих методом.

Ключевые слова: идентификация; распознание лиц; биометрия; искусственные нейронные сети; Марковский процесс; контроль доступа; безопасность; защита.

MODERN METHODS OF BIOMETRIC IDENTIFICATION

Ryskina Vasilisa, Belova Maria
Admiral Makarov State University Of Maritime And Inland Shipping
5/7, Dvinskaya St., St. Petersburg, 198035, Russia
e-mails: vasilisa.rys@mail.ru, m-belova123@mail.ru

Abstract. The methods of biometric identification, their advantages and disadvantages, as well as the areas of application of these methods are considered.

Keywords: identification; face recognition; biometrics; artificial neural networks; Markov process; access control; safety; protection.

21-й век – это современная и научная эра, в ней был, достигнут большой прогресс, который приблизил человечество в реализации многих насущных задач. В настоящее время зачастую используются компьютерные технологии, которые являются неотъемлемой частью нашей жизни.

Компьютеры используются в системах приложений, которые варьируются от простых до сложных методов решения проблем. Среди таких методов появилась технология распознавания лиц, это полезный инструмент целью которого является распознавание особенностей лиц через присущие им черты. И тогда, и сейчас это представляет одну из самых исследуемых сфер в области распознавания образов и компьютерного зрения.

В современном мире данная технология используется все чаще, например, в биометрии, в информационной безопасности, в контроле допуска правоохранительных органов, системе охраны и смарт-картах.

Также эти технологии могут применятся для обеспечения безопасности особо охраняемых помещений на транспорте, в частности водном, в портах, транспортно-логистических центрах и т.д. [1-6].

1.Сложности в области распознания лиц.

A. Старение. Старение является неизбежным естественным процессом в течение жизни человека по сравнению с другими изменениями лица.

B. Частичная Окклюзия. Окклюзия относится к естественным или искусственным препятствиям в изображении. Это может быть локальная область лица вместе с различными объектами, такими как солнцезащитные очки, шарф, руки и волосы. Их обычно называют частичными окклюзиями. Подходы к распознаванию лиц с частичной окклюзией подразделяются на следующие три категории:

1) методы на основе частей

2) методы на основе признаков

3) методы на основе фракталов [7].

C. Инвариантность Позы.

Дисперсия позы является еще одним препятствием в достижении успешной системы распознавания лиц. Люди позируют по-разному каждый раз, когда они делают снимок. Нет никакого стандартизированного правила для принятия позы. Таким образом, это делает более трудным задачу различать и распознавать лица на изображениях с различными позами.

D. Иллюминация (Освещение). Освещение – это наблюдаемое свойство эффекта света. Это может также относиться к эффекту молнии или использованию источников света. Глобальная иллюминация – это алгоритм, который был использован в 3D графике. Изменение освещенности также плохо влияет на систему распознавания лиц.

2. Методы и приемы распознавания лиц.

A. Собственные Лица. Собственное лицо хорошо зарекомендовало себя алгоритмами, которые использовались для распознавания признаков на изображении лица. Метод основан на принципе компонентного анализа (PCA) [8]. В этом методе основной концепцией является распознавание лица, при котором принимается уникальная информация о лице в вопросительной форме. Затем кодируют его для сравнения с результатом декодирования ранее принятого изображения.

Системы распознавания лиц на основе собственных лиц подходят только для изображений, имеющих фронтальные грани, но некоторые исследования идентифицируют лицо с различными позами, которые также были сделаны [9].

B. Искусственные нейронные сети (ИНС). ИНС обеспечивает эффективную технику распознавания признаков. Она стала широко использоваться после появления искусственного интеллекта. ИНС – это нейронная сеть, где нейроны расположены в виде слоев. В итоге точность распознавания лиц была повышена с помощью более современных и сложных сетевых архитектур, и методов контроля, которыми обладает нейронная сеть. И в последнее время разрабатывается все больше и больше мощных методов обучения ИНС распознавания лица [10]. Используя эти методики, можно уже провести более глубокое обучение, которое будет гораздо ближе к человеческому представлению.

C. Метод опорных векторов (SVM). SVM - это своего рода контролируемый алгоритм обучения, который использует данные для классификации и регрессионного анализа. SVM обеспечивает эффективность в анализе глобальных размеров. SVM может быть реализован для распознавания лиц после искажения черт лица [11]. SVM может дать лучшие результаты, при работе с большим объемом данных, на основании которых делается выбор непосредственно с обучением. Однако, машина вектора поддержки наименьших квадратов (LS-SVM) [12, 13] является одним из популярных в типах SVM, который успешно используется для задачи распознавания лиц. Это обеспечивает преимущество быстрого вычисления, скорости наряду с высокой скоростью распознавания [9]. Компонент на основе классификатора метода опорных векторов [14] другой вариант SVM в лицо. Метод опорных векторов (SVM) является наиболее широко используемым методом, который реализуется на широком диапазоне задач классификации.

D. Вейвлет-преобразования Габора. Дэннисом Габором в 1946 году был представлен инструмент для обработки сигнала и удаления помех, назван этот инструмент фильтром Габора. Основными преимуществами вейвлет-преобразования (Вейвлет-преобразование переводит сигнал из временного представления в частотно-временное) Габора являются уменьшение признаков лица и его глобальное представление признаков в распознавании лиц [15 - 17]. Метод вейвлет-преобразований Габора широко используется для отслеживания лица и оценки положения в распознавании лиц. В то время как представление изображения с использованием вейвлет-преобразования обеспечивает как пространственные отношения, так и пространственную частотную структуру.

E. Скрытая Марковская модель (СММ). Скрытая Марковская модель (СММ) - это еще один метод статистического моделирования, при котором система подвергается Марковскому процессу со скрытыми состояниями.

Эта модель была предложена в 1960 году и внесла значительный вклад в распознавание речи. Основное применение СММ получили в области распознавания речи, письма, движений и биоинформатике. В настоящее время он реализуется для распознавания выражений лица. Также его можно приложить к видеопоследовательностям для опознавания людей.

3. Области применения методов распознавания лиц.

Есть много приложений, где методы распознавания лиц успешно используются для выполнения конкретной задачи. Немногие из них описаны:

A. Контроль Доступа. Управление доступом позволяет авторизованной группе пользователей получить доступ к Личному кабинету путем входа в систему через свою учетную запись электронной почты с помощью компьютера, имеющего доступ к банковскому счету через банкомат. Но с помощью системы распознавания лиц фотографии лица принимаются в естественных условиях, таких как фронтальные изображения лица. Такие системы обеспечивают оптимальную точность без какого-либо вмешательства пользователя.

B. Безопасность. Безопасность является наиболее важным элементом во всех местах. Компьютерная безопасность осуществляется с использованием программы распознавания лиц. В этой связи база данных изображений используется для целей исследования [9]; например, поиск изображений для аутентификации лицензированных водителей, для поиска пропавших людей, иммигрантов, в правоохранительных органах, общая проверка личности [9], регистрация избирателей, паспорта, удостоверения личности сотрудников.

