ТУСУР
TUSUR UNIVERSITY

634050, г. Томск, пр. Ленина, 40, каб. 129
Телефон: +7 (3822) 900-100
e-mail: onir@main.tusur.ru

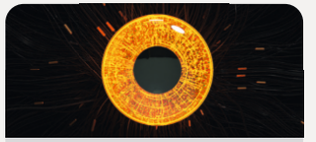
Радиотехнический факультет

Факультет электронной техники

Радиоконструкторский факультет

Факультет систем управления

Экономический факультет



Факультет вычислительных систем

Юридический факультет

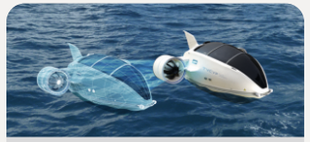
Факультет инновационных технологий

Факультет безопасности

Гуманитарный факультет

Заочный и вечерний факультет

Больше информации о магистратуре в ТУСУР на официальном сайте magistrant.tusur.ru



Электронное приборостроение и системы связи (ПИШ)

Факультет дистанционного обучения

ТУСУР TUSUR UNIVERSITY

Сборник избранных статей научной сессии ТУСУР

ПО МАТЕРИАЛАМ МЕЖДУНАРОДНОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ СТУДЕНТОВ, АСПИРАНТОВ И МОЛОДЫХ УЧЕНЫХ
«НАУЧНАЯ СЕССИЯ ТУСУР–2023»
г. Томск, 17–19 мая 2023 г.
(в трех частях)

ЧАСТЬ 3

г. Томск

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)»

Сборник избранных статей научной сессии ТУСУР

**по материалам
международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2023»**

17–19 мая 2023 г., г. Томск

В трех частях

Часть 3

ТУСУР
В-Спектр
Томск, 2023

УДК 621.37/.39+681.518 (063)
ББК 32.84я431+32.988я431
С 23

С 23 **Сборник избранных статей научной сессии ТУСУР**, Томск, 17–19 мая 2023 г.: в 3 ч. – Томск: ТУСУР (заказчик); В-Спектр (ИП Бочкарева В.М., исполнитель), 2023. – Ч. 3. – 332 с.

ISBN 978-5-902958-09-3
ISBN 978-5-902958-10-9 (Ч. 1)
ISBN 978-5-902958-11-6 (Ч. 2)
ISBN 978-5-902958-12-3 (Ч. 3)

Сборник избранных статей научной сессии ТУСУР включает избранные доклады по итогам международной научно-технической конференции студентов, аспирантов и молодых ученых. Конференция посвящена различным аспектам разработки, исследования и практического применения радиотехнических, телевизионных и телекоммуникационных систем и устройств, сетей электро- и радиосвязи, вопросам проектирования и технологии радиоэлектронных средств, аудиовизуальной техники, бытовой радиоэлектронной аппаратуры, а также автоматизированых систем управления и проектирования. Рассматриваются проблемы электроники СВЧ- и акустооптоэлектроники, нанофотоники, физической, плазменной, квантовой, промышленной электроники, радиотехники, информационно-измерительных приборов и устройств, распределенных информационных технологий, вычислительного интеллекта, автоматизации технологических процессов, в частности, в системах управления и проектирования, информационной безопасности и защиты информации. Представлены статьи по экономике и менеджменту, антикризисному управлению, правовым проблемам современной России, автоматизации управления в технике и образовании, а также работы, касающиеся социокультурных проблем современности, экологии, мониторинга окружающей среды и безопасности жизнедеятельности.

УДК 621.37/.39+681.518 (063)
ББК 32.84я431+32.988я431

ISBN 978-5-902958-09-3
ISBN 978-5-902958-12-3 (Ч. 3)

Сборник избранных статей научной сессии ТУСУР

по материалам
международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2023», 17–19 мая 2023 г.

ПРОГРАММНЫЙ КОМИТЕТ

- Рулевский В.М. – председатель Программного комитета, ректор ТУСУРа, д.т.н.;
- Лощилов А.Г. – заместитель председателя Программного комитета, проректор по научной работе и инновациям ТУСУР, к.т.н.;
- Афонасова М.А., зав. каф. менеджмента ТУСУРа, д.э.н., проф.;
- Бабур-Карателли Г.П., к.т.н., PhD (TU Delft), научный сотрудник каф. ТОР ТУСУРа;
- Беляев Б.А., зав. лаб. электродинамики и СВЧ-электроники Института физики СО РАН, д.т.н., г. Красноярск (по согласованию);
- Ботаева Л.Б., руководитель направления по оказанию инжиниринговых услуг, АНО «Томский региональный инжиниринговый центр», к.т.н. (по согласованию);
- Васильковская Н.Б., доцент каф. экономики ТУСУРа, к.э.н.;
- Голиков А.М., доцент каф. РТС ТУСУРа, к.т.н.;
- Денисов В.П., проф. каф. РТС ТУСУРа, д.т.н.;
- Дмитриев В.М., проф. каф. КСУП ТУСУРа, д.т.н.;
- Еханин С.Г., проф. каф. КУДР ТУСУРа, д.ф.-м.н.;
- Заболоцкий А.М., зав. каф. СВЧиКР ТУСУРа, д.т.н.;
- Зариковская Н.В., доцент каф. АОИ ТУСУРа, к.ф.-м.н.;
- Зейниденов А.К., PhD, декан физико-технического факультета НАО Карагандинский университет им. акад. Е.А. Букетова, проф., г. Караганда (Казахстан) (по согласованию);
- Исакова А.И., доцент каф. АСУ ТУСУРа, к.т.н.;
- Карташев А.Г., проф. каф. РЭТЭМ ТУСУРа, д.б.н.;
- Катаев М.Ю., проф. каф. АСУ ТУСУРа, д.т.н.;
- Ким М.Ю., зав. каф. ИСР ТУСУРа, к.и.н.;
- Кобзев Г.А., проректор по международному сотрудничеству, к.т.н.;
- Костина М.А., доцент каф. УИ, к.т.н.;
- Коцубинский В.П., зам. зав. каф. КСУП ТУСУРа, доцент каф. КСУП, к.т.н.;
- Красинский С.Л., декан ЮФ ТУСУРа, к.и.н.;

- Куприянов Е.А., директор Центра по работе с талантливой молодежью ТУСУРа;
- Лукин В.П., зав. лаб. когерентной и адаптивной оптики ИОА СО РАН, д.ф.-м.н., проф., г. Томск (по согласованию);
- Малюк А.А., проф. отделения интеллектуальных кибернетических систем офиса образовательных программ, Институт интеллектуальных кибернетических систем НИЯУ МИФИ, к.т.н., г. Москва (по согласованию);
- Малютин Н.Д., гл.н.с. НИИ систем электрической связи, проф. каф. КУДР ТУСУРа, д.т.н.;
- Мицель А.А., проф. каф. АСУ ТУСУРа, д.т.н.;
- Озеркин Д.В., декан РКФ ТУСУРа, к.т.н.;
- Орлова В.В., зав. каф. ФиС, д.соц.н.;
- Оскирко В.О., н.с. лаборатории прикладной электроники ИСЭ СО РАН, технический директор ООО «Прикладная электроника», к.т.н.;
- Покровская Е.М., зав. каф. ИЯ ТУСУРа, к.филос.н.;
- Разинкин В.П., проф. каф. ТОР, декан факультета радиотехники и электроники, Новосибирский государственный технический университет, д.т.н., г. Новосибирск (по согласованию);
- Рогожников Е.В., зав. каф. ТОР ТУСУРа, к.т.н.;
- Ромакина О.М., доцент каф. информатики и компьютерных технологий Санкт-Петербургского горного университета, к.ф.-м.н., г. Санкт-Петербург (по согласованию);
- Ромашко Р.В., член-корреспондент РАН, директор ИАПУ ДВО РАН, проф. ДВФУ, д.ф.-м.н., г. Владивосток (по согласованию);
- Семенов Э.В., проф. каф. РСС ТУСУРа, д.т.н.;
- Сенченко П.В., проректор по учебной работе ТУСУРа, доцент каф. АОИ, к.т.н.;
- Суслова Т.И., декан ГФ ТУСУРа, д.ф.н., проф.;
- Титов В.С., проф. каф. вычислительной техники Юго-Западного государственного университета, д.т.н., заслуженный деятель наук РФ, академик международной академии наук ВШ, г. Курск (по согласованию);
- Троян П.Е., зав. каф. ФЭ ТУСУРа, д.т.н., проф.;
- Туев В.И., зав. каф. РЭТЭМ ТУСУРа, д.т.н., проф.;
- Ходашинский И.А., проф. каф. КСУП ТУСУРа, д.т.н.;
- Цветкова Н.А., доцент Высшей школы киберфизических систем и управления института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Великого, к.т.н., г. Санкт-Петербург (по согласованию);
- Чжан Е.А., зам. директора Института космических и информационных технологий (ИКИТ) по научной работе, ФГАОУ ВО «Сибирский федеральный университет», к.т.н. (по согласованию);
- Шарангович С.Н., проф. каф. СВЧиКР ТУСУРа, к.ф.-м.н.;
- Шелупанов А.А., президент ТУСУРа, директор ИСИБ, д.т.н., проф.;
- Шостак А.С., проф. каф. КИПР ТУСУРа, д.т.н.;

- Шурыгин Ю.А., директор департамента управления и стратегического развития ТУСУРа, зав. каф. КСУП, д.т.н., проф.;
- Issakov V., professor at University Otto-von-Guericke Magdeburg, Germany (по согласованию);
- Caratelli D., PhD, professor of the Department of Electrical Engineering (Eindhoven University of Technology), technical director of the company «The Antenna Company Nederland B.V.» (по согласованию);
- Krozer V., professor at Goethe University, Frankfurt am Main (по согласованию).

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

- Лощилов А.Г. – председатель Организационного комитета, проректор по научной работе и инновациям ТУСУРа, зав. каф. КУДР, к.т.н.;
- Медовник А.В. – заместитель председателя Организационного комитета, начальник научного управления, д.т.н.;
- Байгулова Т.А., председатель Студенческого научного сообщества «Система», аспирант каф. УИ;
- Боберь Ю.Н., специалист по учебно-методической работе ОАиД;
- Климов А.С., председатель Совета молодых ученых, ст. научный сотрудник лаборатории плазменной электроники каф. физики, д.т.н.;
- Коротина Т.Ю., зав. аспирантурой, ОАиД, к.т.н.;
- Михальченко Т.С., техник отдела набора и распределения студентов;
- Покровская Е.М., зав. каф. ИЯ, к.филос.н.;
- Юрченкова Е.А., вед. инженер ОАиД, к.х.н.

СЕКЦИИ КОНФЕРЕНЦИИ

Секция 1. Радиотехника и связь

Подсекция 1.1. Радиотехнические системы и распространение радиоволн. *Председатель – Денисов Вадим Прокопьевич, проф. каф. РТС, д.т.н.; зам. председателя – Аникин Алексей Сергеевич, доцент каф. РТС, к.т.н.*

Подсекция 1.2. Проектирование и эксплуатация радиоэлектронных средств. *Председатель – Шостак Аркадий Степанович, проф. каф. КИПР, д.т.н.; зам. председателя – Озёркин Денис Витальевич, декан РКФ, к.т.н.*

Подсекция 1.3. Радиотехника. *Председатель – Семенов Эдуард Валерьевич, проф. каф. РСС, д.т.н.; зам. председателя – Артищев Сергей Александрович, доцент каф КУДР, к.т.н.*

Подсекция 1.4. Видеоинформационные технологии. *Председатель – Курячий Михаил Иванович, доцент каф. ТУ, к.т.н.; зам. председателя – Каменский Андрей Викторович, доцент каф. ТУ, к.т.н.*

Подсекция 1.5. Инфокоммуникационные технологии и системы широкополосного беспроводного доступа. *Председатель – Рогожников Евгений Васильевич, зав. каф. ТОР, к.т.н.; зам. председателя – Дмитриев Эдгар Михайлович, ассистент каф. ТОР.*

Подсекция 1.6. Робототехника. *Председатель – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.*

Подсекция 1.7. Интеллектуальные системы проектирования технических устройств. *Председатель – Шурыгин Юрий Алексеевич, директор департамента управления и стратегического развития ТУСУРа, зав. каф. КСУП, д.т.н., проф.; зам. председателя – Черкашин Михаил Владимирович, доцент каф. КСУП, к.т.н.*

Секция 2. Электроника и приборостроение

Подсекция 2.1. Проектирование биомедицинских электронных и наноэлектронных средств. *Председатель – Еханин Сергей Георгиевич, проф. каф. КУДР, д.ф.-м.н.; зам. председателя – Романовский Михаил Николаевич, доцент каф. КУДР, к.т.н.*

Подсекция 2.2. Разработка контрольно-измерительной аппаратуры. *Председатель – Лощилов Антон Геннадьевич, проректор по НРиИ, зав. каф. КУДР, к.т.н.; зам. председателя – Бомбизов Александр Александрович, начальник СКБ «Смена», к.т.н.*

Подсекция 2.3. Физическая и плазменная электроника. *Председатель – Троян Павел Ефимович, зав. каф. ФЭ, д.т.н., проф.; зам. председателя – Смирнов Серафим Всеволодович, проф. каф. ФЭ, д.т.н.*

Подсекция 2.4. Промышленная электроника. *Председатель – Семенов Валерий Дмитриевич, проф. каф. ПрЭ, к.т.н.; зам. председателя – Оскирко Владимир Олегович, научный сотрудник лаборатории прикладной электроники ИСЭ СО РАН, технический директор ООО «Прикладная электроника», к.т.н., Михальченко Сергей Геннадьевич, зав. каф. ПрЭ, д.т.н.*

Подсекция 2.5. Оптические информационные технологии, нанофотоника и оптоэлектроника. *Председатель – Шарангович Сергей Николаевич, проф. каф. СВЧиКР, к.ф.-м.н.; зам. председателя – Перин Антон Сергеевич, доцент каф. СВЧиКР, к.т.н.*

Подсекция 2.6. Электромагнитная совместимость. *Председатель – Заболоцкий Александр Михайлович, зав. каф. СВЧиКР, д.т.н.; зам. председателя – Белоусов Антон Олегович, доцент каф. ТУ, к.т.н.*

Подсекция 2.7. Светодиоды и светотехнические устройства. *Председатель – Туев Василий Иванович, зав. каф. РЭТЭМ, д.т.н.,*

проф.; зам. председателя – Солдаткин Василий Сергеевич, доцент каф. РЭТЭМ, к.т.н.

Секция 3. Информационные технологии и системы

Подсекция 3.1. Интегрированные информационно-управляющие системы. *Председатель – Катаев Михаил Юрьевич, проф. каф. АСУ, д.т.н.; зам. председателя – Суханов Александр Яковлевич, доцент каф. АСУ, к.т.н.*

Подсекция 3.2. Распределённые информационные технологии и системы. *Председатель – Сенченко Павел Васильевич, проректор по УР, доцент каф. АОИ, к.т.н.; зам. председателя – Сидоров Анатолий Анатольевич, зав. каф. АОИ, к.э.н.*

Подсекция 3.3. Автоматизация управления в технике и образовании. *Председатель – Дмитриев Вячеслав Михайлович, проф. каф. КСУП, д.т.н.; зам. председателя – Ганджа Тарас Викторович, проф. каф. КСУП, д.т.н.*

Подсекция 3.4. Вычислительный интеллект. *Председатель – Ходашинский Илья Александрович, проф. каф. КСУП, д.т.н.; зам. председателя – Сарин Константин Сергеевич, доцент каф. КСУП, к.т.н.*

Подсекция 3.5. Молодежные инновационные научные и научно-технические проекты. *Председатель – Костина Мария Алексеевна, доцент каф. УИ, к.т.н.; зам. председателя – Нариманова Гуфана Нурлабековна, зав. каф. УИ, декан ФИТ, к.ф.-м.н.*

Подсекция 3.6. Разработка программного обеспечения. *Председатель секции – Зариковская Наталья Вячеславовна, доцент каф. АОИ, ген. директор ООО «АльдераСофт», к.ф.-м.н.; зам. председателя – Колотаев Илья Владимирович, старший разработчик ООО «Синкретис».*

Подсекция 3.7. Инструментальные средства поддержки автоматизированного проектирования и управления. *Председатель – Хабибулина Надежда Юрьевна, декан ФВС, доцент каф. КСУП, к.т.н.; зам. председателя – Потапова Евгения Андреевна, ст. преподаватель каф. КСУП.*

Секция 4. Информационная безопасность

Подсекция 4.1. Методы и системы защиты информации. Информационная безопасность. *Председатель – Шелупанов Александр Александрович, президент ТУСУРа, директор ИСИБ, д.т.н., проф.; зам. председателя – Новохрёстов Алексей Константинович, доцент каф. КИБЭВС, к.т.н.*

Подсекция 4.2. Цифровые системы радиосвязи и средства их защиты. *Председатель – Голиков Александр Михайлович, доцент каф. РТС, к.т.н.*

Подсекция 4.3. Экономическая безопасность. *Председатель – Кузьмина Елена Александровна, директор Международной цифровой академии, к.т.н.; зам. председателя – Колтайс Андрей Станиславович, ст. преподаватель каф. ЭБ.*

Секция 5. Экономика, управление, социальные и правовые проблемы современности

Подсекция 5.1. Моделирование в экономике. *Председатель – Мицель Артур Александрович, проф. каф. АСУ, д.т.н.; зам. председателя – Грибанова Екатерина Борисовна, доцент каф. АСУ, к.т.н.*

Подсекция 5.2. Информационные системы в экономике. *Председатель – Исакова Анна Ивановна, доцент каф. АСУ, к.т.н.; зам. председателя – Григорьева Марина Викторовна, доцент каф. АСУ, к.т.н.*