C. Наблюдение. Наблюдение используется для слежки за поведением человека, его деятельностью или другой связанной информацией для обеспечения безопасности людей. Это может быть достигнуто с помощью электронного оборудования, т. е. камер замкнутого телевидения (CCTV) или перехвата передаваемой в электронном виде информации.

D. Посещаемость. Биометрические технологии посещаемости во времени были использованы для разрешений контроля допуска, и это одни из самых последних решений и традиционных вопросов компаний [18]. В этой технологии, пользователи должны выставить свое лицо в камеру машины на определенном расстоянии при этом исключается любой физический контакт с устройством. Это исключает любую возможность порчи или изменения машинного оборудования через свою вне-контактную процедуру метода. Система распознавания лиц фиксирует специфические черты человеческого лица и записывает их в виде математического шаблона. Для того, чтобы узнать лицо, изображение лица нормализуется, как к линии глаз и рта. Затем он выполняет сопоставление с математическими векторами из базы данных. Наконец, система распознавания лиц проверяет лицо и позволяет отмечать посещаемость или доступ к транзакции.

E. Всераспространенные вычисления. Цель всераспространенных вычислений состоит в том, чтобы создать сенсорную сеть, основанную на создании интеллектуальных устройств. Таким образом, сенсорная сеть используется для сбора, обработки и передачи данных, и в конечном итоге, она может понять свое окружение и улучшить качество жизни человека. Тем не менее, всераспространенные вычисления используют беспроводную связь и сетевые технологии, мобильные устройства, носимые компьютеры, встроенные системы, радиочастотные идентификационные устройства (RFID), промежуточное программное обеспечение и программные агенты. Всераспространенные вычисления широко используются в ряде отраслей, например, в энергетике, потребительском секторе, здравоохранении, производстве, военном деле, безопасности и логистике.

Изучение распознавания лиц остается приоритетной областью для исследователей на протяжении многих лет. Среди методов распознавания лиц наиболее популярными являются нейронные сети, машина опорных векторов, классификация на основе разреженного представления (SRC), классификация линейной регрессии (LRC), Регуляризованное Робастное кодирование (RRC) и ближайшая характерная линия (NFL). Основные выводы:

В настоящее время система распознавания лиц была внедрена во многие приложения реального времени, но все же она имеет ряд недостатков, которые необходимо решить, чтобы разработать хорошо зарекомендовавшую себя систему распознавания лиц.

Разработаны методы распознавания лиц, которые могут анализировать информацию по различным выражениям лица, т. е. при различных условиях освещения и позе.

Подобно распознаванию изображений лица, распознавание видеоизображений является более сложным методом и так же нуждается в дальнейшем изучении.

Предполагается, что для оценки распознавания видеоизображений могут быть использованы данные с YouTube.

СПИСОК ЛИТЕРАТУРЫ

1. Boriev, Z. Mathematical and information maintenance of biometric systems / Z. Boriev, S. Sokolov, A. Nyrkov, A. Nekrasova // IOP Conf. Series: Materials Science and Engineering 124(1) 2016. – № 012046 https://doi.org/10.1088/1757-899X/124/1/012046.
2. Kardakova M. Cyber Security on Sea Transport / M. Kardakova, I. Shipunov, A. Nyrkov, T. Knysh // Advances in Intelligent Systems and Computing, Vol. 982. – 2020. – Pp. 481 - 490. https://doi.org/10.1007/978-3-030-19756-8_46.
3. Данилин Г.В. Мультисервисные сети: методы повышения защищенности данных в условиях сетевых атак / Г. В. Данилин, С. С. Соколов, А. П. Ныркова, Т. П. Кныш // XXI век: итоги прошлого и проблемы настоящего плюс. – Т. 9. №2 (50). – 2020. – С. 158–163. https://doi.org/10.46548/21vek-2020-0950-0028.
4. Соколов С.С. Кибербезопасность на водном транспорте / С. С. Соколов, А. П. Ныркова, Н. Б. Глебов // Сборник тезисов докладов национальной научно-практической конференции профессорско-преподавательского состава ФГБОУ «ГУМРФ имени адмирала С. О. Макарова». — СПб: Изд-во ГУМРФ им. адм. С.О. Макарова, 2018. – С. 177–178.
5. Nyrkov, Anatoliy The use of Fuzzy Neural Structures to Increase the Reliability of Drilling Platforms / A. Nyrkov, S. Chernyi, A. Zhilenkov, S. Sokolov // Annals of DAAAM and Proceedings of the International DAAAM Symposium 2015, January, 2016. – Pp. 672-677. https://doi.org/10.2507/26th.daaam.proceedings.091.
6. Boriev Z. V. Review of modern biometric user authentication and their development prospects / Z. V. Boriev, S. S. Sokolov, A. P. Nyrkov // IOP Conf. Series: Materials Science and Engineering 91 (2015) 012063, 2015. https://doi.org/10.1088/1757-899X/91/1/012063.
7. Azeem, Aisha, et al. "A survey: face recognitiontechniques under partial occlusion." Int. Arab J. Inf. Technol. 11.1 (2014): 1-10.
3. Zhang, Xiaozheng, and YongshengGao. "Facerecognition across pose: A review." Pattern Recognition42.11 (2009): 2876-2896.

4. Muhammad Sharif et al.: ―Face Recognition: A Survey‖, Journal of Engineering Science and Technology Review 10 (2) (2017) 166- 177
5. Wang, Jizeng, and Hongmei Yang. "Face detectionbased on template matching and 2DPCA algorithm." Imageand Signal Processing, 2008. CISP'08. Congress on. Vol. 4. IEEE, 2008.
6. Ms. Snehal Houshiram Gorde1, et al.‖ A Review on Face Recognition Algorithms‖ Volume III, Issue I Issn No.:2350-1146, I.F-2.71
7. Zhang, Xinming, and JianZou. "Face recognition based on sub-image feature extraction and LS-SVM." Computer Science and Software Engineering, 2008 International Conference on. Vol. 1. IEEE, 2008.
8. Xie, Jianhong. "Face recognition based on Curvelet transform and LS-SVM." Proceedings of the 2009 (ISIP'09)Huangshan,
9. Huang, Jennifer, Volker Blanz, and Bernd Heisele."Face recognition using component-based SVMclassification and morphable models." Pattern Recognitionwith Support Vector Machines. Springer Berlin Heidelberg,2002.334-34
10. Chongliang Wu1, Shangfei Wang _1 and Qiang Ji"Multi-Instance Hidden Markov Model For Facial Expression Recognition 2015 IEEE
11. KalavdekarPrakash, N. "Face Detection using NeuralNetwork." International Journal of Computer Applications(0975–8887) 1.14 (2010).
12. Li, Yongmin, et al. "Multi-view face detection usingsupport vector machines and eigenspacemodelling." Knowledge-Based Intelligent Engineering Systems and Allied Technologies, 2000. Proceedings. Fourth International
13. Miar-Naimi, H., and P. Davari. "A new fast and efficient HMM-based face recognition system using a 7-state HMM

УДК 004.056

ВЛИЯНИЕ КИБЕРАТАК НА БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Соколов Сергей Сергеевич, Демаков Ярослав Александрович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: sokolovss@gumrf.ru, Chidori.jarik@mail.ru

Аннотация. В статье пойдет речь о кибератаках и их влиянии на безопасность государства, о видах кибератак и способах их осуществления.

Ключевые слова: кибератака; уязвимости программного обеспечения; хакер; вредоносное ПО.

IMPACT OF CYBER ATTACKS ON THE SECURITY OF INFORMATION SYSTEMS

Sokolov Sergei, Demakov Yaroslav
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: sokolovss@gumrf.ru, Chidori.jarik@mail.ru

Abstract. The article will discuss cyberattacks and their impact on state security, the types of cyberattacks and methods of their implementation.

Keywords: cyberattack; software vulnerabilities; hacker; malware.

Введение. В современном мире, большая часть информации в котором принимает электронный облик, преступления в информационной сфере уже давно из мошеннических схем стали перерастать в киберпреступления международного уровня. Действия, которые осуществляют высококвалифицированные специалисты в области информационных технологий могут нанести серьезный ущерб как экономической, так и политической составляющей страны, что в итоге может ввергнуть государство в кризис или привести к серьезным для него последствиям [1]. Осознавая это, спецслужбы многих стран уделяют повышенное внимание развитию специалистов в области информационной безопасности для отражения возможных кибератак со стороны противника и проведения собственных.

Данные атаки могут проводиться по многим направлениям и быть ориентированы на различные сферы жизни общества. Их целью может являться нарушение работы государственных учреждений, таких как больницы или органы самоуправления на местах, телевидение и информационные интернет-ресурсы предназначенные для информирования общественности.

В то же время целью кибератак может являться компрометация государственных служащих для подрыва их авторитета и понижения уровня доверия к управляющим органам среди общественности. Довольно часто подобные киберпреступления совершаются высококвалифицированными хакерами для получения личной выгоды или по заказу третьих лиц, опять же за материальное вознаграждение.

Для осуществления атак хакеры используют уязвимости в программном обеспечении атакуемых электронно-вычислительных машин. Если целью является проникновение в информационную сеть какого-либо предприятия, то преступники могут попытаться взломать аккаунты директоров компании или лиц, занимающих высокие должности. Это осуществляется при помощи методов фишинга или социальной инженерии, то есть для проникновения хакеры «взламывают» не систему, а человека, заставляя его осознанно выдать пароли и секретные данные организации [2].

Получив доступ во внутреннюю сеть, хакеры осваиваются в ней и производят кражу, изменение или порчу важных данных, что впоследствии может нанести компании серьезный ущерб. Точно также могут быть скомпрометированы государственные тайны или секреты правительства, что уже касается национальной безопасности государства [3].

Более того, при помощи социальной инженерии, фальсификации информации на известных новостных интернет порталах и обстоятельной подготовки злоумышленники своими действиями могут

«запрограммировать» поведение людей и устроить внутри государства настоящий искусственный кризис, способный повлечь за собой реальный [4].

В том числе атаки проводятся при помощи эксплуатации уязвимостей в программном обеспечении, используемом целью, благодаря чему на атакуемые сервисы может быть внедрено вредоносное ПО, задачей которого является установка бэкдоров для последующего возвращения хакеров в систему или для дальнейшего распространения вредоносного ПО внутри закрытой сети предприятия или компании. Так как чаще всего целью хакера является как можно дольше оставаться необнаруженным в системе, то программы подобного типа очень хорошо шифруются, обычно оставаясь невидимыми для антивирусов компании-жертвы. В то же время высококвалифицированный специалист по администрированию, то есть системный администратор может локализовать подозрительную активность в сети компании и пресечь дальнейшее распространение вирусного программного обеспечения с его дальнейшей нейтрализацией.

Следовательно, для предотвращения подобных инцидентов проводятся различные обучающие мероприятия с людьми, работающими с важными данными и сообщается о ценности любых корпоративных данных для злоумышленников, но даже такие методы в совокупности с использованием антивирусного ПО, усиленного администрирования внутренней сети и другими защитными методами не способно обеспечить полную безопасность.

Довольно часто причиной успешных хакерских атак на хорошо защищенные компании является неосторожный сотрудник, по невнимательности сообщивший преступнику конфиденциальную информацию организации. Поэтому постоянно идет разработка новых способов защиты от кибератак и противоправных действий в сети, в совокупности с развитием информационной грамотности работников.

Заключение. Статья на данную тему будет интересна для изучения студентам, обучающихся на направлениях, связанных с информационной безопасностью и специалистам в данной области, для расширения собственного кругозора и получения новых знаний. Планируется дальнейшее более глубокое изучение данной темы для выявления ключевых аспектов влияния киберпреступлений на функционирование государства в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Гибридные войны и обеспечение национальной безопасности России [Электронный ресурс] URL: https://cyberleninka.ru/article/n/gibridnye-voyny-i-obespechenie-natsionalnoy-bezopasnosti-rossii/viewer (дата обращения 16.08.2020).
2. Социальная инженерия как метод атаки [Электронный ресурс] URL: https://habr.com/ru/post/348496/ (дата обращения 15.08.2020).
3. Компрометация [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/Компрометация_(криптография) (дата обращения 14.08.2020).
4. Кузнецов М.В. Социальная инженерия и социальные хакеры [Текст]/ М.В.Кузнецов, И.В.Симдянов. 2004.- 344 с.

УДК 004.056

СТРУКТУРА ГОССОПКА

Соколов Сергей Сергеевич, Назаров Никита Михайлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: onik-2000@mail.ru, sokolovss@gumrf.ru

Аннотация. Рассматривается структура, принципы работы Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Ключевые слова: информационная безопасность, информация, угрозы, инциденты, защита, критическая информационная инфраструктура.

GOSSOPKA STRUCTURE

Sokolov Sergey, Nazarov Nikita
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: onik-2000@mail.ru, sokolovss@gumrf.ru

Abstract. The structure, principles of operation of the State system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation.

Keywords. information security, information, threats, incidents, protection, critical information infrastructure.

Введение. 1 января 2018 года вступил в силу федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» ФЗ-187, одной из целей которого являлось создание Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) [1], которая контролируется Национальным координационным центром по компьютерным инцидентам ФСБ России (НКЦКИ). Предпосылками для создания данной системы и координационного центра являлись масштабные эпидемии компьютерных вирусов, таких как WannaCry, Petya.