Подсекция 5.3. Реализация современных экономических подходов в финансовой и инвестиционной сферах. *Председатель – Васильковская Наталья Борисовна, доцент каф. экономики, к.э.н.; зам. председателя – Цибульникова Валерия Юрьевна, зав. каф. экономики, к.э.н.*

Подсекция 5.4. Проектный менеджмент и его использование в цифровой экономике. *Председатель – Афонасова Маргарита Алексеевна, зав. каф. менеджмента, д.э.н., проф.; зам. председателя – Богомолова Алена Владимировна, доцент каф. менеджмента, декан ЭФ, к.э.н.*

Подсекция 5.5. Современные социокультурные технологии в организации работы с молодежью. *Председатель – Орлова Вера Вениаминовна, зав. каф. ФиС, директор НОЦ «СГТ», д.соц.н.; зам. председателя – Корнющенко-Ермолаева Наталия Сергеевна, ст. преподаватель каф. ФиС.*

Подсекция 5.6. Актуальные проблемы социальной работы в современном обществе. *Председатель – Ким Максим Юрьевич, зав. каф. ИСР, к.и.н.; зам. председателя – Куренков Артем Валериевич, доцент каф. ИСР, к.и.н.*

Подсекция 5.7. Актуальные вопросы частного права в условиях цифровой трансформации. *Председатель – Мельникова Валентина Григорьевна, доцент, зав. каф. ИГПиПОИД, к.ю.н.; зам. председателя – Часовских Кристина Виктовна, ст. преп. каф. ИГПиПОИД.*

Подсекция 5.8. Современные тенденции развития российского права. *Председатель секции – Ахмедшин Рамиль Линарович, проф. каф. ГПДиПД, д.ю.н.; зам. председателя – Алексеева Татьяна Александровна, доцент каф. ГПДиПД, к.ю.н.*

Секция 6. Экология и мониторинг окружающей среды. Безопасность жизнедеятельности. *Председатель – Карташев Александр Георгиевич, проф. каф. РЭТЭМ, д.б.н.; зам. председателя – Денисова Татьяна Владимировна, доцент каф. РЭТЭМ, к.б.н.*

Секция 7. Открытия. Творчество. Проекты. (Секция для школьников). *Председатель – Куприянов Евгений Александрович, директор Центра по работе с талантливой молодежью ТУСУРа; зам. председателя – Михальченко Татьяна Сергеевна, специалист по работе с молодежью ОПиРШ) УНН.*

Секция 8. Postgraduate and Master Students' Research in Electronics and Control Systems. *Председатель – Покровская Елена Михайловна, зав. каф. ИЯ, доцент, к.филос.н.; зам. председателя – Шпит Елена Ирисметовна, ст. преп. каф. ИЯ, Соболевская Ольга Владимировна, ст. преп. каф. ИЯ, Таванова Эльвира Борисовна, ст. преп. каф. ИЯ.*

Адрес оргкомитета:
634050, Россия, г. Томск, пр. Ленина, 40,
ФГБОУ ВО «ТУСУР»
Научное управление (НУ), к. 205. Тел.: 8 (382-2) 701-524

Сборник в 3 частях:

1 часть – 1-я секция (подсекции 1.1 – 1.7); 2-я секция (подсекции 2.1 – 2.5).
2 часть – 2-я секция (подсекции 2.6, 2.7); 3-я секция (подсекции 3.1 – 3.7); 6-я секция.
3 часть – 4-я секция (подсекции 4.1 – 4.3); 5-я секция (подсекция 5.1 – 5.8), 8-я секция.

7-я секция издана отдельным сборником.

Генеральный спонсор конференции – АО «ИнфоТеКС»

АО «ИнфоТеКС» +7 (495) 737-61-92
127083, Москва, 8 (800) 250-0-260
ул. Отрадная 2Б, стр. 1 www.infotecs.ru

АО «ИнфоТеКС» является ведущим разработчиком, а также производителем высокотехнологичных программных и программно-аппаратных средств и систем защиты информации. Входит в ТОП-10 крупнейших российских компаний в сфере информационной безопасности. Будучи лидером, ИнфоТеКС активно развивает партнёрскую сеть, в которую на данный момент входит свыше 300 компаний. В штате трудоустроено более 1600 сотрудников, а офисы открыты в 9 городах России.

Главный продукт компании – бренд ViPNet. В этой торговой марке более 50 различных продуктов (программных и программно-аппаратных комплексов), каждый из которых может содержать в себе несколько функциональных модулей. Они по праву признаны самым масштабируемым и гибким решением для построения защищённых сетей, которое соответствует всем требованиям законодательства РФ. ViPNet широко известен среди большинства отраслевых специалистов, ведь с помощью него защищено уже более 10 млн рабочих станций. Например, все элементы системы продажи билетов в ОАО «Российские железные дороги» и Портал государственных услуг РФ.

Помимо этого, АО «ИнфоТеКС» плодотворно взаимодействует с регуляторами, профильными комитетами Росстандарта и профессиональным сообществом по вопросам стандартизации в сфере защиты информации. Эксперты компании принимали участие в разработке нового стандарта ГОСТ Р 34.11–2012 (Стрибог) и криптографического протокола CRISP. А специалисты являются членами таких профильных общественных организаций и ассоциаций, как АРПП «Отечественный Софт», Ассоциация предприятий компьютерных и информационных технологий, Ассоциация документальной электросвязи, Ассоциация защиты информации и Ассоциация ЕВРААС.

Важным направлением для компании является поддержка научных разработок и исследовательских проектов, а также обучение и продвижение молодых специалистов.

Поэтому уже более 12 лет ИнфоТеКС активно работает над развитием потенциала будущего и реализует специальную программу стажировки «ИнфоТеКС Академия». Главная задача проекта – помогать специалистам получать и эффективно использовать знания и

навыки, необходимые для успешной работы в сфере информационной безопасности. Участники стажировки работают над реальными проектами компании под руководством опытных кураторов, а лучших из них ИнфоТеКС приглашает в ряды штатных сотрудников.

Кроме того, в рамках ИнфоТеКС Академии осуществляется грантовая программа, направленная на поддержку молодых учёных, формирование кадрового потенциала и развитие научно-исследовательской среды в области криптографии, ИТ- и ИБ-разработок. В рамках данной программы уже реализовано более 49 проектов и получено 7 патентов.

Спонсор конференции – АО «НПФ «Микран»

АО «НПФ «Микран»
634041, г. Томск,
проспект Кирова, д. 51 д

Т. +7 (382-2) 90-00-29
Ф. +7 (382-2) 42-36-15
www.micran.ru

АО «НПФ «Микран» – ведущий производитель радиоэлектроники России, успешно конкурирующий с зарубежными компаниями. В 1991 г. Виктор Яковлевич Гюнтер с командой из семи человек создал предприятие на базе научной лаборатории Томского института автоматизированных систем управления и радиоэлектроники (сейчас ТУСУР).

Основные направления деятельности сегодня – производство телекоммуникационного оборудования, контрольно-измерительной аппаратуры и аксессуаров СВЧ-тракта, сверхвысокочастотной электроники и модулей, радаров для навигации и обеспечения безопасности, мобильные комплексы связи, комплексные решения в области связи и автоматизации.

Множество наших разработок являются уникальными: начиная от электронной компонентной базы СВЧ и заканчивая серийными изделиями и комплексными решениями. «Микран» активно внедряет инновационные разработки, контролирует процесс создания технологии и отслеживает качество выпускаемой продукции.

В 2020 г. под эгидой Минпромторга «Микран» был включен в перечень системообразующих организаций Российской Федерации в числе предприятий радиоэлектронной отрасли.

Практически с самого начала своей деятельности «Микран» активно взаимодействует с томскими университетами. В 2012 г. была учреждена стипендия имени основателя «Микрана» Виктора Яковлевича Гюнтера. На стипендию могут претендовать студенты технических направлений ТУСУРа, ТПУ и ТГУ, которые имеют достижения в учебной, научной, спортивной и общественной деятельности.

Кроме того, с 2019 г. в компании успешно реализуется проект стажировки для студентов и молодых специалистов технических специальностей MICRANstart. Участники стажировки получают возможность работать над реальными проектами компании под руководством опытных наставников, а лучших из них «Микран» приглашает стать частью своей дружной команды.

Спонсор конференции – ООО «50ом Технолоджиз»

50ohm Technologies	ООО «50ом Технолоджиз» info@50ohm.tech https://50ohm.tech/ru 634045, г. Томск	7-923-408-04-08 50ohmTechRus company/50ohm-technologies-llc

Компания «50ohm Technologies» разрабатывает программное обеспечение для автоматизации измерений, построения моделей компонентов и проектирования ВЧ- и СВЧ-радиоэлектронных устройств.

50ohm Technologies предлагает решения задач автоматизации рабочих процессов с учётом индивидуальных особенностей предприятия. Миссия компании – разрабатывать удобные, умные, интеллектуальные инструменты, которые помогают инженерам в области СВЧ-электроники быстро решать возникающие задачи.

Компания разрабатывает программные решения по направлениям:

- автоматизация измерений устройств электроники и радиоэлектроники;
- базы данных результатов измерений и их автоматическая обработка;
- автоматизация проектирования СВЧ-устройств;
- построение моделей электронных компонентов;
- подготовка научно-технической документации.

Компания обладает компетенциями в использовании методов искусственного интеллекта и экспертных систем. Внедрение данных технологий на предприятие позволяет перейти на качественно новый уровень и автоматизировать наиболее рутинные этапы бизнес-процессов.

«50ohm Technologies» предлагает услуги по разработке систем автоматизации измерений, реализуемых на основе оборудования заказчика. Использование готовых сценариев измерений конкретных компонентов и устройств в значительной степени сократит время тестирования и повысит эффективность измерений. «50ohm Technologies» производит разработку решений автоматизированной генерации технической документации по типовым шаблонам – от оформления графиков до формирования готовых документов.

Компания обладает значительным опытом построения моделей пассивных и активных СВЧ-компонентов. Создание программного обеспечения на основе общепринятых и авторских методик в значительной степени упрощает и автоматизирует процесс построения мо-

делей, уменьшая временные и финансовые затраты предприятия на данном этапе.

Наиболее сложным этапом в процессе проектирования СВЧ-устройства является получение схемотехнического и топологического решений. За годы научной работы коллектив получил успешный опыт разработки и использования программных модулей САПР, основанных на методах искусственного интеллекта. Такие программы позволяют получить целый набор решений, из которых разработчик может выбрать наиболее подходящее для дальнейшей реализации. Также компания занимается автоматизацией проектных операций в популярных коммерческих САПР СВЧ-устройств и интеграцией между ними.

СЕКЦИЯ 4

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПОДСЕКЦИЯ 4.1

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Председатель – ***Шелупанов А.А.****, президент ТУСУРа, директор ИСИБ, д.т.н., проф.;*
зам. председателя – ***Новохрёстов А.К.****, доцент каф. КИБЭВС, к.т.н.*

УДК 004.832.28

МЕТОДЫ РАЗВИТИЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

К.Г. Пономарёв, аспирант ИМКТ ДВФУ;
Е.А. Верещагина, доцент Департамента программного и искусственного интеллекта ИМКТ ДВФУ, к.т.н.
г. Владивосток, ДВФУ, ponomarev.kg@dvfu.ru

Проблематика сокращения трудозатрат аналитика безопасности при работе в системах управления информацией и событиями безопасности является наиболее актуальной темой для научного исследования. Переход этих систем с базовых функций визуализации показателей в реальном времени на более высокий уровень анализа и принятия решений требует новых методик в создании мониторинга событий. Для этого активно внедряются методы машинного обучения и применяются искусственные нейронные сети, что позволяет обучить систему реагировать на аномальное поведение случайных величин и осуществлять экспертную оценку. Формирование новых функций в SIEM-системах предполагается достичь с применением методов построения искусственных нейронных сетей.

Ключевые слова: системы управления информацией и событиями безопасности, корреляция, искусственные нейронные сети, модель нейрона.

Системы управления информацией и событиями безопасности (SIEM-системы) получили большую востребованность в эпоху больших данных и многократного увеличения объема поступающей для аналитики информации. Впоследствии SIEM-системы стали незаменимым программным инструментом для аналитика безопасности, которому приходится ежедневно проводить мониторинг безопасности ИТ-инфраструктуры. Главным ядром SIEM-системы определен процесс корреляции поступающих данных от разнородных физических и виртуальных устройств в организации, качество которого существенно влияет на обработку полученной информации и на определение приоритезации инцидентов безопасности.

Процесс корреляции выявляет взаимосвязи между различными статистическими случайными величинами и позволяет выявлять угрозы по алгоритмам их поведения, а также, что немаловажно, исключать бесполезные для мониторинга события [1]. Выявление инцидентов включает использование готовых правил и накопленных экспертных баз знаний. Основная задача современных SIEM-систем – сократить время выявления инцидентов аналитиком безопасности и предоставить качественные для анализа результаты [2].

В SIEM-системе в качестве экспертного модуля или компонента системы обнаружения вторжений можно применить базовый метод построения искусственных нейронных сетей прямого распространения [3]. Данная искусственная нейронная сеть позволит обеспечить дополнительный экспертный функционал. Структура построения сети с таким подходом представлена подаваемыми входными сигналами, весовыми показателями, сумматором и функцией активации (рис. 1). На выходе мы получаем взвешенную сумму, на основании которой принимаем решение о действии нейрона.

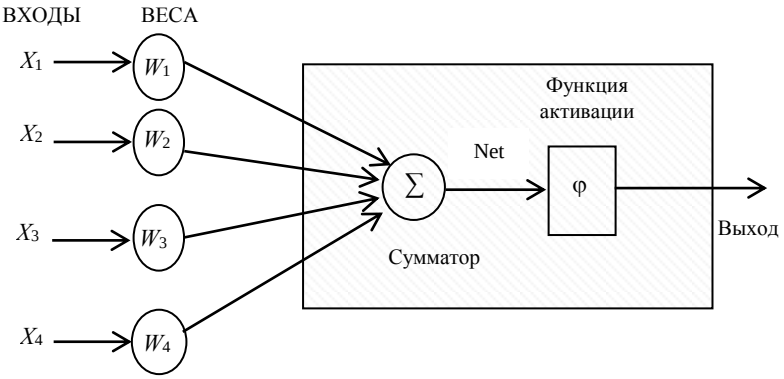


Рис. 1. Модель искусственного нейрона

У каждого нейрона существует вход, который принимает сигнал. Далее используется принцип весов, который суммирует поступивший сигнал. Далее сигнал X умножается на собственный вес W, и таким образом дальнейшее прохождение сигнала позволяет провести суммирование всех элементов через сумматор помноженных на собственные веса. Следовательно, получается следующая формула:

$$X_1W_1 + X_2W_2 + X_3W_3 + ... + X_nW_n = \sum_{i+1}^{n} X_iW_i.$$

Роль сумматора заключается в получении взвешенной агрегированной суммы net от всех сигналов, которая характеризует поступивший сигнал на нейрон.

$$\text{net} = \sum_{i+1}^{n} X_iW_i.$$

Одним из важных компонентов искусственного нейрона является функция активации, принимающая взвешенную сумму как аргумент, представленная следующей формулой:

$$\text{out} = \varphi(\text{net}).$$

Выход из функции активации может быть представлен следующими вариантами: функция единичного скачка с выходными значениями 0 или 1, сигмоидальной функцией с приближенными значениями с применением крутизны функции и гиперболическим тангенсом со значениями от –1 до 1.

По итогам исследований выявлен большой потенциал в развитии новых подходов мониторинга инцидентов безопасности для построения мониторинга в SIEM-системах, построенных на искусственных нейронных сетях. Их применение в практических задачах информационной безопасности будет только возрастать, а SIEM-системы из функционала уведомительного характера все больше будут переходить в область экспертных систем, применяемых методы машинного обучения и нейронных сетей, что в целом качественно сократит время процесса изучения в SIEM-системах аналитиком безопасности.

ЛИТЕРАТУРА

1. Кириллов В.А. Система сбора и корреляции событий (siem) как ядро системы информационной безопасности / В.А. Кириллов, А.Р. Касимова, А.Д. Алёхин // Вестник Казан. технол. ун-та. – 2016. – № 13. – С. 132–134 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/ sistma-sbora-i-korrelyatsii-sobytiy-siem-kak-yadro-sistemy-informatsionnoy-bezopasnosti, свободный (дата обращения: 10.03.2023).

2. Арзамасцев Н.А. Особенности использования искусственных нейронных сетей в сфере информационной безопасности // StudNet. – 2022. – № 5. – С. 3936–3945 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/osobennosti-ispolzovaniya-iskusstvennyh-neyronnyh-setey-v-sfere-informatsionnoy-bezopasnosti, свободный (дата обращения: 10.03.2023).

3. Андреев В.В. Обработка сигналов нейросетью прямого распространения: аппроксимация и принятие решений / В.В. Андреев, Л.А. Славутский,

Е.В. Славутская // Вестник ЧГУ. – 2022. – № 1. – С. 14–22 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/obrabotka-signalov-neyrosetyu-pryamogo-rasprostraneniya-approksimatsiya-i-prinyatie-resheniy, свободный (дата обращения: 10.03.2023).

УДК 004.056.2

ТЕХНОЛОГИЗАЦИЯ ПРОЦЕССОВ ДЛЯ ЗАДАЧ СИНХРОНИЗАЦИИ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УСТОЙЧИВОГО ФУНКЦИОНИРОВАНИЯ

С.И. Штеренберг, к.т.н., доцент

Научный консультант О.И. Шелухин, д.т.н., проф.
Московского технического университета связи и информатики
г. Санкт-Петербург, Санкт-Петербургский гос. университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича,
shterenberg.stanislaw@yandex.ru

Рассмотрен процесс развития систем защиты информации (далее – СЗИ), базирующихся на принципах построения генетических алгоритмов в интеллектуальных системах обнаружения вторжений (далее – СОВ), иммунных систем и мультиагентном подходе к представлению самоорганизующихся карт нейронных сетей (далее – НС). Данное технологизированное мероприятие входит в общий комплексный подход по развитию интеллектуальных СЗИ в рамках четвертой промышленной революции (Индустрия 4.0).