Основной задачей НКЦКИ является координация деятельности субъектов критической информационной инфраструктуры (КИИ) по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты [2]. Для выполнения данной задачи НКЦКИ осуществляет следующий набор функции:

- Координация и участие в компьютерных инцидентах;
- Организация и осуществление обмена информацией о инцидентах между субъектами КИИ;
- Сбор, хранение и анализ информации о компьютерных инцидентах;
- Участие в обнаружении, предупреждении и ликвидации последствий атак;
- Анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий атак

Каждый субъект КИИ, являющийся участником ГосСОПКА, создаёт в своём составе центр ГосСОПКА. Центрами ГосСОПКА являются органы власти, юридические лица, которые в рамках данной системы занимаются противодействием компьютерным атакам. В рамках ГосСОПКА противодействие атакам означает выполнение участником системы определенного набора функций:

- Инвентаризация информационных ресурсов;
- Выявление уязвимостей;
- Анализ угроз ИБ;
- Составление перечня угроз;
- Ликвидация последствий инцидентов;
- Составление перечня инцидентов;
- Анализ результатов ликвидации последствий инцидентов;
- Подготовка рекомендаций по повышению защищенности.

Для выполнения этих функции, центры ГосСОПКА получают все возможные данные об ИС, контролируют их защищенность и анализируют события, регистрируемые их ПО. При этом они не заменяют собой системы защиты информационных систем. Всё то же самое владельцы объектов КИИ должны делать самостоятельно, а центр ГосСОПКА всего лишь координирует.

Государственные регуляторы тщательно подчеркивают, что защита объекта КИИ от компьютерных атак – это обязанность и ответственность самого субъекта КИИ. Государство не будет нести никакую ответственность, подтверждая достаточность принятых субъектом КИИ мер защиты. Это предполагает возможность ошибок, допускаемых субъектами КИИ при защите своих ИС. Поэтому федеральный закон допускает, что в значимых объектах КИИ возможны инциденты, и в этом случае обязывает владельца объекта информировать об инциденте ФСБ и реагировать в этом случае на инцидент так, как установлено нормативными документами ФСБ [3].

При реагировании на атаки центр ГосСОПКА сочетает в себе роли координатора и экспертной группы. Для атак, с которыми центр уже сталкивался, отрабатываются специальные сценарии, которые определяют необходимые действия персонала для отражения атак. Если же центр ранее не встречался с данной атакой, то формируется специальная рабочая группа из представителей персонала защищаемой ИС и экспертов центра, и дальнейшие решения по предотвращению атаки принимаются в процессе реагирования.

Действия специальной рабочей группы при встрече с неизвестным видом атаки не всегда являются корректными, поэтому после каждого реагирования проводится тщательный разбор действий участников, по итогам которого совершенствуется система защиты самой ИС и работа центра ГосСОПКА. Из этого следует, что работа центра ГосСОПКА строится на принципах самосовершенствования.

Заключение. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак – своего рода партнёрство частных компаний, являющихся субъектами КИИ, и государства в сфере противодействия компьютерным инцидентам. В рамках ГосСОПКА обеспечивается некое слияние компетенций, необходимых для предотвращения атак и реагирования на них, и воспользоваться такими компетенциями могут как представители крупного бизнеса, так и малого. В свою очередь государство в лице НКЦКИ выступает гарантом добросовестности центров ГосСОПКА, устанавливая определённые требования к их деятельности, осуществляя надзор за этой деятельностью и даже иногда участвуя в реагировании на некоторые атаки.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ [Электронный ресурс] URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения 15.08.2020).
2. ВЫПИСКА ИЗ КОНЦЕПЦИИ государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс] URL: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf (дата обращения 15.08.2020).
3. Колесникова М.Н., Ананьев С.В. ОСНОВНЫЕ ФУНКЦИИ ГОССОПКА В РАМКАХ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ КОМПЬЮТЕРНЫХ АТАК [Электронный ресурс] URL: https://elibrary.ru/download/elibrary_41482602_50958077.pdf (дата обращения 16.08.2020).

УДК 004.056

О НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ ВЫСОКОГО УРОВНЯ ИФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Соколов Сергей Сергеевич, Швец Артем Дмитриевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails:sokolovss@gumrf.ru, shvets.gora@mail.ru

Аннотация. Рассматриваются методы и средства по обеспечению кибербезопасности, угрозы кибербезопасности и необходимость обеспечения кибербезопасности на персональном и государственном уровне.

Ключевые слова: кибербезопасность; социальная инженерия; APT-атака; удаленный доступ.

ABOUT THE NEED TO ENSURE HIGH LEVEL OF INFORMATION SACURITY

Sokolov Sergey, Nazarov Nikita
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails:sokolovss@gumrf.ru, shvets.gora@mail.ru

Abstract. Consider cybersecurity techniques and tools, cybersecurity threats, and the need for cybersecurity at the personal and state levels.

Keywords: cyber security; social engineering; APT attack; remote access.

В современных условиях кибернетическая безопасность является главной составляющей любой организации, пусть это будет какая-то частная компания или огромная военная корпорация. Все они имеют данные, которые надо защищать, иначе их могут направить против них же. Кроме того, сейчас, в условиях пандемии COVID-19 увеличилось количество кибернетических атак, что прибавляет немало работы экспертам в области информационной безопасности.

В данный момент существует множество проблем кибербезопасности, связанных как с персональными информационными системами, так и с системами международного уровня. Главными уязвимостями для информационной безопасности в нынешних условиях являются фишинг, безопасность удаленного доступа, отказы, сбои в работе, нарушение доступности и т.п. Но все же основная проблема - это социальная инженерия, так как весь мир постепенно перешел на дистанционную работу в сети интернет, и все чаще злоумышленники стараются получить данные обычных людей, госслужащих, военных и других личностей [1].

Но также появляются новые методы атак на предприятия, например APT-атаки, поиск аппаратных уязвимостей и громких утечек. Группировки, использующие такие типы атак, постепенно становятся главной угрозой кибербезопасности, так как используют самые новые методы атак, все делают быстро и четко, а также постоянно меняют инструментарий и тактику атаки. Если в 2018 таких групп было обнаружено около 12, то в 2019 году их насчитывалось уже около 27, что совершенно не в пользу защитников информации. В результате этого компании и фирмы стали действовать по принципу парадигмы «ability to detect», т.е. главной задачей они ставят как можно быстрее обнаружить уязвимость и найти атакующего, чтобы не допустить непоправимого ущерба. Это все привело к тому, что компании ищут высокоинтеллектуальные методы защиты информации, по выявлению угроз, таких как Security information and event management (SIEM), Network traffic analysis (NTA), комплексные antiAPT решения.