Ключевые слова: нейронные сети, генеративное обучение, система обнаружения вторжений, генетические алгоритмы, квазибиологическая парадигма.

Стоит отметить, что целью настоящей разработки является конструирование комплекса методологических и научно-технических решений для системы искусственного интеллекта (далее – ИИ), которая обеспечивает «жизнеспособность» и устойчивость к компьютерным атакам, направленным в основном на нарушение целостности прочих НС, в частности, [1]. Стоит заметить, что в данную идеологему входит и общее развитие таких НС, как части общей линейки строения современных систем ИИ (рис. 1).

Стоит в значительной степени отметить, что в структуре разрабатываемых СОВ уместны так называемые «генетические алгоритмы».

Для настоящего исследования, положенного в рамки развития интеллектуальной СОВ, должна присутствовать линейка имитации эволюции алгоритмов, которые улучшаются по мере тестирования и

видоизменения угроз от компьютерных атак. Разрабатывая СОВ в рамках «квазибиологической парадигмы», провоцируется появление генеративно-состязательной сети.

Рис. 1. Основные области, в которых задействован концепт ИИ в большинстве случаев

Такие сети могут обладать накапливаемой бинарной перекрестной энтропией [2], которые в процессе обучения дискриминатора вычисляют потери, которые могут допускаться, в случае успеха или, напротив, при совершении компьютерных атак.

$$-\frac{1}{n}\sum_{i=1}^{n}(y_i \log(p_i)+(1-y_i)\log(1-p_i)). \quad (1)$$

В процессе дальнейшего обучения имеет место стремление к добавлению особых генераторов, которые бы обеспечили потенциальные потери при работе интеллектуальных механизмов в СОВ [4]. Положительные генераторы для минимизации потерь в разрабатываемых интеллектуальных СОВ, будет считать по формуле

$$\min_D -(E_{x\sim p_x}[\log D(x)]+E_{z\sim p_z}[\log(1-D(G(z)))]). \quad (2)$$

В рамках «квазибиологический парадигмы» могут быть добавлены в общую технологизацию допустимые ограничения на развитие сверхсложных систем ИИ. Потому для целой концепции актуально динамическое развертывание (рис. 2).

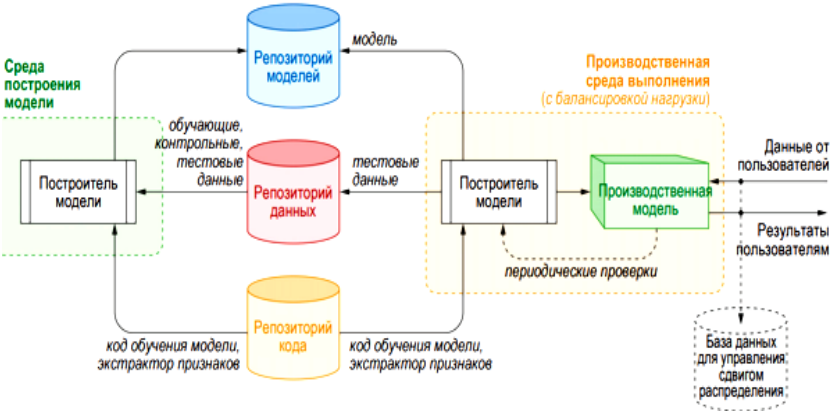


Рис. 2. Архитектура автоматизации развертывания
и сопровождения системы машинного обучения

Добавление балансировщиков нагрузки создаст прецедент для направления входящих запросов НС и дальнейшего перераспределения для реализации потребностей генеративного обучения [3]. Данное условие следует проверять при каждом запуске сервисов генетических алгоритмов в СОВ или потокового приложения и периодически во время работы.

Итого эффективная среда архитектуры должна обладать:

- безопасностью и корректностью, гарантиями правильности модели, легкостью развертывания и восстановления,
- отсутствием расхождений между ГО и МО, а также синхронизированным выполнением различных балансировщиков в системе ИИ.

ЛИТЕРАТУРА

1. Гэри Маркус. Искусственный интеллект: перезагрузка: Как создать машинный разум, которому действительно можно доверять / Гэри Маркус, Эрнест Дэвис; пер. с англ. – М.: Альпина ПРО, 2021.

2. Фостер Д. Генеративное глубокое обучение. Творческий потенциал нейронных сетей. – СПб.: Питер, 2020. – 336 с.

3. Бурков А. Инженерия машинного обучения / пер. с англ. А.А. Слинкина. – М.: ДМК-Пресс, 2022. – 306 с.

4. Ушаков И.А. Обнаружение инсайдеровв корпоративной компьютерной сети на основе технологий анализа больших данных // Вестник СПб. гос. ун-та технологии и дизайна. – Сер. 1: Естественные и технические науки. – 2019. – № 4. – С. 38–43.

УДК 004.934.2

ОПРЕДЕЛЕНИЕ ПСИХОЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ ДИКТОРА МЕТОДОМ ИЗВЛЕЧЕНИЯ И ОЦЕНКИ ПАТТЕРНОВ РЕЧЕВОГО СИГНАЛА С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА DTW

Б.О. Орлов, студент каф. БИС;
Харченко С.С., доцент каф. БИС, к.т.н.
г. Томск, ТУСУР, mrwiggle40000@gmail.com

Рассмотрен метод оценки психоэмоционального состояния на основе извлекаемых из речевого сигнала паттернов, выделенных из аудиозаписей открытого датасета RAVDESS, в частности: способ извлечения паттернов и алгоритм, позволяющий построить ассоциации с одним из основных эмоциональных классов на основе алгоритма DTW.

Ключевые слова: эмоция, психоэмоциональное состояние, распознавание паттернов, RAVDESS, DTW.

Проблема влияния эмоционального состояния на параметры речевого сигнала представляет большой научный интерес как в теоретическом плане, так и для решения различных прикладных задач. В их числе определение объективного состояния человека по звучанию его голоса в различных сферах деятельности, в частности, в психологии [1], в маркетинговом бизнесе, в криминалистике, в медицине [2]. Большинство способов классификации эмоций невозможны без использования искусственного интеллекта.

Используемый датасет. Собранные в реальном времени аудиозаписи спонтанной речи заметно ухудшают эффективность решения задачи, в то время как речь профессиональных актёров содержит ярко выраженный эмоциональный окрас [3]. Для тестирования работы алгоритма был использован речевой корпус RAVDESS [4]. Это проверенная база данных эмоциональной речи и песен. База данных гендерно сбалансирована и состоит из 24 профессиональных актеров, озвучивающих лексически подобранные высказывания с нейтральным североамериканским акцентом.

Датасет включает в себя аудиозаписи с выражением спокойствия, счастья, грусти, злости, страха, удивления и отвращения.

Алгоритм по получению паттернов. На языке Python были написаны три класса: Pitch_detect, Percents и Pattern. Все классы были объединены в одну программу, которая последовательно применяет их для составления паттерна конкретного аудиофайла по схеме: Аудиофайл → Массив частот (ЧОТ) → Массив процентов → Паттерн.

Количество литералов в паттерне будет равно количеству выделенных диапазонов перепадов ЧОТ. Литерал представляет собой не что иное, как символ любого существующего языка с соответствующей ему кодировкой. Соответственно, чем больше диапазонов перепадов ЧОТ будет выделено, тем точнее будет отражено изменение ЧОТ в последовательности литералов паттерна.

Следующий этап – получение массива процентов изменения ЧОТ на указанном интервале. Определенному диапазону перепада ЧОТ присваивается свой литерал, паттерн же представляет собой последовательность этих литералов, соответственно последовательность перепадов ЧОТ.

Метод ассоциации паттерна с эмоциональным классом. Ассоциация паттерна анализируемой аудиозаписи происходит следующим образом: полученный паттерн сравнивается с уже существующими в базе данных и ассоциированными с конкретным эмоциональным классом последовательностями литералов. После этого в каждом из классов выявляется последовательность, наиболее похожая на входную. Далее происходит сравнение коэффициентов схожести, и входному паттерну присваивается эмоциональный класс, в котором содержится последовательность, наиболее похожая на входную.

Существенной проблемой может являться то, что последовательности могут различаться по длине, состоять из очень большого запаса входных символов и могут потребовать от модели изучения долгосрочного контекста или зависимостей между символами во входной последовательности.

Итогом поиска информации о методах сравнения [6–8] стал выбор алгоритма динамической трансформации временной шкалы.

Реализация алгоритма динамической трансформации временной шкалы (DTW) и проведение экспериментов. Подразумевается, последовательность, поступающая на вход, будет сравниваться последовательно с каждым из паттернов в базе данных соответствующей эмоции. Сравнение двух паттернов происходит в два этапа:

– расчёт матрицы расстояний;

– расчет минимальных путей на основе матрицы расстояний.

В результате вычисляется метрика, позволяющая классифицировать паттерн в соответствующую эмоциональную группу.

Эксперименты проводились на базе группы аудиозаписей дикторов мужчин, произносящих фразы с ярким эмоциональным окрасом. В эксперименте использовались эмоции трех наиболее различимых между собой [9] эмоциональных групп: гнев, радость, спокойствие. Датасет, использующийся для тестирования, включает в себя записи

двадцати четырех дикторов мужчин и 576 паттернов аудиозаписей. Результаты эксперимента представлены на графиках, изображенных на рис. 1–3.

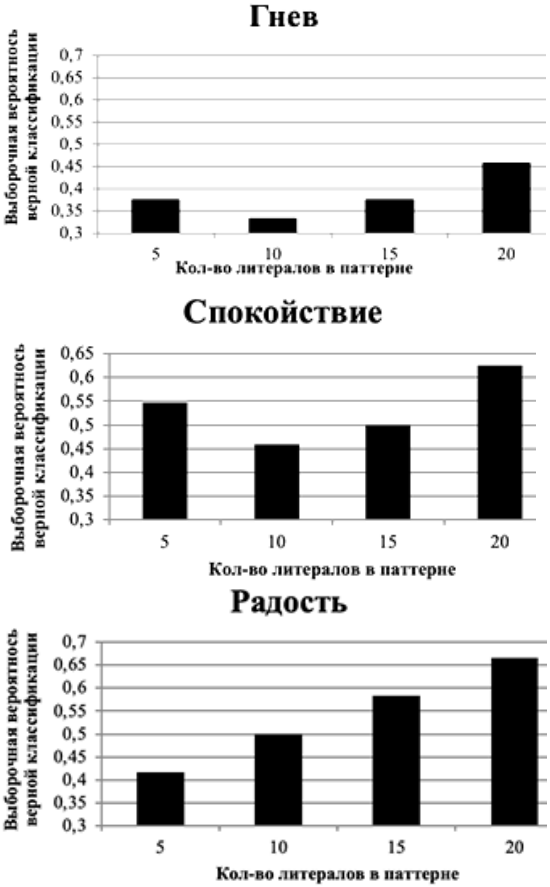


Рис. 1. Выборочная вероятность верной классификации эмоций «гев», «радость», «спокойствие» в зависимости от числа литералов в паттерне

Исходя из графиков, представленных выше, можно сделать следующие выводы:

– при малом количестве выделенных диапазонов перепадов ЧОТ вероятность верной классификации стремится к случайному значению;

– при увеличении количества выделенных интервалов ЧОТ вероятность верной классификации возрастает;

– наиболее точно классифицируются эмоции «радость» и «спокойствие».

Проблема с классификацией гнева может быть связана с тем, что часто эта эмоция ложно классифицировалась как «Радость», так как аудиозаписи с этими эмоциональными окрасами имеют схожее количество перепадов ЧОТ. Решением этой проблемы может стать увеличение числа паттернов в базе данных, что будет способствовать лучшей классификации, увеличению количества выделяемых диапазонов ЧОТ и изменению временного периода измерения перепадов ЧОТ.

ЛИТЕРАТУРА

1. Бутузова Ю.А Психологическая сущность эмоционального состояния личности // Омский научный вестник. – 2011. – № 5 (101). – С. 173–175.

2. Чуркин А.А. Распространенность психических расстройств в Российской Федерации в 2009 г. /А.А. Чуркин, Н.А. Творогова // Вестник неврологии, психиатрии и нейрохирургии. – 2011. – № 1. – С. 5–12.

3. Ле Нгуен Виен. Подходы к выделению речи из исходного сигнала для системы обработки речи / Нгуен Виен Ле, Д.П. Панченко. – Текст: непосредственный // Молодой ученый. – 2011. – № 5 (28), Т. 1. – С. 77–79. – URL: https://moluch.ru/archive/28/3172/

4. The Ryerson Audio-Visual Database of Emotional Speech and Song (RAVDESS): A dynamic, multimodal set of facial and vocal expressions in North American English [Электронный ресурс]. – Режим доступа: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0196391

5. Parselmouth – Praat in Python, the Pythonic way [Электронный ресурс]. – сайт Parselmouth. – URL: https://parselmouth.readthedocs.io/en/stable/

6. Senin P. Dynamic Time Warping Algorithm Review. – 2009.

7. Deza M.M., Deza E. Encyclopedia of Distances (англ.). – Fourth Edition. – Springer, 2016. – PP. 102–103.

8. Basseville M. Distance measures for signal processing and pattern recognition // Signal Processing. – 1989. – Vol. 18, No. 4. – PP. 349–369.

9. Tappert C.C., Das S.K. Memory and time improvements in a dynamic programming algorithm for matching speech patterns // IEEE Transactions on Acoustics. – Speech and Signal Processing. – 1978. – No. 26 (6). – PP. 583–586.

10. Орлов Б.О. Влияние эмоций на параметры речевого сигнала / Б.О. Орлов, С.В. Шенцова, Д.О. Дахалаева // Наука и практика: проектная деятельность – от идеи до внедрения: матер. IX рег. науч.-практ. конф., Томск, 2020. – Томск: ТУСУР, 2020. – С. 235–237.

11. Орлов Б.О. Распознавание эмоций по речевому сигналу используя паттерны спектрограмм как признак / Б.О. Орлов, С.В. Шенцова, Д.О. Дахалаева // Наука и практика: проектная деятельность – от идеи до внедрения: матер. X рег. науч.-практ. конф., Томск, 2021. – Томск: ТУСУР, 2021. – С. 317–319.

УДК 004.056.5

РАЗРАБОТКА СЦЕНАРИЯ КИБЕРАТАКИ «ЗАЩИТА КОМПАНИИ ОТ КРАЖИ ДЕНЕЖНЫХ СРЕДСТВ КОМПАНИИ ВНУТРЕННИМ НАРУШИТЕЛЕМ»

В.С. Репкин, Г.Ю. Семёнов, Н.И. Сермавкин, студенты
Научный руководитель А.А. Конев, доцент каф. КИБЭВС, к.т.н.
Проект ГПО КИБЭВС-1909. Интерактивная игра по управлению безопасностью
г. Томск, ТУСУР, kaa@fb.tusur.ru

Разработан сценарий кибератаки «Защита компании от кражи денежных средств компании внутренним нарушителем». На основе структуры построения методических указаний по прохождению сценариев от киберполигона Ampire было описано прохождение разработанного сценария. Было составлено формальное описание сценария с использованием методологии моделирования «Деревья атак».

Ключевые слова: сценарий кибератаки, киберполигон, ampire, формализованное описание, деревья атак.

Кибербезопасность является крайне актуальной темой в современном мире. С развитием технологий и увеличением количества цифровых устройств, которые мы используем в повседневной жизни, возникает всё больше уязвимостей и угроз в сфере информационной безопасности. В свете этого обучение специалистов по информационной безопасности является очень важным вопросом. Они должны понимать, какие уязвимости и угрозы существуют, какие методы и технологии используют киберпреступники и как защитить информацию от несанкционированного доступа и кибератак. Специалисты по информационной безопасности должны быть в курсе последних тенденций в кибербезопасности и постоянно совершенствовать свои навыки. Это важно для того, чтобы максимально быстро и эффективно реагировать на инциденты в случае их возникновения.

Для получения практических навыков был разработан киберполигон Ampire. В основе учений лежит сценарий – имитация реальной компьютерной атаки на инфраструктуру. Однако для того, чтобы обучение с помощью данной учебно-тренировочной платформы было актуальным, необходимо регулярно пополнять базу сценариев кибератак [1].

Целью работы является составление сценария кибератаки «Защита компании от кражи денежных средств компании внутренним нарушителем» с описанием его прохождения для его дальнейшего интегрирования в систему киберполигона Ampire. Также необходимо

формально описать созданный сценарий с помощью метода моделирования «Деревья атак» [2].

Сценарий – это шаги нарушителя для реализации недопустимого события в инфраструктуре компании. Сценарий обычно включает в себя шесть шагов: преодоление сетевого периметра, получение максимальных привилегий в доменной инфраструктуре, получение доступа в ключевые сегменты сети, к ключевым компьютерам и серверам, развитие атаки на целевые системы, реализация недопустимых событий. Для выполнения шагов злоумышленник эксплуатирует определенные уязвимости в инфраструктуре компании.

В общем случае для достижения конечной цели внутреннего нарушителя – кражи денежных средств компании нарушителю сначала необходимо проанализировать инфраструктуру организации. Далее – получить контроль над инфраструктурой (максимальные привилегии в домене). Получив контроль, нужно осуществить доступ к финансовым системам – сегменту бухгалтерии во внутренней сети компании (компьютеры, серверы) и похитить денежные средства.

Для данного сценария были определены три уязвимости: CVE-2021-40444 [3], CVE-2017-0199 [4] и автоматическая авторизация в корпоративную почту при запуске рабочей станции. Дерево атак для разработанного сценария представлено на рис. 1.