В связи с существованием множества угроз информационной безопасности, появляется необходимость защиты в следующих областях: в промышленности, в телекоммуникации, в финансовом секторе, в аппаратной разработке систем, а также при разработке мобильных устройств и операционных систем [2].

Для защиты данных довольно часто используются уже устоявшиеся методы и средства, например средства ограничения физического доступа к информации, межсетевые экраны, системы мониторинга сетей, различные анализаторы сетей, антивирусы, методы криптографии и многое другое, которые в полной мере выполняют свою задачу, но иногда и их недостаточно. Поэтому компаниям приходится составлять собственные алгоритмы защиты или нанимать людей извне для этих целей, что несет дополнительные расходы.

На государственном уровне закреплено немало методов защиты информационных систем. Так в связи с переходом на удаленную работу ФСТЭК России подготовил рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры, которые включают в себя проведение инструктажа работников, работающих с критической инфраструктурой; определение перечня средств вычислительной техники, которые будут предоставлены работникам для удаленной работы; определение информации и информационных ресурсов, к которым будет осуществляться удаленной доступ; разграничение доступа к информации; идентификация устройств по физическим адресам (MAC-адресам); двухфакторная аутентификация и многие другие методы защиты информации [3]. Это говорит о вовлеченности в кибербезопасность не только отдельно взятых людей, но и целых держав, которым надо защищать конфиденциальную информацию.

Так компания Comparitech, изучив уровень кибербезопасности 76 стран, заявила, что российское законодательство в области кибербезопасности лучше всего соответствует современным требованиям. А самыми кибербезопасными странами являются Дания и Япония. Кроме того рейтинг многих стран в данной отрасли либо немного опустился, либо начал подниматься, что однозначно показывает, что уровень вовлеченности в сферу кибербезопасности только растет, и всем странам становится важна защита их данных [4].

Таким образом, кибернетическая безопасность становится важной составляющей в жизни людей. На неё с каждым годом будут только расти расходы в мире, так в 2020 году прогнозируют увеличение на 5,6 %, что составляет $43,1 млрд [5]. Поэтому всем нам надо пополнять свои знания в области кибербезопасности, развиваться в этом направлении и быть аккуратными, чтобы не потерять важные данные, связанные с вами, с вашими знакомыми или с государством.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность в условиях пандемии COVID-19 [Электронный ресурс] URL: https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-covid-19/ (дата обращения 16.08.2020).
2. Кибербезопасность 2019-2020. Тренды и прогнозы. [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/ (дата обращения 17.08.2020).
3. Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры. ФСТЭК России, 2020. - Письмо ФСТЭК России от 20 марта 2020 г. N 240/84/389 - 3 с. - URL: https://fstec.ru/component/attachments/download/2711
4. Кибербезопасность в России хорошо отрегулирована [Электронный ресурс] URL: https://www.comnews.ru/content/204880/2020-03-05/2020-w10/kiberbezopasnost-rossii-khorosho-otregulirovana (дата обращения 18.08.2020).
5. Canalys: затраты на кибербезопасность существенно вырастут в 2020 году [Электронный ресурс] URL: https://www.securitylab.ru/news/510438.php (дата обращения 18.08.2020).

УДК 621.391.26

ИССЛЕДОВАНИЕ РАБОТЫ АЛГОРИТМОВ ПРЕДУПРЕЖДЕНИЯ СТОЛКНОВЕНИЙ ПРИ ПОЛЁТЕ ДВУХ ВОЗДУШНЫХ СУДОВ В ОДНОМ НАПРАВЛЕНИИ С МЕДЛЕННЫМ ГОРИЗОНТАЛЬНЫМ СБЛИЖЕНИЕМ

Худошин Владимир Викторович
Институт Авиационного Приборостроения «Навигатор»
Шкиперский проток, 14З/19, Санкт-Петербург, 199106, Россия
e-mail: cmex81@gmail.com

Аннотация. Рассматривается сценарий воздушной обстановки, при котором алгоритмы бортовой системы предупреждения столкновения второго поколения могут предоставить экипажу воздушного судна некорректные рекомендации по разрешению конфликтной ситуации в воздухе. Проведено моделирование набора сценариев, соответствующих полету двух воздушных судов в одном направлении с медленным горизонтальным сближением. В результате анализа данных моделирования получены рекомендации по улучшению алгоритма предупреждения столкновения в эксплуатируемой в настоящее время авиационной аппаратуре и намечены пути для дальнейшей модернизации.

Ключевые слова: воздушная обстановка; алгоритмы; предупреждение столкновений; исследование; моделирование сценариев.

RESEARCH FOR THE COLLISION AVOIDANCE ALGORITHMS DURING THE FLIGHT TWO AIRCRAFTS IN ONE DIRECTION WITH A SLOW HORIZONTAL CLOSURE RATES

Khudoshin Vladimir
Institute of Avionics Engineering “Navigator”
14Z/19, Shkiperski Protok, St. Petersburg, 199106, Russia
e-mail: cmex81@gmail.com

Abstract. The scenario of an encounter simulation, which algorithms collision avoidance would issue non-correct resolution advisories for the induced near mid-air collision. Scenario cases has been performed for the flight two aircrafts in one direction with horizontal closure rates. The results allowed obtain conclusions and recommendations for an improving current algorithms for further modernization.

Keywords: near mid-air collision; algorithms; collision avoidance; research; scenario modeling.

В 2019-2020гг были опубликованы документы с требованиями к новому, третьему, поколению систем предупреждения столкновений в воздухе, при этом в настоящее время активно эксплуатируются первое и второе поколения этой системы. В докладе рассмотрена работа системы второго поколения в определенной воздушной обстановке.

Бортовая система предупреждения столкновений предназначена для выдачи экипажу оповещений с целью предотвращения столкновения при возникновении потенциальной опасности. Эта цель достигается путем выдачи рекомендаций RA (Resolution Advisory) для выполнения манёвра пилотом, а также путем выдачи предупредительной

информации о воздушном движении TA (Traffic Advisory), которая является признаком необходимости визуального обнаружения близ летящего воздушного судна и сигнализирует о возможности выдачи RA [1].

В процессе эксплуатации систем предупреждения столкновений по результатам анализа полётных данных экспертами рабочей группы SC-147 организации RTCA (Radio Technical Comission for Aeronautics) был выявлен ряд недостатков в работе алгоритмов предупреждения столкновений систем второго поколения, в том числе выработка некорректного оповещения экипажа воздушного судна. При полёте воздушных судов, оборудованных данной системой, в одном направлении с траекториями движения, при которых происходит медленное сближение в горизонтальной проекции и с высокими скоростями сближения в вертикальной проекции может произойти ложное формирование рекомендации RA [2].

Для исследования работы алгоритмов предупреждения столкновений в описанной выше воздушной ситуации было использовано программное обеспечение TSIM, поставляемое организацией RTCA по запросу [3]. Данное приложение предназначено для исследования работы алгоритмов эталонной реализации версии 7.1 и проверки собственной реализации алгоритмов на соответствие спецификации требований, предъявляемых к логике работы системы.