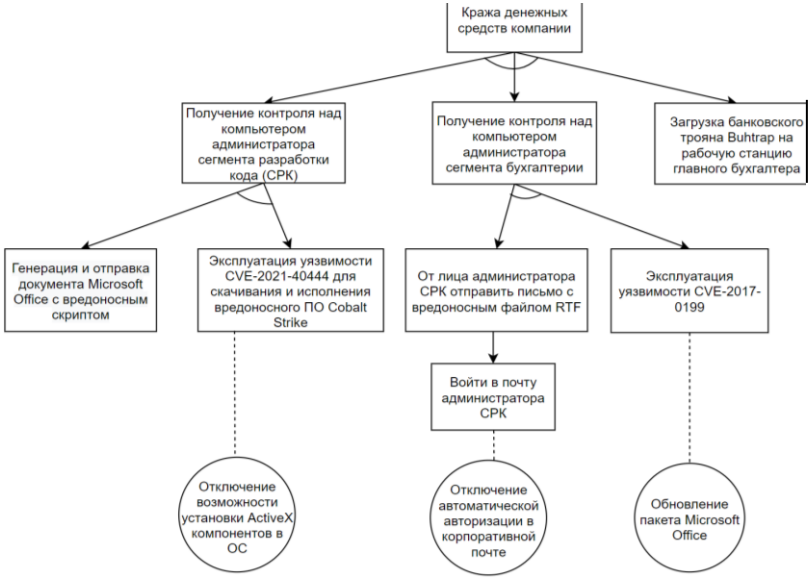


Рис. 1. Формальное описание сценария с помощью методологии «Деревья атак»

Деревья атак являются формальным методом моделирования реализации угроз информационной безопасности в отношении информационных систем. Атаки представляются в виде деревьев, где корнем является цель атаки, ближайшие узлы – подцелями, а листья – способами достижения подцелей и реализации атаки на основную цель. В кружках прописываются контрмеры.

Заключение. Разработка сценариев кибератак является перспективным направлением в области информационной безопасности. В ходе работы был описан сценарий кибератаки «Защита компании от кражи денежных средств компании внутренним нарушителем», а также составлено его формальное описание с использованием методологии моделирования «Деревья атак». Результаты работы, а именно созданный сценарий, планируется интегрировать в киберполигон Ampire.

ЛИТЕРАТУРА

1. Novokhrestov A. Computer network threat modelling / A. Novokhrestov, A. Konev, A.A. Shelupanov, A. Buymov // IOP Conf. Series: Journal of Physics: Conf. Series. – 2020. – Vol. 1488. – P. 012002.

2. Schneier on Security. Attack Trees [Электронный ресурс]. – Режим доступа: https://www.schneier.com/academic/archives/1999/12/attack_trees.html, свободный (дата обращения: 14.07.2022).

3. CVE. CVE-2021-40444 [Электронный ресурс]. – Режим доступа: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444, свобойдный (дата обращения: 14.07.2022).

4. CVE. CVE-2017-0199 [Электронный ресурс]. – Режим доступа: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199, свободный (дата обращения: 14.07.2022).

УДК 004.934.1

СРАВНЕНИЕ РЕЗУЛЬТАТОВ РАСПОЗНАВАНИЯ С ИСПОЛЬЗОВАНИЕМ KALDI ВЕРСИИ 0.1 И 0.22 ДЛЯ ЗАДАЧ ОЦЕНКИ КАЧЕСТВА РЕЧИ

С.В. Шенцова, студентка каф. БИС

Научный руководитель С.С. Харченко, доцент каф. БИС, к.т.н.

г. Томск, ТУСУР, svetlaying@gmail.com, kss@keva.tusur.ru

Представлены результаты сравнения распознавания Kaldi версии 0.1 и 0.22. В частности, проведение эксперимента по распознаванию с использованием двух версий, выдвижение гипотезы о статистической различимости результатов и проверка гипотезы с помощью статистического критерия Уилкоксона.

Ключевые слова: Kaldi, распознавание речи, оценка распознавания, реабилитация, программное обеспечение, критерий Уилкоксона.

В настоящее время направление распознавания речи – одна из самых популярных задач компьютерной лингвистики. Технологии распознавания сейчас используются повсеместно не только в бытовой жизни, но и в медицине [1]. На сегодняшнем этапе развития науки и техники оценка качества речи используется при диагностировании нейродегенеративных заболеваний [2], также стоят задачи по оценке качества эффективности реабилитаций после хирургического лечения злокачественных образований органов речи и шеи [3], при которых потеря голоса может грозить частичной или полной потерей трудоспособности, психологической изоляцией и трудностями в коммуникации [4]. Сложный характер заболеваний органов речи и реабилитации требует комплексной диагностики и длительного лечения. Коррекция нарушений голоса – проблема междисциплинарная, требующая участия не только врача-оториноларинголога. Ввиду этого вопросы изучения оценки качества речи являются актуальными на сегодняшний день.

Целью данной работы является сравнение результатов распознавания с использованием Kaldi [5] версии 0.22 и 0.1 [6] для повышения качества реабилитации пациентов после лечения онкологических заболеваний органов речеобразующего тракта.

Для качественной оценки реабилитации больных используется программное обеспечение на основе утилиты Kaldi. На рис. 1 представлен пример качественной оценки реабилитации одного пациента в течение трех сеансов. В столбцах D1, D2, D3 отражено значение расстояния Левенштейна для первого, второго и третьего сеанса соответственно.

Исходная фраза	Распознанная фраза 1	Распознанная фраза 2	Распознанная фраза 3	D1	D2	D3
Белая пелена лежала на полях	белую пузанов зажал он опоздал	да ты прав	да да зал зна	17	24	20
Солнце поднялось над лесом	солнце поднялось магнусом		сондра догнал нага	5	26	17
В подъезде стояли санитары	подъедешь твоё самое то	да	козла за рога сразу за	16	24	21
Стало известно место встречи	стой известному месту становище	ну	да	13	27	27
На участке ведется наблюдение	но шапкой волос на глубину	ну вот	на зар зав надо	19	24	20
В класс вошел преподаватель	ухват вошёл тупо да вот он	о	ахнуть поднос он полозова зовут	16	26	25
Полено раскололось надвое	подумал раскололась надвое	да но	повязав на	6	21	19
Надо зарядить ружье	надо зарядить ружье	но	назад завязнут	0	17	13
Телега начала скрипеть	загон начала скрипеть	ха ха	назад	6	19	19
Мать отвела ребенка в сад	мат а слова ребёнка фасад	мар	басом задал корм	10	22	21
Ребята сидели на берегу	ребята сидели на берегу	ага	да сэр	0	21	19
В школу приезжали герои фронта	о проезжали героя фронту		тоже знают о здрав	9	30	23
В магазине продаются яблоки	магазине подаются яблоков	но	но он же нравился заго	5	25	20
Директор сравнил доход с расходом	где ты в самом доход с восходом	браун	да да да с сыном	14	30	22
Высокая рожь колыхалась	высокая ров о хаос	вот оно	лицо овёс алёша	8	18	18
Цветы пестрели в долине	с этой пестрели вдолину	гм	фр	7	23	22
Чудный запах леса освежает	чудно запах роз от по служак	рогов	иза графа завеса зда	14	24	20
День был удивительно хорош	день был удивительно хорош	за бы фаллом	да да за	0	20	22
Белый пар расстилается над лужами	белый пар а стоя над лужину	да оно	да расплываются базу заодно	11	30	22
Экипаж танка понял задачу	экипаж танка он-от удачу	а	брута но по зал за залом	6	24	17
Этот блок работает хорошо	а тот блок обутую хорошо	да	это был сон	8	24	18
Начинаются степные пожары	начинался степного пожара	права	нас зайца	6	23	20
Ученики поливают огород	ученики побывал огород	ага	не знаю	4	21	19
Тяжелый подъем закончился	тяжёлую подъём закончился	она афар	озола позор зав са	4	22	17
Тропинка уперлась в глинистый уступ	тропинка пополз по полу глинистые уступом	то что вы	хав	15	29	33
			Среднее значение	8,76	23,8	20,6

Рис. 1. Пример качественной оценки реабилитации

В ходе работы был проведен эксперимент с использованием модели версии 0.1 и 0.22 при помощи программного обеспечения на основе утилиты Kaldi, для проведенияктороого использовались записи голоса с фразами из ГОСТ Р 50840–95 [7]. Результаты эксперимента представлены на рис. 2, где D – расстояние Левенштейна.

ИСХОДНАЯ ФРАЗА	Распознанная фраза Kaldi 1.0	Распознанная фраза Kaldi 2.0	D1	D2
Белая пелена лежала на полях	белая пелена лежала на паях	белая пелена лежал на паях	2	3
Солнце поднялось над лесом	солнце поднялось над лесом	солнце поднялось над лесом	0	0
В подъезде стояли санитары	а здесь здесь стоять	а ведь здесь стоять за это	19	15
Стало известно место встречи	стало известно место встречи	стало известно место встречи	0	0
На участке ведется наблюдение	на участке велось наблюдение	на участке велось наблюдение	4	4
В класс вошел преподаватель	за свои шутки подорвать и	нас вошёл преподаватель	19	6
Полено раскололось надвое	паяльная раскололась надвое	военно раскололась надвое	6	4
Надо зарядить ружье	надо зарядить ружье	надо зарядить проживёт	0	6
Телега начала скрипеть	ты я занята цветы	ты его начала скрипеть	15	3
Мать отвела ребенка в сад	мать ребёнка в сад	мать отца ребёнка в сад	8	4
Ребята сидели на берегу	видать посидеть на берегу	ребята сидели на берегу	9	0
В школу приезжали герои фронта	приезжай герои фронта	куплю нельзя и герои фронта	10	13
В магазине продаются яблоки	магазине продаются яблоки	магазине продаются яблоки	2	2
Директор сравнил доход с расходом	да я сравню доход расходам	диета сравнить да хоть расходам	12	12
Высокая рожь колыхалась	высокая русь хаоса	высокая русь полыхал и	9	6
Цветы пестрели в долине	цветы то есть две и да и	цветы быстрее да и не	13	9
Чудный запах леса освежает	судне запах и яйца освежает	чудный запах и яйца освежает	8	5
День был удивительно хорош	день был девять ты не права	день был удивительно	14	6
Белый пар расстилается над лужами	белый пар растирался зубьями	белый пак растерялся над жизням	12	12
Экипаж танка понял задачу	эти повстанцы понял задачу	эти повстанцы понял задачу	7	7
Этот блок работает хорошо	это зло работает	этот блог работает	10	8
Начинаются степные пожары	начинается пожар	начинается степные пожары	10	1
Ученики поливают огород	ученики поливают	ученики погибают ага вот	7	7
Тяжелый подъем закончился	ты зоны позовём закончился	ты зол и пойдём закончился	10	9

Рис. 2. Результаты экспериментов

После проведения экспериментов была выдвинута гипотеза о том, что распознавание речи с помощью программного обеспечения на основе утилиты Kaldi 0.22 выполнено лучше. Для проверки гипотезы и сравнения результатов был произведен расчет критерия Уилкоксона [8], который применяется для сопоставления показателей, измеренных в двух разных условиях на одной и той же выборке испытуемых, с помощью программного обеспечения SPSS Statistics [9]. Результат представлен на рис. 3.

Критерий знаковых рангов Вилкоксона

Ранги

		N	Средний ранг	Сумма рангов
V2.0 - V1.0	Отрицательные ранги	649[a]	444,13	288238,00
	Положительные ранги	181[b]	312,86	56627,00
	Совпадающие наблюдения	414[c]		
	Всего	1244		

a. V2.0 < V1.0
b. V2.0 > V1.0
c. V2.0 = V1.0

Статистические критерии[a]

	V2.0 - V1.0
Z	-16,793[b]
Асимп. знач. (двухсторонняя)	<,001

a. Критерий знаковых рангов Вилкоксона
b. На основе положительных рангов.

Рис. 3. Результаты сравнения

Из рис. 3 следует:

– отрицательные ранги: 649 значений модели Kaldi версии 0.22 меньше Kaldi версии 0.1;

– положительные ранги: 181 значение модели Kaldi версии 0.22 больше Kaldi версии 0.1;

– совпадающие наблюдения: 414 случаев, значения в которых двух версий программ Kaldi одинаковые.

Асимптотическая значимость составляет 0.001, что говорит о том, что вероятность ошибки первого рода равна 0,001 и не превышает 0,05 и что гипотеза о статистической различимости верна. Распознавание с использованием Kaldi версии 0.22 проводится эффективнее.

ЛИТЕРАТУРА

1. Бондаренко В.П. Программные средства комплекса исследования речевого сигнала при злокачественных заболеваниях гортани / В.П. Бондаренко, Е.Л. Чойнзонов, Л.Н. Балацкая // Медицинская техника. – 2009. – № 4. – С. 33–38.

2. Способ диагностики и реабилитации пациентов с нарушениями голосо-речевой функции [Электронный ресурс]. – Режим доступа: https://patents.google.com/patent/RU2738660C1/ru?inventor=%D0%9C%D0%B0%D1%80%D1%8C%D1%8F%D0%BC+%D0%AF%D1%85%D1%8A%D1%8F%D0%B5%D0%B2%D0%BD%D0%B0+%D0%A4%D0%B0%D1%82%D1%82%D0%B0%D1%85%D0%BE%D0%B2%D0%B0 (дата обращения: 20.11.2022).

3. Харченко С.С. Программный комплекс речевой реабилитации онкологических больных после резекции гортани / С.С. Харченко, Р.В. Мещеряков, Д.А. Вольф и др. // Медицинская техника. – 2016. – № 2. – С. 51–55.

4. Вельтищев Д.Ю. Психопатологические проблемы расстройства голоса / Д.Ю. Вельтищев, С.Г. Романенко, А.В. Стукало // Доктор.Ру. – 2011. – № 4 (63). – С. 63–69.

5. Kaldi [Электронный ресурс]. – Режим доступа: https://kaldi-asr.org/ (дата обращения: 15.09.2022).

6. Vosk model [Электронный ресурс]. – Режим доступа: https://alphacephei.com/vosk/models (дата обращения: 05.12.2022).

7. ГОСТ Р 50840–95. Государственный стандарт Российской Федерации. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200027288, (дата обращения: 05.12.2022).

8. Павлова В.Ю. Основные вопросы статистического анализа в медицинских исследованиях // Клиническая онкогематология. – 2009. – Т. 2, № 4. – С. 374–377.

9. SPSS Statistics [Электронный ресурс] – Режим доступа: https://www.ibm.com/products/spss-statistics (дата обращения: 06.12.2022).

УДК 004.056.53

МОДЕЛИРОВАНИЕ АТАК НА ФИЗИЧЕСКИЙ УРОВЕНЬ УСТРОЙСТВ IIOT

К.И. Цимбалов, аспирант каф. КИБЭВС; Д.С. Брагин, ст. преп. каф. ТОР; В.В. Мартышечкин, студент каф. БИС

Научный руководитель А.А. Конев, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, cki@nti.tusur.ru

Рассматриваются сценарии атак, направленные на нарушение целостности и доступности информации на физическом уровне устройств IIoT. Производится зашумление канала связи внешним генератором, а также производится дестабилизация канала связи магнитным полем.

Ключевые слова: IIoT, OSI, ПЛК.Ethernet.

На текущий момент промышленный интернет вещей (IIoT) интегрируется в различные сферы жизнедеятельности, которые требуют автоматизации [1]. Текущая технология позволяет масштабировать промышленные сети и системы, упрощая способы организации каналов связи между ними. В погоне за автоматизацией упускаются моменты, связанные с обеспечением информационной безопасности на физическом уровне.

В частности, существующие протоколы, которые используются в IIoT, не гарантируют целостность информации, а также доступность канала связи на физическом уровне [2]. Используя текущие недостатки, злоумышленник имеет возможность влиять на каналы передачи информации.

В рамках текущей работы производится исследование устойчивости канала связи в системе IIoT к атакам на физическом уровне.

Проблема безопасности IIoT. В соответствии с моделью OSI, на физическом уровне данные передаются в виде физических объектов (ток, свет, радиоволна). В качестве среды передачи могут выступать как проводные, так и беспроводные каналы связи. Возможность влияния на среду передачи данных является ключевой проблемой безопасности [2, 3]. Используя, например, наводку побочного электромагнитного импульса, имеется возможность нарушить доступность канала связи, а также целостность передаваемой информации.

Планирование эксперимента. Для проведения исследования были определены сценарии атак, в рамках которых нарушаются конфиденциальность, целостность информации на физическом уровне.

В рамках атак производилось зашумление канала связи с помощью внешнего генератора, проверялась возможность влияния на систему передачи с помощью внешнего магнитного поля.

Для моделирования атак был реализован стенд, который имитирует работу системы IIoT. Структурная схема стенда представлена на рис. 1.

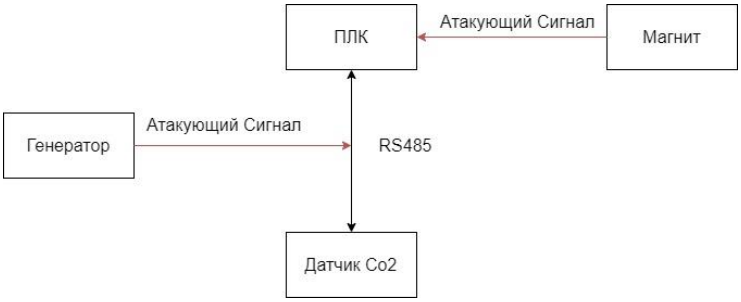


Рис. 1. Структурная схема стенда

Как видно из рис. 1, стенд состоит из программируемого логического контроллера (ПЛК) и датчика Co2. В качестве протокола передачи используется Modbus RTU. Канал связи был организован с помощью интерфейса RS 485.

Зашумление канала связи внешним генератором. В рамках текущего сценария атаки производилось зашумление канала связи генератором, который подавал в канал сигналы с напряжением от 1 до 1,5 В с шагом 0,5 В и различной частотой в течение одной минуты. В зависимости от уровня сигнала частота изменялась от 10 до 70 кГц. По результатам проведения атаки определялось количество ошибок в единицу времени, равную 1 с.

Полным отказом канала связи являлось количество ошибок за одну минуту, равное 60.

На рис. 2 представлена зависимость количества ошибок от частоты атакующего сигнала.

Как видно из рис. 2, при увеличении частоты атакующего сигнала возрастает количество ошибок при передаче. При моделировании атаки с уровнем сигнала, равным 1 В, отказ канала связи происходит на частоте 70 кГц. После увеличения уровня сигнала до 1,5 В отказ происходит при частоте 40 кГц.

Из полученных данных можно сделать вывод о том, что рассматриваемая система не устойчива к атаке зашумления канала связи внешним генератором, так как нарушается целостность информации и доступность канала связи.

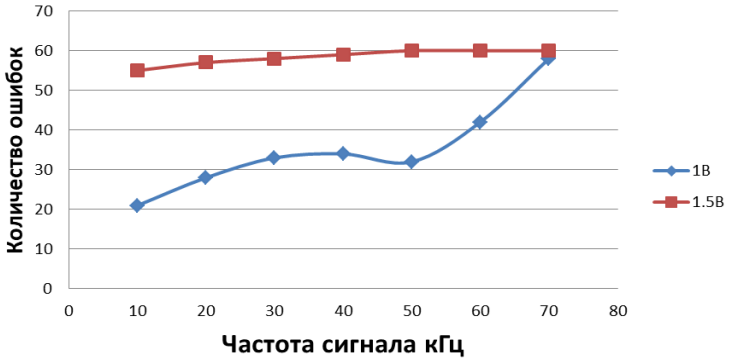


Рис. 2. Зависимость количества ошибок от частоты атакуемого сигнала

Дестабилизация канала магнитным полем. В данном сценарии атаки проверялась возможность дестабилизации канала связи при помощи поискового двухстороннего магнита Forceberg F400x2. Для этого магнит наводился в область Ethernet порта ПЛК. В результате чего пропадала связь с программируемым логическим контроллером, а также останавливалась передача данных по интерфейсу Ethernet.

Заключение. По результатам, полученным в рамках моделирования атак, можно сделать вывод о том, что имеющаяся система не устойчива к атакам на физический уровень. При изменении параметров атакуемого сигнала или среды передачи количество ошибок растет, что постепенно приводит к полному отказу канала связи.

ЛИТЕРАТУРА

1. Shelupanov A. Threat Model for IoT Systems on the Example of OpenUNB Protocol / A. Shelupanov, A. Konev, T. Kosachenko, D. Dudkin // International Journal of Emerging Trends in Engineering Research. – 2019. – Vol. 7, No. 9. – PP. 283–290.

2. Kalinin E. IoT Security Mechanisms in the Example of BLE / E. Kalinin, D. Belyakov, D. Bragin. A. Konev // Computers. – 2021. – Vol. 10, Is. 12. – 162 p.

3. Novokhrestov A. Computer network threat modelling / A. Novokhrestov, A. Konev, A.A. Shelupanov, A. Buymov // IOP Conf. Series: Journal of Physics: Conf. Series. – 2020. – Vol. 1488. – P. 012002.

УДК 004.89

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ В ЖУРНАЛАХ МОНИТОРИНГА СОСТОЯНИЯ ОБЪЕКТА ЗАЩИТЫ

Н.М. Башмаков, аспирант каф. ВТиЗИ; В.В. Уразаев, магистрант; А.М. Вульфин, доцент каф. КУДР, д.т.н.

Научный руководитель В.М. Картак, зав. каф. ВТиЗИР, д.ф.-м.н.

г. Уфа, УУНиТ, KVmail@mail.ru

Рассматривается возможность обнаружения аномалий в журналах регистрации событий средств защиты информации при условии, что сама инфраструктура представляет собой «черный ящик». В качестве возможного решения предлагаются алгоритмы кластеризации данных и методы линейного программирования.

Ключевые слова: информационная безопасность, анализ журналов регистрации событий, выявление аномалий, машинное обучение.

Несмотря на усилия специалистов в области информационной безопасности и развитие средств защиты, успешные компьютерные атаки на корпоративные информационные системы продолжают происходить, растет квалификация злоумышленников и наносимый ими ущерб. Так, в 2019–2022 г., согласно отчету компании Positive Technologies, значительно возросло общее количество атак [1], а также количество атак на информационную инфраструктуру промышленных предприятий [2].

В связи с кадровым голодом в области информационной безопасности ведущие эксперты области прогнозируют повышение спроса на технологии обеспечения информационной безопасности с высокой степенью автоматизации и предполагают, что обнаружение компьютерных атак и реагирование на них может быть возложено на искусственный интеллект [3–5]. Еще одна трудность – использование множества средств защиты информации, генерирующих множество различных оповещений и событий. Следствием этого является перегруженность специалистов, которые оказываются не в состоянии адекватно и своевременно выявлять инциденты и реагировать на них. Даже использование SIEM-систем не является гарантией эффективной интеграции оповещений от всех средств защиты информации и прочих систем – они, в свою очередь, тоже требуют настройки и сопровождения правил корреляций, индивидуальных для каждой конкретной организации. В связи с этим многими специалистами высказывается предположение, что повысить эффективность обнаружения инцидентов информационной безопасности можно, воспользовавшись методами искусственного интеллекта.

Предполагается, что операторы средств защиты информации в основном занимаются анализом журналов регистрации событий. Однако практика показывает, что по ряду причин это может быть невозможно, а если и возможно, то часто неэффективно. В таком контексте перспективной выглядит идея возложить анализ таких журналов на системы искусственного интеллекта.

С помощью методов интеллектуального анализа и машинного обучения (автоматическая классификация – кластеризация) предлагается выделять аномальные записи журнала регистрации событий (ЖРС). Под аномалией понимаются отклонения в функционировании конечных систем или отклонения, связанные с нарушением взаимодействия устройств при обмене данными в составе информационной системы [7,8].

Целью исследования является повышение эффективности обнаружения инцидентов информационной безопасности за счет использования методов машинного обучения при анализе журналов регистрации событий.

Задачи:

1. Анализ существующих решений в задачах выявления аномалий состояния конечных систем в составе корпоративной сети на основе автоматической классификации журналов регистрации событий.
2. Разработка структурно-функциональной организации системы анализа журналов регистрации событий для выявления аномалий состояния.
3. Разработка модели анализа журналов регистрации событий на основе методов автоматической классификации.
4. Оценка эффективности предложенного решения в задаче обнаружения аномальных состояний при анализе журналов регистрации событий.

Анализ существующих решений в задаче обнаружения аномалий в журналах мониторинга состояния. Одним из рассматриваемых подходов к анализу журналов событий является выявление в них аномальных событий. При этом предполагается первоначальное выявление значимой информации из записей в журналах в ходе разбора текстовых файлов – парсинг.

Исследователи в работе [9] отмечают, что существующие методы основаны на допущении, что данные журнала стабильны во времени, а набор различных событий журнала известен. Однако исследование показывает, что на практике данные журналов часто содержат ранее не встречающиеся события или последовательности событий. Нестабильность данных журнала возникает по двум причинам: эволюция

операторов регистрации и шум предобработки данных журнала. Предложен подход к обнаружению аномалий на основе журналов LogRobust, который извлекает семантическую информацию о событиях журнала и представляет их в виде семантических векторов.

Затем для обнаружения аномалий используется нейросетевая модель Bi-LSTM, основанная на механизмах внимания, которая может накапливать контекстную информацию из последовательностей журналов и автоматически определять важность различных событий журнала. Выполнена оценка модели LogRobust, используя журналы, собранные из системы Hadoop и реальной системы онлайн-сервисов Microsoft. Экспериментальные результаты показывают, что предлагаемый подход может решить проблему обнаружения новых событий и получить надежные результаты на реальных, постоянно меняющихся данных ЖРС.

В статье [9] предложен метод анализа неструктурированных журналов для обнаружения аномалий. Предложен алгоритм для преобразования текстовых сообщений произвольной формы в файлах журнала в ключи журнала. После преобразования сообщений журнала в ключи журнала строится машина состояний (FSM) из обучающих последовательностей журнала, чтобы представить нормальный рабочий процесс для каждого компонента системы. С помощью предложенных моделей имеется возможность автоматически обнаруживать аномалии в новых файлах журнала. Эксперименты с Hadoop и SILK показывают, что этот метод может эффективно обнаруживать текущие аномалии.

В работе [10, 11] предложен подробный обзор и оценка шести современных методов обнаружения аномалий на основе журналов, включая три контролируемых метода и три неконтролируемых метода, а также набор инструментов с открытым исходным кодом, упрощающий повторное использование. Эти методы были оценены на двух общедоступных наборах данных журналов. Даны рекомендации по применению моделей машинного обучения в задачах анализа ЖРС и рекомендации для дальнейшего развития моделей.

В работе [12] предложена DeepLog – модель глубокой нейронной сети, использующая долговременную кратковременную память (LSTM) для моделирования системного журнала в виде последовательности на естественном языке. Это позволяет DeepLog автоматически изучать шаблоны журналов и обнаруживать аномалии, когда шаблоны журналов отклоняются от модели, обученной на основе данных журнала при обычном выполнении. Показано, как поэтапно обновлять модель DeepLog в режиме онлайн, чтобы она могла адап-

тироваться к новым шаблонам журналов. Обширные экспериментальные оценки журналов показали, что DeepLog превзошел другие существующие методы обнаружения аномалий на основе журналов, основанные на традиционных технологиях интеллектуального анализа данных.

Таким образом, современные исследования в задаче обнаружения аномалий работы системы на основе анализа ЖРС активно применяют методы и модели машинного обучения в варианте контролируемого и неконтролируемого обучения.

Разработка структурно-функциональной организации системы обнаружения аномалий. Парсинг производился с использованием языка программирования Python. В том случае, если необходимо было первоначальное извлечение значимой части из сообщения SYSLOG, использовалась библиотека pygrok, реализующая для языка Python возможности использования grok-выражений. Grok-выражения являются некоторым развитием регулярных выражений и широко применяются в ELK-стеке.

Следующим шагом данные преобразовывались в формат JSON, который представляет собой набор названий полей и их значений, причем поля могут быть вложенными. Впрочем, в нашем случае вложенные поля не использовались.

После парсинга сообщения блоками конвертировались в структуру Pandas DataFrame и записывались в файловую систему в формате parquet для более компактного хранения. На следующем этапе были предприняты попытки выделить из получившихся данных значимую информацию в сообщениях.

Был получен ряд признаков, которые можно было проанализировать с точки зрения обнаружения аномалий. Далее все признаки были сведены в таблицу, а затем были проанализированы. После этого были выделены те признаки, которые могут быть использованы с точки зрения выявления аномалий. В экспериментах же использовался дополнительно усеченный набор признаков: **SessionID** (ID сессии), **Packets** (количество пакетов, переданных в рамках одной сессии), **Elapsed time in seconds** (время сессии), **cnt** (количество сессий), **spt** (порт источника), **dpt** (порт назначения), **src** (ip-адрес источника сетевого пакета), **dst** (ip-адрес назначения сетевого пакета), **proto** (протокол транспортного уровня), **out** (количество байт переданных в рамках одного сеанса от ip-адреса источника ip-адресу назначения), **in** (количество байт, переданных в рамках одного сеанса от ip-адреса назначения ip-адресу источника), **bytesflexNumber1** (in+out).

Используя оценку корреляции Пирсона для группы выделенных признаков, оценили степень линейной связи между численными признаками. Коэффициент корреляции больше заданного порога (например, 0,75) позволил исключить зависимые признаки и сократить результирующий вектор признаков.

На следующем шаге выполняется кодирование выделенного набора признаков: категориальных и числовых типов. Оценка отношения суммы внутрикластерных расстояний к сумме межкластерных расстояний позволяет оценить приемлемое количество кластеров в наборе данных.

Однозначно определить количество кластеров при прямолинейном применении кластеризации к образцам записей ЖРС с непреобразованным вектором признаков большой размерности не удалось. Применение преобразования T-SNE и UMAP для понижения размерности признакового пространства позволяет спроецировать записи журнала в пространство признаков меньшей размерности и визуализировать кластерную структуру.

К набору записей в пространстве признаков, преобразованному с помощью UMAP, применен алгоритм кластеризации HDBSCAN, не требующий предварительного задания количества кластеров и позволяющий с помощью пороговой величины определить образцы, существенно отстоящие от центров выделенных кластеров. Величина порога определяется из анализа гистограммы плотности распределения записей ЖРС. Для анализируемого набора данных порог выбран как $k = 0{,}75$.

Заключение. В ходе работы был проведен анализ существующих решений в задачах выявления аномалий состояния конечных систем в составе корпоративной сети на основе автоматической классификации журналов регистрации событий.

Разработана структурно-функциональная организация системы анализа журналов регистрации событий для выявления аномалий состояния. Была осуществлена разработка модели анализа журналов регистрации событий на основе методов автоматической классификации.

Подготовлена программная реализация предлагаемых подходов к обнаружению аномальных событий из ЖРС, проведено испытание на ЖРС реальной информационной инфраструктуры. Оценки на тестовых данных подтверждают обоснованность предложенного подхода и предоставляют обширный инструментарий. Оценка эффективности предложенного решения требует интерпретации получающихся результатов с привлечением специалистов, непосредственно ответ-

ственных за эксплуатацию, СЗИ, журналы которых использовались в работе. Это является следующим этапом исследования.

ЛИТЕРАТУРА

1. Актуальные киберугрозы: IV квартал 2022 года [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/

2. Актуальные киберугрозы для промышленных организаций: итоги 2022 года [Электронный ресурс] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/#id4

3. Таров Е.В. Искусственный интеллект в защите информации // Инновации. Наука. Образование. – 2021. – № 31. – С. 434–438.

4. Симаворян С.Ж. и др. О концепции создания интеллектуальных систем защиты информации на основе нейросетевых систем обнаружения вторжений в АСОД // Программные системы и вычислительные методы. – 2019. – №. 3. – С. 30–36.

5. Ковун В.А., Каширина И.Л. Применение методов машинного обучения в задачах обеспечения кибербезопасности // Актуальные проблемы прикладной математики, информатики и механики. – 2019. – С. 233–239.

6. Зегжда Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – М.: Горячая Линия-Телеком, 2020. – 560 с.

7. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic control and computer sciences. – 2016. – Vol. 50, № 8. – PP. 673–681.

8. Zhang X. et al. Robust log-based anomaly detection on unstable log data // Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. – 2019. – PP. 807–817.

9. Fu Q. et al. Execution anomaly detection in distributed systems through unstructured log analysis // 2009 ninth IEEE international conference on data mining // IEEE, 2009. – PP. 149–158.

10. Yadav R.B. A survey on log anomaly detection using deep learning / R.B. Yadav, P.S. Kumar, S.V. Dhavale // 2020 8th Interna-tional Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). – IEEE, 2020. – PP. 1215–1220.

11. He S. et al. Experience report: System log analysis for anomaly detection // 2016 IEEE 27th international symposium on software reliability engineering (ISSRE). – IEEE, 2016. – PP. 207–218.

12. Du M. et al. Deeplog: Anomaly detection and diagnosis from system logs through deep learning // Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. – 2017. – PP. 1285–1298.

УДК 004.923.2

СТЕГОАНАЛИТИЧЕСКИЙ КОМПЛЕКС ДЛЯ РАБОТЫ С ИЗОБРАЖЕНИЯМИ С НИЗКОЙ СТЕГОНАГРУЗКОЙ

Д.Э. Вильховский, ассистент каф. информационной безопасности
г. Омск, Омский государственный университет им. Ф.М. Достоевского (ОмГУ)

Представлен разработанный автором стегоаналитический программный комплекс, позволяющий производить стегоанализ цветных изображений и изображений в градациях серого с целью повышения уровня информационной безопасности организации. Комплекс осуществляет стегоатаку на такие методы стеганографии как метод Коха–Жао и метод LSB-замены. Показывает высокую эффективность обнаружения встраивания и локализацию области встраивания при работе с низким уровнем стегонагрузки.
Ключевые слова: стегоанализ, стеганографический анализ, анализ стегоконтейнера, стегоатака, обнаружение встраиваний, обнаружение LSB-вставки, обнаружение DCT-вставки, обнаружение вставки Коха–Жао.

Несмотря на развитие и эффективность новых методов и алгоритмов стеганографии, все еще широко используются такие методы стеганографии, как метод Коха–Жао [1] и метод LSB-замены (замены наименее значащих бит) [2]. В рамках встраивания в изображения первый работает с пространственной областью, второй – с частотной. Кроме того, злоумышленники стараются обойти существующие методы обнаружения встраивания, снижая уровень наполнения стегоконтейнера. Для противодействия обозначенным выше методам, а также практики низкого заполнения стегоконтейнера автором создан специальный программный стегоаналитический комплекс, работающий как с изображениями в градациях серого, так и с цветными изображениями и обладающий высокой чувствительностью.

Функционал разработанного программного комплекса. Ниже представлена общая характеристика функционала разработанного программного комплекса. В основе функционала положены алгоритмы стегоанализа изображений в противодействие методам LSB-замены и метода Коха–Жао, обладающие высокой чувствительностью к стеговставкам малого объема [3–5].

Функционал обнаружения встраиваний, выполненных методом Коха–Жао. Алгоритм обнаружения стеганографических вставок, выполненных методом Коха–Жао, имеет возможность обнаружить области их расположения как в черно-белых, так и в цветных изображениях. Работает с низким уровнем стеганографической нагрузки –

10–25% от общего объема стегоконтейнера. В основе алгоритма лежит использование двух сигнатур и методов кластеризации с использованием алгоритма DBSCAN [6] имеющейся последовательности коэффициентов дискретного косинусного преобразования, при которой выделяется кластер, в котором содержатся элементы последовательности, единообразно достаточные условиям, заданным по каждой из сигнатур.