При исследовании описанной выше воздушной ситуации был создан набор имитационных сценариев, соответствующих ей. Для воздушных судов, участвующих в воздушном конфликте, был задан ряд параметров: путевая скорость, высота полета, вертикальная скорость, курс собственного воздушного судна, пеленг другого воздушного судна, смещение по горизонтали, вертикальное ускорение с i-го по j-й цикл симуляции, время моделирования сценария.

По результатам анализа данных моделирования стало понятно, что в ряде сценариев алгоритмы предупреждения столкновений выдали помимо сообщения TA рекомендации экипажу на совершение маневра. При этом столкновение воздушных судов было невозможно физически, так как хотя их траектории могли пересечься в вертикальной проекции, но в горизонтальной проекции они располагались друг от друга на расстоянии около одной морской мили.

Одна из причин в формировании некорректной рекомендации экипажу заключается в алгоритме определения ряда величин, используемых для проверки условий этого формирования. В случае прохождения проверки на угрозу по дальности и дальнейшем сближении воздушных судов может быть неверно определен момент времени столкновения. При относительно больших скоростях сближения в горизонтальной проекции возможная ошибка расчётов невелика и является несущественной. Однако при малых скоростях сближения триггер формирования угрозы может сработать значительно раньше, вплоть до десятков секунд. Если же другое воздушное судно находится на расстоянии меньшем, чем порог безопасности в горизонтальной проекции и продолжит двигаться параллельным курсом, триггер формирования угрозы сработает немедленно. На больших высотах полета порог безопасности в горизонтальной проекции принимает значение в 1.1 морскую милю. То есть воздушное судно с малой скоростью сближения (почти нулевой) на дальности менее чем 1.1 морских миль будет трактоваться так, как будто оно может столкнуться с нами в следующий момент времени даже при том, что это невозможно физически.

В результате проведенного исследования были определены значения параметров движения воздушных судов в обстановке данного типа, при которых необходимо провести дополнительный анализ траекторий воздушных судов для исключения выдачи нежелательных рекомендаций экипажу. Одним из способов дополнительной обработки траектории воздушных судов может быть применение алгоритмов машинного обучения [4, 5]. Был проведен анализ использования различных типов алгоритмов машинного обучения применительно к нашей проблеме и выбрано для первичного исследования использование обученной нейронной сети. По окончанию исследования были получены следующие результаты: применение дополнительных вычислений для анализа вышеописанной воздушной обстановки позволило успешно уточнить сформированные рекомендации и не ухудшить качественные характеристики всех контролируемых параметров.

СПИСОК ЛИТЕРАТУРЫ

1. Doc 9863. Руководство по бортовой системе предупреждения столкновений (БСПС). – Монреаль, ИКАО, 2012, 254 с.
2. RTCA DO-337. Recommendations for Future Collision Avoidance Systems. – Вашингтон, RTCA, 2012, 44 с.
3. RTCA DO-185B. MOPS for Traffic Alert and Coliision Avoidance System II (TCAS II). – Вашингтон, RTCA, 2008, 548 с.
4. Николенко С.И., Кадурин А.А., Архангельская Е.О., Глубокое обучение. – СПб: «Питер», 2020, 480 с.
5. Нейрокомпьютеры в авиации (самолеты).Кн.14 / под ред. А.Н. Галушкина. – М: «Радиотехника», 2003, 496с.

УДК 004.3

IOT УСТРОЙСТВА КАК ВАЖНЫЙ АСПЕКТ СОВРЕМЕННОГО МОРСКОГО ТРАНСПОРТА

Шипунов Илья Сергеевич, Ныркoв Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: mr-shis@yandex.ru, kaf.koib@gmail.com

Аннотация. Рассматриваются принципы применения устройств IoT на современных судах. Предлагаются схемы построения умной грузовой инфраструктуры, а также подходы к решению задач маневрирования с применением данных полученных от системы сенсоров.

Ключевые слова: современное судоходство, IoT, сенсорные системы, умные контейнеры.

IOT DEVICES AS AN IMPORTANT ASPECT OF MODERN MARITIME TRANSPORT

Shipunov Ilya, Nyrkov Anatoly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: mr-shis@yandex.ru, kaf.koib@gmail.com

Abstract. Principles of application of IoT devices on modern ships are considered. Schemes of building smart cargo infrastructure as well as approaches to solving maneuvering tasks using the data obtained from the sensor system are proposed.

Keywords: modern navigation, IoT, sensor systems, smart containers.

На сегодняшний день IT тренды все больше внедряются в работу современной индустрии морских перевозок. В ходе данной работы будут выделены несколько наиболее перспективных для отрасли IT трендов. И предложены варианты использования их в рамках морских перевозок. Стоит отметить, что современное развитие IT индустрии — это сложный процесс, в котором развитие одного компонента влечет за собой развитие другого. Это обусловлено очень высоким уровнем зависимости компонентов друг от друга. Однако каждый новый шаг в развитии приносит не только положительные эффекты, но и определенный пул проблем, связанных в первую очередь с безопасностью, стоимостью внедрения и подготовки кадров [1]. Кроме того, даже сегодняшний уровень автоматизации и роботизации требует новаторский решений в области законодательства. Многие нормативно правовые акты нужно привести к условиям современной реальности.

Никто сегодня не оспорит тезис о невообразимо быстром внедрении в нашу жизнь технологий интернета вещей. Ведь это так удобно, взять привычные для некоторого процесса устройства и научить их взаимодействовать друг с другом. Кроме этого, необходимо научить устройства анализировать среду, в которой они находятся, накапливать информацию и предпринимать определенные действия в той или иной ситуации. Дать подобным устройствам пространство для обмена информацией и командами друг с другом (объединить в сеть) и на выходе получится отличный помощник по управлению данным процессом.

Главная задача при создании таких устройств это «обучение» восприятия окружающей среды или более конкретного объекта наблюдения. С этой задачей инженеры и программисты современности справляются все лучше и лучше. И подобным устройствам доверяется участие во все более сложных процессах.

Наиболее сложной технической задачей в рамках морского транспорта считается создание безэкипажных судов [2]. В данном направлении трудятся практически все крупные игроки рынка морских перевозок. Одной из сложностей при проектировании судов подобного типа становится разрешение задачи замены команды. Однако, если механические действия экипажа, с современными возможностями роботизации, имитировать вполне реально, то вот анализ человеком окружающей обстановки заменить очень сложно. Все прекрасно понимают, что выработка тех или иных управленческих решений часто происходит исходя из личного опыта и применения его к наблюдаемой картине происходящего. Именно для решения данной проблемы могут подойти устройства IoT.

Рассмотрим технологический слой подобного проекта. Именно здесь находится точка пересечения потоков информации, поступающей из внешних источников (например, со спутников) и источников внутренних – различных бортовых систем и сенсоров. Внедрение устройств IoT на данном уровне позволит обеспечить не только должный уровень прогнозирования, но и реализовать механизм накопления опыта, который потом может служить для совершенствования механизма принятия решений. Подобные технологии могут служить фундаментом в навигационных системах судов безэкипажного типа. Обработка спутниковой информации о морской обстановке позволит строить наиболее эффективные маршруты следования. Способность устройств обмениваться сообщениями с устройствами которые только обнаружены или с уже знакомыми устройствами, пропадавшими из поля видимости, позволит научить подобные системы видеть друг друга на море и избежать аварийных ситуаций. Общение систем с береговой инфраструктурой позволит заранее подготовить порт к прибытию судна и снабдит администрацию порта всей необходимой информацией о судне и грузе.

Еще одной областью применения IoT в морских перевозках это создание на судне умной грузовой инфраструктуры. В такую инфраструктуру должны войти умные трюмы, умные контейнеры и центр управления и взаимодействия с ними.

Умные контейнеры должны отслеживать и при необходимости корректировать температуру, влажность, давление воздуха. Так же фиксировать вибрации и место положение контейнера как в общей геолокации, так и свое место нахождение на судне после погрузки. Центр взаимодействия позволит на берегу отслеживать всю телеметрию с контейнера, что поможет при решении споров о порче груза при перевозке. А знание местоположения всегда позволит проследить весь путь перемещения груза [3].

Подобные разработки уже внедряются в свой рабочий цикл компанией CMA CGM. Для организации умной системы грузов используется технология Traxen. Данная технология служит для отслеживания рефрижераторных контейнеров. Для подобной системы был переоборудован контейнеровоз Bougainville. Все контейнеры на его борту образуют единую умную сеть и всегда поддерживают связь с береговым офисом компании.

В рамках безэкипажных судов очень важным аспектом является общение морского дрона с берегом для интеллектуальной интеграции его в морской трафик. Как уже говорилось ранее этот так же можно организовать на основе технологии IoT. В качестве объектов наблюдения и анализа могут выступать временные параметры

маневрирования судов при заходах в порт. Ведение учета и хранения подобных данных позволит сократить время простоя и ускорить подготовку к принятию судна. Передовой опыт подобных внедрений можно наблюдать в порту Роттердам. Данный порт совместно с компанией IBM ведет работы по внедрению умных устройств, оцифровке и обработке данных с них. На данный момент порт может начать подготовку еще в тот момент как судно будет находится в чуть более 40 километрах от него. Это повышает как уровень эффективности работы данного порта, так и уровень его безопасности.

С помощью IoT так же можно решить спектр задач, связанных с навигацией в непростых условиях. Под непростыми условиями здесь понимается большой объем трафика на путях следования, а также плохие погодные условия.

Подобная интеллектуальная система опираясь на данные с сенсоров и на алгоритмы обработки должна строить пространственную модель препятствий и опасных зон [4]. Что прямо должно влиять на ход маневрирования судна. Это повысит уровень безопасности судоходства.

Современный уровень разработки и облачного обучении искусственного интеллекта (AI) позволяет строить описанные выше интеллектуальные системы с использованием AI. В качестве основы можно взять технологию Google Cloud Machine Learning Engine. Данная система опирается на AI и способна помочь в распознавании, классификации и отслеживанию объектов, с которыми судно может столкнуться в море.

Так же IoTможно использовать при контроле отхода судна или же автономной постановки судна в док. Данные контроля судозаходов можно использовать для фиксации в блокчейн цепочках. Этот фактор позволит развивать область смарт контрактов и контроля груза страховыми компаниями.

Таким образом приходит понимание, что область применения IoT устройств на современных судах очень обширна. Развитие алгоритмов и технологических платформ — это стратегически важное направление в современном судостроении. Однако всегда остается риск реализации различных кибер атак на подобные устройства [5]. Поэтому при разработке и внедрении подобных решений крайне важно озаботится вопросами кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. “The Safety Assessment of Critical Infrastructure Control System” 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 5 November 2018, pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948
2. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “About the Problems of Ensuring Information Security on Unmanned Ships” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 339-343. https://doi.org/10.1109/EIConRus.2019.8657219
3. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “Trusted transport telemetry by using distributed databases” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 344-347. https://doi.org/10.1109/EIConRus. 2019.8657215
4. S. Shipunov, A. P. Nyrkov, M. V. Kardakova, Y. F. Katorin and V. V. Vychuzhanin, "Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 497-500, doi: 10.1109/EIConRus49466.2020.9039181.
5. Kardakova, M., Shipunov, I., Nyrkov, A., Knysh, T. “Cyber Security on Sea Transport” Advances in Intelligent Systems and Computing, vol. 982, (2020), pp.481-490. https://doi.org/10.1007/978-3-030-19756-8_46

УДК 004.3

УМНЫЕ СИСТЕМЫ - ВАЖНАЯ СОСТАВЛЯЮЩАЯ В ВОПРОСАХ АВТОМАТИЗАЦИИ МОРСКИХ ПЕРЕВОЗОК

Шипунов Илья Сергеевич, Ныркov Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: mr-shis@yandex.ru, kaf.koib@gmail.com

Аннотация: рассматриваются возможности построения систем мониторинга на современных судах с использованием технологий IoT и Blockchain. Приводится возможная схема построения системы мониторинга с использованием IOT

Ключевые слова: современное судоходство, IoT, системы мониторинга, blockchain.

SMART SYSTEMS ARE AN IMPORTANT COMPONENT IN THE AUTOMATION OF MARITIME TRANSPORTATION

Shipunov Ilya, Nyrkov Anatoly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: mr-shis@yandex.ru, kaf.koib@gmail.com

Abstract. The possibilities of building monitoring systems on modern ships using IoT and Blockchain technologies are considered. The possible scheme of building a monitoring system using IOT is given.

Keywords: modern shipping, IoT, monitoring systems, blockchain.

Перспективным направлением применения устройств IoT на судах является создание различных систем мониторинга. Эти системы позволяют судовладельцам извлекать из них пользу уже на стадии проектирования перевозки. Своевременный ремонт узлов, экономичная схема заправки судна и многое другое, так или иначе, приносят экономическую выгоду и сокращают расходы [1].

Основной артерией таких систем можно назвать канал передачи информации между бортовым контроллером и облачной платформой. Если речь идет о речных судах, то в качестве канала можно использовать мобильную сеть. Но если речь идет о морском судоходстве, то сегодня можно надеяться только на спутниковую связь. Этот момент сразу указывает на слабое место в таких системах - спутниковый Интернет не всегда стабилен на протяжении всего пути судна. Этот фактор необходимо учитывать при построении такой системы и обеспечить надежный резервный режим устойчивой сети для передачи данных на облачную платформу [2].