Функционал обнаружения встраиваний, выполненных методом LSB-замены. Функционал обнаружения встраиваний, выполненных методом LSB-замены, является двухкомпонентным.

Первая компонента призвана работать с искусственными изображениями, в том числе и с изображениями, имеющими градиентную заливку. Производится последовательный анализ комбинаций пикселей в нулевом слое с целью выявления областей, содержащих повторяющиеся последовательности. Далее с использованием задачи о наибольшем пустом прямоугольнике [7] формируется область подозрительных значений (предполагаемая область встраивания), которая последовательно обрабатывается специально разработанным фильтром для исключения случайно-ложных результатов.

Вторая компонента призвана работать с фотографическими изображениями. Анализирует признаки попарного сходства между нулевым и первым слоями и выделяет подозрительные области при помощи задачи о наибольшем пустом прямоугольнике. После чего подключает разработанную автором модель доминирования пикселей и моментов изображения для дополнительной верификации подозрительной области и отсечения чистых областей, входящих в нее.

Общие принципы работы стегоаналитического программного комплекса. Предложенный стегоаналитический программный комплекс разработан на основе микросервисной архитектуры с использованием GET/POST-запросов. Данный программный комплекс может функционировать в виде отдельного приложения либо может быть интегрирован в CRM-систему в виде модуля.

Анализируемое изображение подается одним из двух способов: загружается из локального компьютера или загружается из сети Интернет по указанному URL-адресу.

Результат стеганографического анализа, возвращаемого программным комплексом, – ответ о наличии/отсутствии встраивания и локализация области встраивания при обнаружении.

Более подробно общая схема работы данного программного комплекса представлена в работе [8].

Точность стегоаналитического программного комплекса. Точность разработанного стегоаналитического программного комплекса на предмет обнаружения и локализации DCT-вставок (встраиваний, осуществленных методом Коха–Жао) и LSB-вставок (встраиваний, осуществленных методом LSB-замены) представлена, соответственно, в табл. 1 и 2.

Таблица 1

Точность стегоаналитического программного комплекса (обнаружение встраиваний), %

Уровень стегонагрузки	Boss Base		INRIA	
	Вставки			
	LSB	DCT	LSB	DCT
Изображения без встраивания	TN = 96,6 FP = 3,4	TN = 95,8 FP = 4,2	TN = 92,5 FP = 7,5	TN = 98,2 FP = 1,8
25%	TP = 88,53 FN = 11,47	TP = 96,1 FN = 3,9	TP = 84,3 FN = 15,7	TP = 98,8 FN = 1,2
10%	TP = 69,07 FN = 30,93	TP = 95,9 FN = 4,1	TP = 65,1 FN = 34,9	TP = 98,6 FN = 1,4
В среднем по изображениям со встраиванием	TP = 78,8 FN = 21,2	TP = 96,0 FN = 4,0	TP = 74,7 FN = 25,3	TP = 98,7 FN = 1,2

Таблица 2

Точность стегоаналитического программного комплекса (локализация встраиваний), %

Уровень стегонагрузки	Boss Base		INRIA	
	Вставки			
	LSB	DCT	LSB	DCT
25%	92,37	98,11	90,95	98,57
10%	85,47%	96,88	83,12	97,16
В среднем по изображениям со встраиванием	88,92%	97,50	87,04	97,87

При проведении эксперимента по стегоатаке на метод LSB-замены встраивания в изображения были осуществлены поочередно в каждую из трех компонент (красную, зеленую, синюю). Представленные в таблице данные по результативности являются средними значениями, полученными при работке с тремя компонентами.

Полученные данные показывают высокую эффективность работы программного комплекса. Алгоритмы, лежащие в основе бизнес-логики комплекса, выдают минимальную ошибку (FP – false positive, т.е. изображения, ошибочно определенные как имеющие встраивание) при работе с изображениями без встраивания, правильно классифицируя изображения без встраивания (TN – true negative, т.е. изображения, правильно определенные как чистые, без встраивания).

Лежащие в основе алгоритмы показывают высокую точность обнаружения встраиваний (TP – true positive, т.е. изображения, правильно определенные как стегоизображения) и, соответственно, невысокий процент ошибок (FN – false positive, т.е. изображения, ошибочно определенные как чистые).

Стегоатака на метод Коха–Жао показывает большую точность по сравнению с результатами стегоатаки на метод LSB-замены как по точности обнаружения встраивания, так и по точности локализации обнаруженных стего-вставок, что обусловлено особенностями метода Коха–Жао. При этом точность стегоатаки на метод Коха–Жао практически не показывает зависимости от уровня заполнения стегоконтейнера. В обличие от него, стегоатака на метод LSB-замены, хотя и показывает высокую эффективность в целом, фиксирует снижение точности классификации при снижении уровня стегонагрузки, что обусловлено более высокой сложностью LSB-замены как метода стеганографии.

Выводы. Предложенный стегоаналитический программный комплекс, работающий на основе разработанных автором алгоритмов стегоанализа, при интеграции в бизнес-процессы документооборота организации любого профиля позволяет выстроить эффективную систему защиты от несанкционированной передачи данных, что способствует повышению информационной безопасности организации.

ЛИТЕРАТУРА

1. Koch E. Towards robust and hidden image copyright labeling / E. Koch, J. Zhao // IEEE Workshop on Nonlinear Signal and Image Processing. – 1995. – PP. 452–455.

2. Luo W. Edge Adaptive Image Steganography Based on LSB Matching Revisited / W. Luo, F. Huang, J. Huang // IEEE Trans. Information Forensics & Security. – 2010. – Vol. 5(2). – PP. 201–214.

3. Вильховский Д.Э. Метод обнаружения LSB-вставок в цветных фотографических изображениях с низким заполнением стегоконтейнера // Проблемы информационной безопасности. Компьютерные системы. – 2022. – № 1 (49). – С. 68–76.

4. Вильховский Д.Э. Метод обнаружения стеганографических вставок, встроенных методом Коха–Жао, в изображениях с низким заполнением стегоконтейнера // Вопросы защиты информации. – 2022. – № 1 (136). – С. 38–42.

5. Вильховский Д.Э. Метод обнаружения LSB-вставок в искусственных цветных изображениях с градиентной заливкой с низким заполнением стегоконтейнера / Д.Э. Вильховский, А.К. Гуц // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 1 (43). – С. 43–49.

6. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn, Keras и TensorFlow: концепции, инструменты и техники для создания интел-

лектуальных систем. – 2-е изд.; пер. с англ. – СПб.: ООО «Диалектика», 2020. – 1040 с.

7. Acharyya A. Variations of largest rectangle recognition amidst a bichromatic point set / A. Acharyya, M. De, C. Subhas, S. Pandit // Discrete Applied Mathematics. – 2020. – Vol 286. – PP. 35–50.

8. Гуц А.К. Стегоанализ цветных изображений с низким заполнением стегоконтейнера с использованием программного комплекса / А.К. Гуц, Д.Э. Вильховский // Математические структуры и моделирование. – 2020. – № 4 (56). – С. 103–111.

УДК 004.056

МЕТОДИКА ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ ЭЛЕМЕНТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРИМЕНИТЕЛЬНО К УСЛОВИЯМ ВОЗДЕЙСТВИЯ DDOS-АТАК

И.В. Виноградов, студент каф. ИБ

Научный руководитель В.А. Воеводин, доцент каф. ИБ, к.т.н.

г. Москва, г. Зеленоград, НИУ МИЭТ, ivanvinogradov1111@gmail.com

Рассмотрено применение метода Монте–Карло к решению задачи выявления и оценки защищенности от DDoS-атак слабых узлов информационной инфраструктуры. В условиях DDoS-атак поток запросов атаки не является стационарным, поэтому известные аналитические модели дают значительную погрешность. Разработанная методика применима для моделирования DDoS-атак, направленных на элементы информационной инфраструктуры, с целью оценки их функциональной устойчивости.

Ключевые слова: имитационное моделирование, метод Монте–Карло, DDoS-атака, функциональная устойчивость, оценка функциональной устойчивости.

В результате анализа среды киберпреступлений было выявлено, что одной из распространенных компьютерных атак является атака типа «отказ в обслуживании». В случае проведения такой атаки несколькими распределенными источниками ее позиционируют как DDoS-атаку [1, 2]. Принятие мер по защите от названной атаки является актуальной задачей органов управления информационной безопасностью (ИБ).

Классификация DDoS-атак. DDoS-атаки различаются по воздействию, а также по уровню реализации [3]. На основе классификации был проведен анализ программных средств [4, 5] стресс-тестирования и применяемых на практике инструментов злоумыш-

ленников. Результаты анализа позволяют утверждать, что абсолютное большинство ресурс-ориентированных атак проводится на уровне приложений, а атаки на пропускную способность канала проводятся на транспортном и сетевом уровнях. На рис. 1 и 2 представлены графики одних из самых масштабных в мире DDoS-атак за 2019 и 2020 г. соответственно, проходящие через CDN сеть Imperva. Из рис. 1 и 2 видно принципиальное отличие атаки на ресурсы от атаки на пропускную способность. В первом случае (рис. 1) атака основывается на сложности обработки запросов, во втором (рис. 2) – на частоте поступающих запросов в единицу времени.

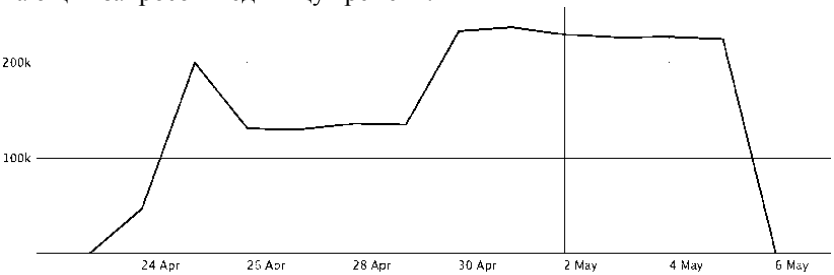


Рис. 1. График RPS (запросов в секунду) при DDoS-атаке на ресурсы. Поток на пике – около 292000 RPS

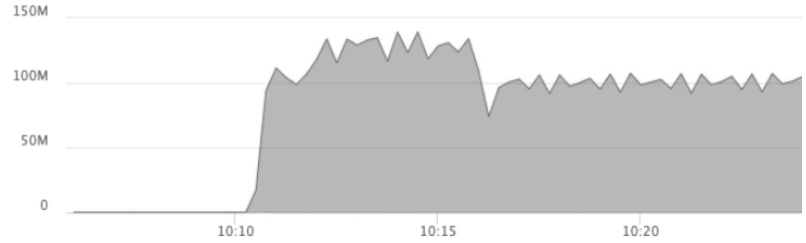


Рис. 2. График RPS при DDoS-атаке на пропускную способность. Поток на пике – около 140000000 RPS

Информационная инфраструктура как объект DDoS-атаки. Результаты анализа организации компьютерных сетей как объекта DDoS-атаки представлены на рис. 3.

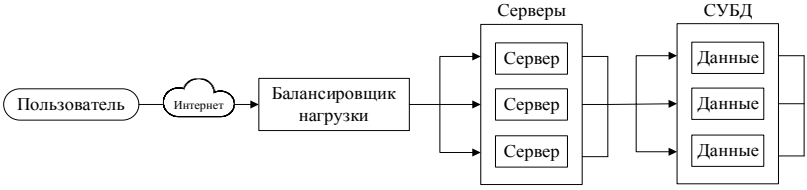


Рис. 3. Общая схема организации компьютерной сети

Успешность DDoS-атаки находится в зависимости от выбора режима работы балансировщика нагрузки, в качестве которого может выступать как внешний сервер, не принадлежащий организации, в том числе целая сеть серверов, так и внутренний сервер организации. Задача балансировщика – распределить входящие в сеть запросы между внутренними серверами организации. Для этого, как правило, используется метод балансировки «Least Connections» [6]. В этой связи при моделировании запросы перенаправляются на узлы, которые имеют меньше активных соединений в данный момент времени.

Для моделирования сервер был представлен как элемент в системе массового обслуживания (СМО), а сама компьютерная сеть – как сеть массового обслуживания. Запросы, поступающие на сервер, рассматривались как поток заявок, который может содержать как полезные, так и ложные запросы (DDoS-атаки).

Частота появления заявок характеризуется интенсивностью их поступления λ, число обслуженных заявок за единицу времени – интенсивностью их обслуживания μ. Отношение λ к μ позиционируется как интенсивность нагрузки СМО и обозначается буквой ρ. В условиях рассматриваемой задачи модель была описана как многоканальная система с ограниченной очередью и ограниченным временем ожидания в очереди [7]. В рамках модели обслуживание заявок происходит по принципу FIFO [8].

Вербальная модель обслуживания была представлена следующим образом. Пусть на сервер поступают заявки с некоторой интенсивностью λ. При функционировании в штатном режиме закон распределения входного потока этих заявок можно рассматривать как пуассоновский на достаточно большом промежутке времени. Обслуживание поступивших заявок происходит с интенсивностью μ. В качестве обслуживающих каналов выступают процессы-обработчики. Очередь заявок соответствует очереди запросов, приходящих на сервер. Если все каналы и места в очереди заняты, наступает отказ, что соответствует переполнению очереди запросов на реальном сервере и наступлению ошибки «502 Bad Gateway».

При моделировании DDoS-атаки на ресурсы важно учитывать обращение сервера к базе данных, которая может располагаться как внутри компьютерной сети, так и с привлечением облачных сервисов и центров обработки данных. При DDoS-атаке на пропускную способность обращений к базе данных не происходит, поэтому взаимодействие с ней моделировать нецелесообразно.

Существуют аналитические выражения [7], с помощью которых можно оценить вероятность нахождения СМО в каждом из состояний

и частоту отказов. Однако в условиях DDoS-атак их применение является некорректным, так как при моделировании DDoS-атаки на сервер в отдельный момент времени на сервер может прийти несколько заявок, что нарушает требования ординарности для потока входящих заявок, и, следовательно, его уже нельзя считать пуассоновским без грубых допущений, которые могут привести к значительным ошибочным результатам [9]. Таким образом, классический инструментарий теории СМО является неприспособленным для решения поставленной задачи. Выходом является применение имитационного моделирования методом Монте–Карло. Имитационное моделирование позволяет отслеживать изменения состояний системы во времени и применимо для моделирования случайных процессов, таких как DDoS-атаки [10, 11].

Моделирование. Важным этапом при моделировании является формирование потоков ложных запросов. С учетом этого осуществлялась постановка задачи моделирования атак на ключевые узлы информационной инфраструктуры, которыми являются серверы, и осуществления оценки их подверженности DDoS-атакам. В результате моделирования лицо, принимающее решение (ЛПР), получает информацию о вероятности отказа сервера, достаточную для принятия ряда организационных и технических мер для снижения риска.

В основе имитационной модели лежит случайный характер прихода заявок в каждый момент времени. Дальнейшее обслуживание заявок и освобождение каналов описывается с помощью логических выражений. Значение оценки вероятности успешной DDoS-атаки, равной оценке вероятности отказа сервера, рассчитывается как отношение среднего числа отказов к общему числу заявок. В результате проведения экспериментов с разработанной имитационной моделью были получены графики, представленные на рис. 4–6 В условиях высокой интенсивности поступления заявок и высоком значении отношения λ к μ ($\rho = 1000$), что соответствует DDoS-атаке, оценка вероятности отказа снижается на 4–6% при увеличении количества каналов на пять единиц (см. рис. 5).

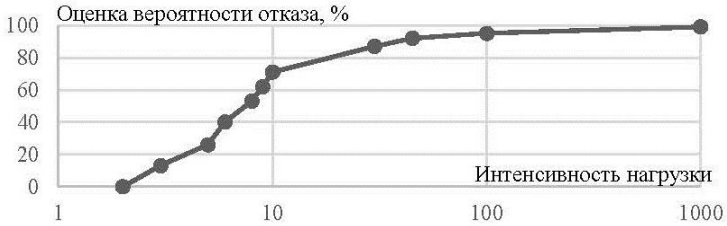


Рис. 4. Зависимость оценки вероятности успешной DDoS-атаки от интенсивности нагрузки сервера

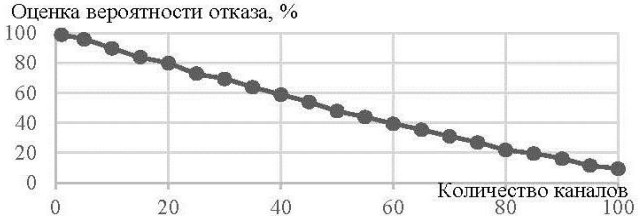


Рис. 5. Зависимость оценки вероятности отказа от количества каналов

Увеличение очереди обслуживания на 100 единиц позволяет снизить вероятность отказа на 1%. Так, при начальной вероятности отказа в 80% и длиной очереди, равной единице, для снижения вероятности отказа до 50% потребовалось увеличение очереди до 3000 единиц (рис. 6). Полученные результаты свидетельствуют о том, что наиболее эффективным способом снижения вероятности отказа является повышение производительности сервера путем увеличения его каналов обслуживания.

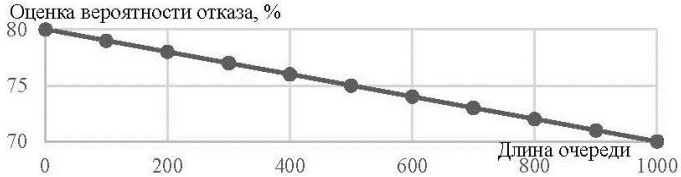


Рис. 6. Зависимость оценки вероятности отказа от длины очереди

Выводы. Таким образом, показана целесообразность применения имитационного моделирования методом Монте–Карло для оценки функциональной устойчивости элементов информационной инфраструктуры в условиях DDoS-атак.