Такая система может включать в себя следующие компоненты:

– различные сенсорные системы управления для получения данных для дальнейшего анализа;
– контроллер платы как главный агрегатор и передатчик данных в облачную платформу;
– облачная платформа как система обработки цифровых данных, поступающих от бортовых контроллеров судов и генератор отчетов для менеджеров.

Одной из возможных функций такой схемы является организация эффективной системы мониторинга расхода топлива. Датчики для такой системы могут быть двух типов: уровнемеры и расходомеры. Первый тип предназначен для контроля уровня топлива в баках, второй - для мгновенной оценки расхода и является расходомером. Конфигурация и места установки датчиков должны выбираться в зависимости от требуемой точности измерений и мощности топливной системы [3].

Индикаторы от датчиков обрабатываются бортовым контроллером и передаются на облачную платформу, которая в свою очередь формирует отчет и дает рекомендации по оптимальному циклу заправки. В отчет также могут быть записаны предупреждения о возможных сливах топлива, что позволяет обнаружить кражу. Добавив к обработке данные из других систем, можно также оценить качество топлива и отсеять недобросовестных поставщиков. С другой стороны, такие оценки могут указывать на необходимость начать работы по техобслуживанию энергоблоков.

Следует понимать, что такая система сама по себе не экономит топливо, а является мощным инструментом прогнозирования реального потребления при различных условиях и интенсивности работы энергоблоков. Так как система имеет память, то на основе анализа типичных показателей легко определить отклонение расхода от нормы. Эти измерения не позволят привести в движение нечестные схемы слива топлива. Еще одним важным нюансом является повышение уровня планирования закупок топлива, что позволит более эффективно распределять бюджет.

Еще одним важным преимуществом при использовании такой системы может быть постоянное наличие актуальной информации о выбросах углекислого газа. Зная точный расход топлива, система легко предоставит эту информацию. Это обеспечит выполнение требований MRV и IMO в этой области.

Кроме того, когда судно входит в зону ECA (SECA), система сообщит о необходимости перехода на топливо с низким содержанием серы.

Еще одной особенностью таких систем мониторинга является возможность повышения отказоустойчивости за счет внедрения дополнительных алгоритмов управления индикаторами в систему Processing. То есть, даже в условиях, когда тот или иной датчик системы выходит из строя и этот факт фиксируется системой, могут быть подключены дополнительные подсистемы обработки, а недостающие данные будут заменены на те, которые могут быть получены по данным от работающих датчиков.

Рассмотрим следующий пример. На дизельном генераторе вышел из строя основной топливный датчик расходомера. Система зафиксировала этот факт. При передаче данных на облачную платформу бортовой контроллер также передаст факт выхода из строя датчика. Облачная платформа может ввести дополнительный алгоритм в рабочий цикл. Из базы знаний платформа также загрузит информацию о характеристике дизель-генератора, установленного на судне, после чего сможет производить расчеты на основе показателей от датчика уровня энергии, вырабатываемой этим генератором.

При создании таких систем необходимо обеспечить надлежащий уровень безопасности и правильную работу оборудования, установленного на борту судна. Как правило, такие системы оснащены специальной бортовой панелью, на которой контроллер может выводить на экран цифровые индикаторы от датчиков для быстрого реагирования команды на ситуацию возникновения проблемы. Увидев индикаторы от датчиков в реальном времени, квалифицированный инженер может настроить работу бортовых датчиков и контроллера таким образом, чтобы контроллер передавал некорректные данные на облачную платформу. Для защиты оборудования лучше использовать дополнительную систему блокировки видеосигнала, обеспечить резервное питание системы и герметизировать корпуса, в которых установлено внешнее оборудование [4].

Еще одна технология, которая позволит в итоге получать выгоду это Blockchain. Blockchain — это технология распределенного реестра, позволяющая безопасно регистрировать операции в реестре сразу в нескольких местах и через нескольких физических лиц без необходимости в централизованной администрации или посредниках.

Следует понимать, что в настоящее время морская индустрия по-прежнему сильно зависит от бумажных записей. Одним из факторов этой зависимости является слабая стандартизация форматов электронного обмена данными.

Одной из проблем кибербезопасности при использовании IoT-устройств на судах может стать централизованное хранение и обработка данных. Чтобы исключить ситуацию, при которой злоумышленник достаточно атаковать уникальное устройство, чтобы подвергнуть опасности всю систему, можно организовать хранение информации по блочному принципу. Также используя этот механизм, можно надежно реализовать процесс согласования и подписания документов, что позволит частично выйти из бумажного документооборота.

Также возможно реализовать с помощью этого механизма:

- системы отслеживания грузов;
- системы визуализации цепочки поставок;
- система регистрации судовых данных;
- глобальная система анализа рисков;
- интеллектуальная система управления контрактами
- система электронного страхования;

Умные контракты - еще одна быстрорастущая тенденция. Эти программные контракты, исполнение которых основано на технологии Blockchain. Они предназначены для автоматизации отслеживания исполнения пунктов, установленных программистами-контрактниками. Используя данную технологию, можно без особых затруднений реализовать "умный" шаблон коносамента при морском судоходстве.

Как только применение "умных" контрактов достигнет высокого уровня развития, дальнейший план действий будет включать в себя: переговоры по фрахтовым ставкам непосредственно между судовладельцами и их контрагентами; автоматическую обработку платежей, а также оформление страховых полисов и урегулирование претензий по морскому страхованию с использованием технологии Blockchain [5].

СПИСОК ЛИТЕРАТУРЫ

1. Sokolov, S.S., Glebov, N.B., Antonova, E.N., Nyrkov, A.P. “The Safety Assessment of Critical Infrastructure Control System” 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 5 November 2018, pp. 154-157. https://doi.org/10.1109/ITMQIS.2018.8524948
2. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “About the Problems of Ensuring Information Security on Unmanned Ships” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 339-343. https://doi.org/10.1109/EIConRus.2019.8657219
3. S. Shipunov, A. P. Nyrkov, M. V. Kardakova, Y. F. Katorin and V. V. Vychuzhanin, "Information System for Monitoring and Analyzing the Technical Condition of Autonomous Vehicles," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 497-500, doi: 10.1109/EIConRus49466.2020.9039181.
4. Kardakova, M., Shipunov, I., Nyrkov, A., Knysh, T. “Cyber Security on Sea Transport” Advances in Intelligent Systems and Computing, vol. 982, (2020), pp.481-490. https://doi.org/10.1007/978-3-030-19756-8_46
5. Shipunov, I.S., Voevodskiy, K.S., Nyrkov, A.P., Katorin, Y.F., Gatchin, Y.A. “Trusted transport telemetry by using distributed databases” 2019 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), St. Petersburg; 2019. pp. 344-347. https://doi.org/10.1109/EIConRus. 2019.8657215

ОГЛАВЛЕНИЕ

CONTENTS