ЛИТЕРАТУРА

1. RFC 4732. Internet Denial-of-Service Considerations. – 2006.

2. RFC 8612. DDoS Open Threat Signaling. – 2019.

3. Douligeris C. DDoS attacks and defense mechanisms: a classification / C. Douligeris, A. Mitrokotsa // Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology. – 2003. – PP. 190–193. DOI: 10.1109/ISSPIT.2003.1341092.

4. De Donno M. DDoS-Capable IoT Malwares / M. De Donno, N. Dragoni, A. Giaretta, A. Spognardi // Comparative Analysis and Mirai Investigation Security and Communication Networks. – 2018. – PP. 1–30. DOI: 10.1155/2018/7178164.

5. Cika P. Stress–2019. Tester and Network Emulator in Apache JMeter / P. Cika, V. Clupek // Computer Science, Photonics and Electromagnetics Research

Symposium. – 2019. – Spring (PIERS-Spring). – PP. 3722–3726. DOI: 10.1109/PIERS-Spring46901.2019.9017650

6. Mustafa M.E. Load Balancing Algorithms Round-Robin (RR) // Least-Connection and Least Loaded Efficiency Computer Science and Telecommunications. – 2017. – Vol. 1, No. 1. – PP. 25–29.

7. Солнышкина И.В. Теория систем массового обслуживания: учеб. пособие. – Комсомольск-на-Амуре: КнАГТУ, 2015. – 76 с.

8. FIFO – Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/FIFO (дата обращения: 25.04.2023).

9. Воеводин В.А. О применении имитационной модели оценки вероятности отказа сервера в условиях DDoS-атак / В.А. Воеводин, В.С. Черняев, Д.С. Буренок // 76-я Всерос. конф. «Радиоэлектронные устройства и системы для инфокоммуникационных технологий (РЭУС–2021)»: доклады. – М., РНТОРЭС им. А.С. Попова, 2021. – 409 с.

10.Lee J.L. Nonparametric Detection Methods against DDoS Attack / J.L. Lee, C.S. Hong // Korean Journal of Applied Statistics. – 2013. – Vol. 4. – PP. 291–305.

11.Chen L. Quickest attack detection in smart grid based on sequetial Monte Carlo filtering / L. Chen, X. Wang // IET Smart Grid. – 2020. – Vol. 3. – PP. 686–696.

УДК 004.056

КРИМИНАЛИСТИЧЕСКОЕ ВОССТАНОВЛЕНИЕ ДАННЫХ

С.Д. Иванова, студентка каф. ИБ

Научный руководитель Д.А. Елизаров, доцент каф. ИБ, к.т.н.

г. Омск, ОмГУПС, dvore@mail.ru

В настоящее время общество привыкло сохранять и редактировать информацию на своих персональных компьютерах и мобильных устройствах. Данные устройства содержат огромное количество данных от плейлиста с музыкой и семейных фотографий до значимых бумаг и секретных файлов. Но, помимо безвредных данных, многие модели устройств могут хранить персональные сведения о пользователе и его действиях, которые могут стать полезными при расследовании различных преступлений.

Ключевые слова: форензика, восстановление, данные, программы, потерянные данные.

Потребность в восстановлении данных возникает у всех людей, которые работают с информацией. Возможно, это файлы, связанные с работой, а возможно, на компьютере хранились персональные данные, которые тоже были утеряны. Но особенно эта потребность возникает у сотрудников правоохранительных органов, ведь информация необходима для того, чтобы расследовать различные правонарушения.

На рис. 1 представлен алгоритм восстановления данных.

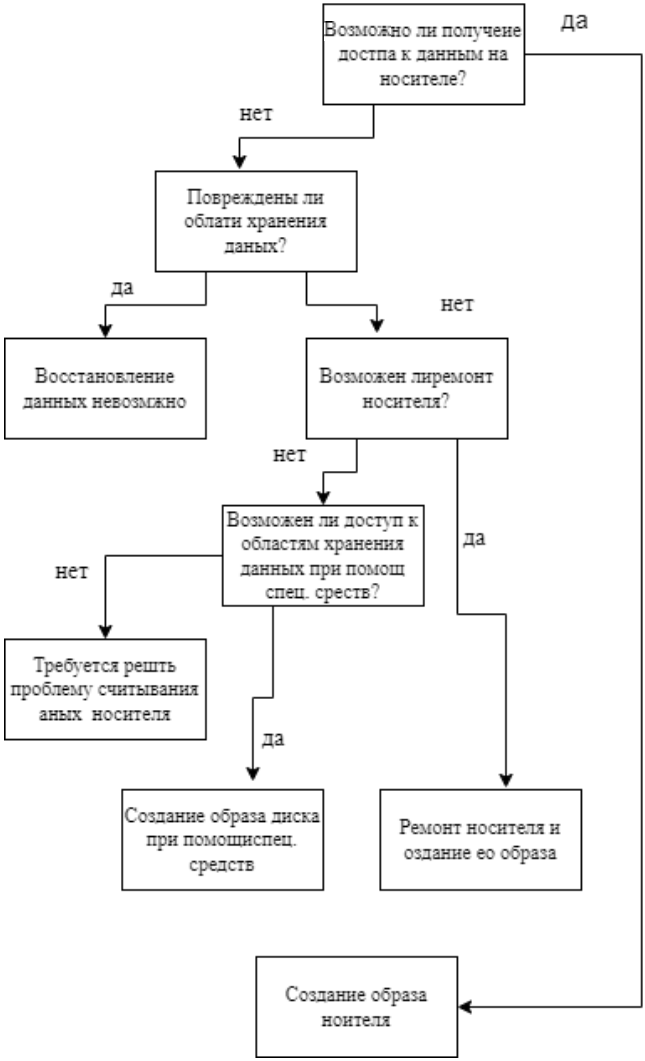


Рис. 1. Алгоритм восстановления данных

В операционной системе Windows (от Windows 8 и выше) существует встроенный механизм резервного копирования данных – File history (история файлов), основное предназначение которого заключается в обеспечении возможности восстановления удалённых файлов. Для мобильных телефонов с операционными системами iOS или

Android также существует способ восстановления данных без установки дополнительных программ – восстановление файлов из резервной копии, если она создавалась.

Рассмотрим некоторые из наиболее популярных свободно распространяемых программ восстановления данных для ОС Windows [3].

1) R.saver – легкая в использовании программа для восстановления файлов с разными версиями файловых систем NTFS, FAT и т.д.;

2) Recuva – программа представляет собой легкий в управлении и довольно сильный механизм восстановления данных;

3) RecoveRx – программное обеспечение от Transcend, который дает возможность осуществлять глубокий поиск файлов, подлежащих восстановлению;

4) Wise Data Recovery – программа для лёгкого и быстрого восстановления удаленных данных с локальных дисков, внешних накопителей, USB-накопителей и других съёмных устройств;

5) Undelete 360 – программа, использующая быстрый и эффективный алгоритм, который позволяет находить и восстанавливать файлы, удалённые по самым разным причинам.

Для проведения исследования эффективности указанных программ было использовано три файла различных типов и размеров:

- текстовый документ «Соня.docx» объёмом 10 кБ;
- аудиофайл «Соня.mp3» объёмом 20 кБ;
- графический файл «Соня.jpg» объёмом 58 кБ.

Было произведено безвозвратное удаление вышеуказанных файлов, после чего была выполнена попытка их восстановления с помощью различных программ.

Результаты проведённого эксперимента отражены в табл. 1.

Таблица 1

Результаты восстановления данных для ОС Windows

Название программы	Найденные файлы			Результат восстановления, %
	Документ	Аудио	Изображение	
R.Saver	+	+	+	100
Recovery	–	–	–	0
Wise Data	–	–	–	0
Undelete 360	–	–	–	0
RecoveRx	–	–	–	0
Recuva	+	+	–	70

В результате проведённого эксперимента наибольшую эффективность показала программа R.saver, с её помощью удалось найти и восстановить все удалённые файлы в первоначальном виде.

Далее рассмотрим некоторые программы, предназначенные для восстановления уничтоженных данных с внутренней памяти мобильных устройств на Android.

1) Dumpster – принцип работы данной программы подобен компьютерной корзине;

2) File Recovery – приложение для восстановления удаленных фото-, видео-, аудиоматериалы;

3) Restore All Files – программа, основной целью которой является восстановление всех удаленных файлов, в том числе видео, сообщений, контактов;

4) Restore Deleted Files – технология, созданная для восстановления потерянных данных с мобильных устройств Android. Root-доступ не требуется;

5) Recovery Files – приложение, использующее различные алгоритмы и параметры, которые помогают пользователям восстановить «посеянные» данные;

6) Undeleter – приложение для root-пользователей, которое дает возможность восстанавливать файлы какого-либо вида, удалённые с внешней SD-карты или внутренней памяти мобильного устройства.

Для проверки эффективности программ, предназначенных для мобильных устройств, было использовано два файла:

– аудиофайл «Соня1.mp3» объёмом 16 кБ;

– графический файл «Изображение.jpg» объёмом 58 кБ.

Было произведено удаление вышеуказанных файлов и последующее их восстановление с помощью различных программ. Результаты проведённого эксперимента приведены в табл. 2.

Таблица 2

Результаты восстановления данных для Android

Название программы	Найденные файлы		Результат восстановления, %
	Аудио	Изображение	
Undeleter	+	+	100
Dumpster	–	+	50
Restore All Files	–	–	0
Restore Deleted Files	–	–	0
Recovery Files	–	+	50
File Recovery	–	–	0

В данном случае наиболее полезной оказалась программа Undeleter, с помощью которой удалось найти и восстановить оба файла.

Подводя итог всему вышесказанному, можно сделать вывод, что правоохранительные органы используют в своих целях различные компьютерные программы или алгоритмы, которые помогают восстанавливать данные о злоумышленнике. Поэтому компьютерный специ-

алист приходит на помощь к сотруднику, тем самым помогая расследовать дело с помощью разработок различных программ.

ЛИТЕРАТУРА

1. Альтерман А.Д. Восстановление утраченных данных на компьютере / А.Д. Альтерман, А.С. Парфенова // Современные научные исследования и разработки. – 2019. – № 1 (30). – С. 110–112.

2. Федотов Н.Н. Форензика – компьютерная криминалистика. – М.: Юридический Мир, 2007. – 432 с.

3. Восстановление удаленных файлов в Windows 10, 8, 7, Vista и XP [Электронный ресурс]. – Режим доступа: https://hetmanrecovery.com/ru/recovery_news/recover-deleted-files-in-windows-10-8-7-windows-vista-or-windows-xp.htm (дата обращения: 02.03.2023).

4. Этапы восстановления данных [Электронный ресурс]. – Режим доступа: https://disk-on.ru/articles/steps-data-recovery.html (дата обращения: 02.03.2023).

5. История файлов в Windows [Электронный ресурс]. – Режим доступа: https://support.microsoft.com/ru-ru/help/17128/windows-8-file-history (дата обращения 05.03.2023).

УДК 004.056.5

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ: КАК ИСПОЛЬЗОВАТЬ БЕЗОПАСНЫЕ ПАРОЛИ И УСТРОЙСТВА ДЛЯ БЛОКИРОВКИ ДОСТУПА К КОМПЬЮТЕРУ

Д.Р. Игнатьев, студент

Научный руководитель Ф.А. Сухоносов, доцент каф. информационной безопасности Южно-Российского государственного политехнического университета (НПИ)

г. Новочеркасск, f.suhonosov@npi-tu.ru

Рассмотрена особая важность защиты персональных данных. Актуализация темы обусловлена ростом интернет-зависимости и угрозами безопасности персональных данных. Одним из способов защиты данных является использование безопасных паролей и устройств, которые блокируют доступ к компьютеру. Изучены методы защиты персональных данных в интернете и представлены примеры программных кодов, картинок и практик, которые могут быть использованы для повышения уровня безопасности. Предложены новые и уже ранее известные методы защиты персональных данных в интернете с помощью безопасных паролей и устройств блокировки доступа к компьютеру.

Ключевые слова: защита персональных данных, интернет, безопасные пароли, блокировка доступа к компьютеру, устройства безопасности.

Интернет стал неотъемлемой частью нашей жизни. Мы проводим много времени в интернете, работая, общаясь с друзьями, покупая товары и услуги. Однако вместе с возможностями интернета появляются и угрозы для безопасности наших персональных данных. Для того, чтобы защитить свои персональные данные в интернете, необходимо использовать различные методы, включая безопасные пароли и устройства для блокировки доступа к компьютеру.

В наше время интернет стал неотъемлемой частью нашей жизни. Каждый день мы проводим много времени в онлайн-сервисах, делая покупки на маркетплейсах, так называемых платформах, которые позволяют взаимодействовать покупателям с продавцами, не выходя из дома, общаясь со своими друзьями при помощи онлайн-почты и социальных сетей. Но, несмотря на все преимущества, интернет также является источником рисков и угроз для нашей безопасности и конфиденциальности.

Защита персональных данных – это ключевой аспект нашей безопасности, когда мы находимся в онлайн-режиме. Однако понимание того, как мы можем защитить свои персональные данные, может быть сложным. В этой статье мы рассмотрим, как использовать безопасные пароли и устройства для блокировки доступа к компьютеру, чтобы защитить нашу частную жизнь в онлайн-сервисах и защититься от угроз.

На данный момент статистика показывает, что не все люди задумываются о том, насколько важно подбирать и устанавливать правильные безопасные пароли. По данным экспертно-аналитического центра InfoWatch в I полугодии 2022 г. количество инцидентов с похищением информации в России возросло по сравнению с предыдущим годом в 16,75 раза, достигнув 187,6 млн записей [5].

Почему пароль – это важно?

Как уже упоминалось ранее, пароль – это важный аспект нашей безопасности, когда мы находимся в онлайн-режиме. Пароль – это первая линия защиты нашей учетной записи [2]. Использование пароля может предотвратить нежелательный доступ к нашим личным данным. Однако многие из нас ошибочно считают, что используют достаточно сложные пароли, но на самом деле они могут быть уязвимы к взлому.

Существует множество способов взлома пароля: от брутфорса (метод перебора всех возможных паролей) до фишинга (метод обмана). Поэтому, используя сложный пароль, мы повышаем наши шансы на защиту от таких угроз.

Как правильно выбрать пароль?

Эффективный пароль должен быть длинным, состоять из различных символов, различных регистров (буквы большого и малого шрифта), цифр и специальных символов. Например, пароль, состоящий из 8–12 символов, должен включать буквы различных регистров, цифры и специальные символы [9].

Однако как только все больше людей начинают использовать компьютеры и интернет, злоумышленникам становится все легче взломать пароли. Это означает, что мы должны использовать все более сложные пароли – такие, которые шифруются с помощью алгоритмов шифровок. Для этого разработаны специальные программы по выбору паролей.

Программное обеспечение для защиты паролей. Существует множество программ, которые помогают генерировать пароли с высоким уровнем безопасности [8]. Они могут рекомендовать пароли и генерировать их на основе геометрических фигур или конкретных случайных чисел. Эти программы также могут предоставить нам информацию о том, является ли наш пароль «слабым» или «сильным». 1Password, LastPass и Keeper – это некоторые из них. Например, сайт www.lastpass.com помимо прочего предлагает создавать и хранить сложные пароли автоматически.

Также часто пользователи устройств нового поколения могут заметить, что их устройство самостоятельно предлагает сгенерировать безопасный пароль при создании аккаунтов в сети интернет или приложений на устройствах. Данная опция на устройствах довольно удобна и практична в использовании. Не стоит отказываться от предложенного, как делает это большинство, поскольку это наиболее простой способ создания пароля без прикладывания собственных усилий.

Нейросети – одно из наиболее популярных программных решений для защиты паролей [11]. Эти программы используют для генерации безопасных паролей. Кроме того, не стоит забывать, что неиросети в последнее время становятся все более популярными, возможно, когда-нибудь на их основе будут созданы приложения, которые защищали бы данные и в целом электронно-вычислительные устройства от взломов, краж данных и заражения устройств вредоносными программами.

Устройства для блокировки доступа. Кроме паролей, мы также можем использовать различные устройства, чтобы защитить наш компьютер от нежелательного доступа. Это могут быть физические ключи (например, USB-ключи), которые должны быть подключены к компьютеру, чтобы войти в систему, или датчики отпечатка пальца, которые могут определить, являемся ли мы авторизованным пользователем [7].

Другие устройства могут включать камеры, которые могут обнаруживать и зафиксировать несанкционированный доступ к компьютеру. При этом данный механизм поможет обезопасить наши личные данные и защитить нашу частную жизнь.

Кроме того, устройства для блокировки доступа, такие как антивирусное программное обеспечение и файрволы, могут помочь предотвратить утечку персональных данных [1]. Эти программы помогают защитить ваш компьютер от вредоносного программного обеспечения и хакеров, которые могут попытаться взломать вашу систему.

На данный момент как государственные учреждения, так и частные предприятия практикуют использование специальных технологических устройств аутентификации, которые также защищают данные, но уже не только персональные – каждого сотрудника, но и корпоративные, например, такие как программно-аппаратные комплексы «Соболь» и «Росомаха». Они обеспечивают защиту устройств от несанкционированного вхождения в них нежелательных пользователей, предубеждают утечки информации, а также запрещают загрузку различных вредоносных программ по типу червей, ботов или троянских программ.

Но не только технические средства могут помочь обезопасить ваши персональные данные. Самое важное – не давать доступ к своей личной информации посторонним [10]. Не пользуйтесь общественными Wi-Fi точками доступа, не отвечайте на подозрительные сообщения от незнакомых отправителей и не посещайте подозрительные веб-сайты. Важно также не делать публичными свои личные данные в социальных сетях и онлайн-сервисах.

При пользовании сетью Интернет важно понимать, что никто не защищен от утечки данных. И чем больше внимания мы уделяем средствам и программам защиты, тем меньше риск утечки. Одним из возможных программных решений являются VPN-программы, их следует использовать при пользовании общественным Wi-Fi, поскольку он позволяет создавать одно или несколько сетевых соединений поверх другой сети.

Также еще одним способом обезопасить себя является регулярный бэкап данных. Регулярный бэкап данных является важным мероприятием для защиты персональных данных от потерь. Никто не застрахован от случаев удаления различных программ или ошибок в работе электронно-вычислительных устройств. Регулярный бэкап позволит сохранить важную информацию, такую как документы, фотографии и другие файлы, в случае возникновения подобных проблем [12].

Помимо всего прочего очень важно быть осторожным в социальных сетях [4]. Даже максимально защищенные и закрытые социаль-

ные сети, например, такие как Telegram, не могут полностью обезопасить вас от кражи информации. Социальные сети – это один из самых распространенных источников утечки персональных данных в интернете. Очень важно следить за тем, какую информацию публикуете в своих профилях в социальных сетях, так как она может быть доступна для просмотра другими пользователями, включая злоумышленников.

Следует избегать публикации личной информации, такой как адрес, номера телефона, паспортные данные и т.д. [3]. Также следует быть осторожным при подключении к новым друзьям и не принимать запросы на добавление в друзья от незнакомых людей. Общение в социальных сетях необходимо вести также осторожно и бережно, не рассказывая слишком много о себе.

И последнее, что важно предпринимать, – регулярно обновлять программное обеспечение. Регулярное обновление программного обеспечения является одним из самых важных аспектов защиты персональных данных в интернете [6]. Обновления программного обеспечения часто содержат улучшения в области безопасности, исправления ошибок и закрытие уязвимостей, которые могут быть использованы злоумышленниками.

Поэтому необходимо регулярно обновлять все программы на компьютере, включая операционную систему, браузер, антивирус и другие приложения. Некоторые программы могут быть настроены на автоматическое обновление, что упрощает этот процесс.

Заключение. Все мы хотим защитить свои персональные данные в интернете, поэтому использование сложных паролей и специальных устройств для блокировки доступа к компьютеру – это важная превентивная мера. Помните, что пароль – это первая линия защиты нашей учетной записи, но он становится уязвимым, если он не соответствует правилам создания безопасного пароля. Поэтому не забывайте использовать программное обеспечение для защиты паролей и устройства для блокировки доступа к компьютеру, чтобы быть уверенными в безопасности своих персональных данных. Важно осознать, что защита ваших персональных данных – это неотъемлемая часть современной жизни, и тщательное следование правилам безопасности поможет избежать неприятностей и возникновения возможных проблем в дальнейшем.

ЛИТЕРАТУРА

1. Приказ ФСТЭК России от 17 июля 2017 г. № 134. Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицен-

зированию деятельности по технической защите конфиденциальной информации.

2. Мартынова Л.Е. Исследование и сравнительный анализ методов аутентификации / Л.Е. Мартынова, М.Ю. Умницын, К.Е. Назарова, И.П. Пересыпкин // Молодой ученый. – 2016. – № 19 (123). – С. 90–93. – URL: https://moluch.ru/archive/123/34077/

3. Стриженко Ю.Г. Правомерность обработки персональных данных // Вестник электронного правительства. – 2019. – № 1. – С. 63–73. – URL: http://egov-journal.ru/wp-content/uploads/2019/06/strijenko_1_2019.pdf (дата обращения: 08.12.2022).

4. Главный информационный центр Министерства обороны Российской Федерации. Официальный сайт. – URL: https://function.mil.ru/auth/auth.aspx

5. Отчет об исследовании утечек информации ограниченного доступа в 1-й половине 2022 г. / Экспертно-аналитический центр InfoWatch. – 2022. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf

6. National Institute of Standards and Technology. Official Website. – URL: https://www.nist.gov/cyberframework

7. Kumar P. USB Key-Based Authentication and Encryption of Stored Data in Cloud Computing / P. Kumar, N. Sharma, R. Singh // Journal of Network Security. – 2017. – No. 5 (2). – PP. 1–12.

8. Vladimirov V. Cybersecurity governance models: a brief overview // Information & Security: An International Journal. – 2017. – Vol. 38, No. 2. – PP. 58–66. – URL: https://risu.org.ua/static/images/pdf/Information_Security/publications/2017/38_2/Vladimirov.pdf

9. Carbone R. Possible Measures to Strengthen Password Protection / R. Carbone, P. Kantor / S. Eguchi, S. Uchida, N. Sebe, S. Satoh (eds) // Computer Vision. – ACCV–2014. Workshops. Lecture Notes in Computer Science. – 2014. – Vol. 9008. – Springer, Cham.

10. Zhu B., Zhang Y. VPN-based privacy-preserving big data outsourcing framework for healthcare systems // Peer-to-Peer Networking and Applications. – 2019. – Vol. 12 (1). – PP. 61–73.

11. Oparin V. Modern Approaches to Data Encryption / V. Oparin, Yu. Shevchenko. In: Safonov A. (eds.) // Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance. ICEGOV–2013. Lecture Notes in Computer Science, – 2013. – Vol. 8074. – Berlin, Heidelberg: Springer.

12. Chatzopoulos S. Cybersecurity challenges in the European Union: the impact of the General Data Protection Regulation (GDPR) // International Journal of Cybersecurity Intelligence & Cybercrime. – 2020. – Vol. 1(1). – PP. 1–14. – URL: https://s3-eu-west-1.amazonaws.com/pstorage-ijcic/18914863/ID-2020-1-1-1-14_full.pdf

УДК 378.147

РОЛЬ И ПРИМЕНЕНИЕ DLP-СИСТЕМ НА ПРЕДПРИЯТИИ: РЕШЕНИЕ ПРОБЛЕМ ВНЕДРЕНИЯ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Маринов, к.э.н., доцент ЦК по кибербезопасности;
А.С. Гордин, магистрант Института информационных технологий
г. Иркутск, ИРНИТУ, am-irk@yandex.ru

Рассматриваются роль DLP-системы в защите информации, достоинства и недостатки имеющихся DLP-систем. Даны рекомендации по устранению недостатков DLP-систем. Рассмотрена модель настройки гиперпараметров.
Ключевые слова: DLP-система, безопасность, информационная безопасность, угрозы информационной безопасности, утечка данных, защита пользователя.

В настоящее время информационная безопасность является приоритетным направлением деятельности любого предприятия. Особое значение приобретают вопросы защиты персональных данных, которые являются наиболее ценным ресурсом предприятий. Одним из инструментов защиты данных являются DLP-системы. Однако, несмотря на их значимость, внедрение и использование DLP-систем нередко становится проблемой для предприятий.

Целью данной исследовательской работы является изучить роли и значимости DLP-систем в защите персональных данных на предприятии и выявить методы решения проблем при их внедрении и использовании.

Поэтому для начала необходимо понять, что собой представляют DLP-системы и персональные данные.

DLP-система представляет собой комплекс программно-аппаратных средств, обеспечивающих защищенность информации от угроз нелегитимной передачи из защищенного сегмента автоматизированной системы путем анализа и блокирования исходящего трафика [1].

Персональные данные представляют собой любую информацию, относящуюся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). Примерами того являются: фамилия, имя, отчество, дата рождения, номер телефона, электронная почта [2].

Развитие DLP-систем позволило значительно улучшить защиту конфиденциальных данных и предотвращать утечки информации в организациях, а также существенно упростить процесс управления правами доступа к данным и снизить риски нарушения безопасности информации.

Роль DLP-систем в защите информации. Роль DLP-систем в защите информации можно сформулировать следующим образом: DLP-системы играют важную роль в защите конфиденциальной информации компаний от внутренних угроз и утечек. Они осуществляют контроль передачи и сохранения информации на различных устройствах и протоколах, блокируют попытки пересылки информации по ключевым словам, и другим атрибутам [3].

Эти системы не могут гарантировать полную защиту от утечек, но их использование снижает риски утечки информации и улучшает безопасность корпоративной информационной системы [4].

Поэтому DLP-системы являются важным инструментом в обеспечении информационной безопасности.

DLP-системы обеспечивают контроль передачи информации через различные приложения и протоколы, защищают информацию от утечки на внешние носители и блокируют попытки пересылки или сохранения конфиденциальных данных.

Они также осуществляют поиск конфиденциальной информации на рабочих станциях и файловых серверах, по ключевым словам и атрибутам файлов, а также предотвращают утечки информации путем контроля ее жизненного цикла и движения [3].

В целом DLP-системы снижают риски утечки информации по неосторожности или умышленно со стороны сотрудников компании, что делает их важным элементом информационной безопасности.

Достоинства и недостатки DLP-систем. DLP-системы являются эффективным инструментом для защиты конфиденциальной информации в организации. Они позволяют контролировать передачу и использование конфиденциальных данных, обнаруживать утечки информации, а также предотвращать несанкционированный доступ. Это позволяет повысить экономическую безопасность компании и обеспечить прозрачность бизнеса.

Однако, высокая стоимость DLP-систем делает их доступными только для крупных и прибыльных компаний, а также требует высокой квалификации персонала и немалых трудозатрат для установки и настройки. Кроме того, возможность обхода системы защиты и высокий процент ложных срабатываний являются недостатками.

Также стоит отметить, что DLP-системы могут не учитывать изменения в среде предприятия, что может затруднять их использование в долгосрочной перспективе. Чтобы решить эти проблемы, рекомендуется постепенный переход к модульным структурам и адаптация систем к отраслевым спецификам. Это позволит добиться оптимальной работы системы и повысить ее эффективность при минимальных недостатках [5].

Способы устранения недостатков DLP-систем:

1. Снижение стоимости DLP-систем: одним из способов снижения стоимости DLP-систем может быть выбор доступных для организации более экономичных вариантов или покупка более простых программных продуктов, которые могут удовлетворять потребности организации. Кроме того, существуют облачные решения DLP, которые не требуют больших инвестиций в аппаратное и программное обеспечение.

2. Обучение персонала: требуется обучение специалистов, которые будут устанавливать и настраивать DLP-системы, а также обучение персонала, который будет использовать эти системы. Это позволит улучшить эффективность системы и снизить количество ложных срабатываний.

3. Использование передовых технологий: разработка новых технологий, таких как анализ больших данных, машинное обучение и искусственный интеллект, помогает повысить точность обнаружения и предотвращения утечек данных, адаптировать DLP-системы к специфике отрасли, чтобы повысить эффективность и уменьшить число ложных тревог.

4. Адаптация к специфике отрасли: медицинские учреждения могут требовать иных настроек, чем решения для финансовых учреждений.

5. Регулярное обновление и анализ системы: регулярные обновления и анализ системы помогут улучшить ее работу и обнаружить возможные недостатки и уязвимости. Также рекомендуется проводить периодические аудиты для оценки эффективности системы.

На рис. 1 представлена модель настройки гиперпараметров DLP-системы.

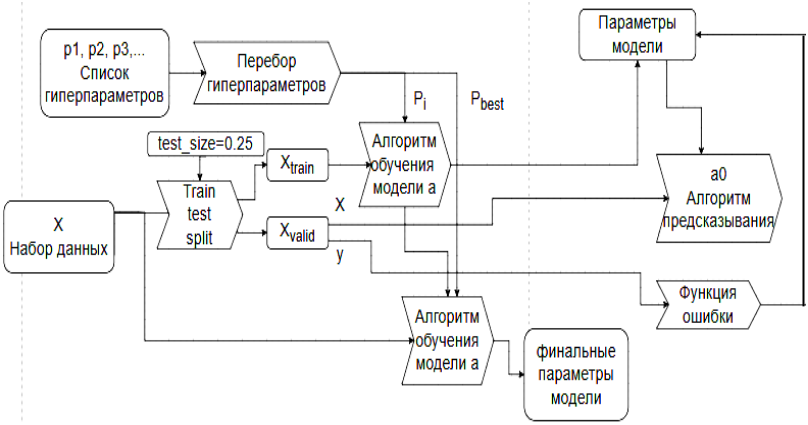


Рис. 1. Модель настройки гиперпараметров системы

Выводы. Таким образом, DLP-система не может гарантировать полную защиту информации от утечек, но ее использование снижает риски утечки информации и улучшает безопасность корпоративной информационной системы.

Были рассмотрены роль DLP-системы в защите информации, достоинства и недостатки имеющихся DLP-систем. Даны рекомендации по устранению недостатков DLP-систем. Рассмотрена модель настройки гиперпараметров.

ЛИТЕРАТУРА

1. Барабанов А.В. Формирование требований по безопасности информации к DLP-системам / А.В. Барабанов, М.И. Гришин, А.С. Марков // Вопросы радиоэлектроники. – 2013. – № 2. – С. 67–76.
2. Полянский Д.А. Оценка защищенности: учеб. пособие. – Владимир, Изд-во Владим. гос. ун-та, 2005. – 80 с.
3. Гречанная А.Ю. DLP-системы и их роль в защите от утечек конфиденциальной информации / А.Ю. Гречанная, А.Д. Тастенов // Наука и техника Казахстана. – 2015. – № 3-4. – С. 23–27.
4. DLP-системы. Leta IT Company [Электронный ресурс]. – Режим доступа: http://www.leta.ru/library/analytics/inside-015/inside-015.html (дата обращения: 20.02.2023).
5. Борботько Т.В. Система противодействия утечке данных «Контур информационной безопасности SearchInform» / Т.В. Борботько, О.В. Бойправ, В.Е. Морозов. – Минск: БГУИР, 2021. – 284 с.

УДК 004.771

РАЗРАБОТКА ОПЕРАТОРСКОЙ ВЕБ-СИСТЕМЫ ДЛЯ ОБСЛУЖИВАНИЯ АСУ ТП

Д.А. Мирошников, студент

Научный руководитель А.В. Цавнин, доцент каф. ОАР, к.т.н.

г. Томск, НИ ТПУ, avc14@tpu.ru

Предложена веб-система для обслуживания АСУ ТП. Вся информация о системе находится на микрокомпьютере, что позволяет обслуживающему персоналу получать доступ к ней непосредственно при обслуживании, избежав переноса документации от одного устройства к другому.

Ключевые слова: веб-система, JavaScript, React, документация, обслуживание.

С развитием технологий в сфере автоматизации отслеживание состояний и параметров определенных устройств стало достаточно важной задачей. Например, для получения информации о каком-либо процессе, о состоянии определенных параметров или же о количестве задвижек, клапанов и т.д. необходимо либо ознакомиться с докумен-

тацией, либо посмотреть на АРМ диспетчера, на котором будет отображена необходимая информация. Было решено разработать систему, которая даст возможность просмотра и редактирования (при необходимости и наличия соответствующих прав) определенных параметров, состояний датчиков и т.д.

Для реализации подойдет любая платформа, основанная на ядре Linux, модуль Wi-Fi, либо встроенный, либо установленный отдельно, блок и провод питания, а также Ethernet-кабель для подключения к PLC. Клиент реализован на языке JavaScript, на фреймворке React, а сервер – на фреймворке Express для Node.js. Данный стек технологий был выбран, потому что у этих фреймворков большая база пользователей и огромное количество готовых библиотек, в которых уже реализованы необходимые для создания ПО элементы, например, создание TCP клиента для опроса PLC посредством Modbus, или же компоненты в React, позволяющие масштабировать объекты и менять их внешний вид, что позволит создать современную и приятную глазу картинку, с которой будут работать инженеры.

Для начала был создан сервер, который будет обмениваться данными с PLC по протоколу Modbus TCP и записывать значения в базу данных, из которой уже они будут отправляться клиенту. При запуске клиента отправляется запрос на сервер, и при наличии устройства, которое необходимо опрашивать, раз в определенный промежуток времени циклично будет происходить опрос устройства. При наличии данных будет формироваться ответ, который в последующем будет отправлен клиенту. Если данных нет либо нет связи с устройством, будет приходить информация о том, что устройство недоступно.

Клиент реализован таким образом, что изначально пользователя приветствует страница авторизации. Если у клиента уже есть JWT-токен, то он будет перенаправлен на главную страницу, либо в меню настроек проекта в зависимости от уровня его доступа. Если же JWT-токена нет, пользователь должен ввести свои данные.

В случае введения валидных данных сервер сформирует JWT-токен для этого пользователя и вернет его клиенту. Также разработана панель настроек для администратора, в которой можно добавлять и удалять пользователей, а также выдавать им определенные роли, например «operator» или «editor».

В дальнейшем после входа, пользователя встречает главный экран, на котором расположены меню и элементы, установленные там другим пользователем. Каждый элемент имеет функционал по изменению размеров и внешнего вида, также есть возможность изменения внешнего вида, например цвета фона или цвета текста при определен-

ных значениях параметров. Для этого каждый из этих элементов можно привязать к определенному значению опрашиваемого устройства. Есть возможность добавления изображений на сервер, чтобы впоследствии использовать их в нужном количестве, если это необходимо. Если вдруг необходимо, то с клиента можно изменить IP устройства, которое будет опрашиваться, а также просмотреть и изменить параметры, если это нужно.

На рис. 1 изображена страница авторизации. После успешной авторизации (рис. 2), в зависимости от уровня доступа, пользователь попадает либо на главный экран (рис. 3), либо на экран настроек проекта (рис. 4). На рис. 2 изображено окно настроек элемента. В нем можно изменять цвет, размер и шрифт текста объектов, а также их содержание.

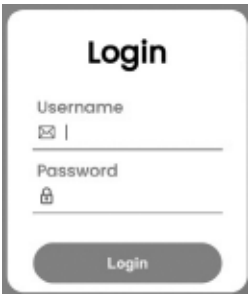


Рис. 1. Страница авторизации

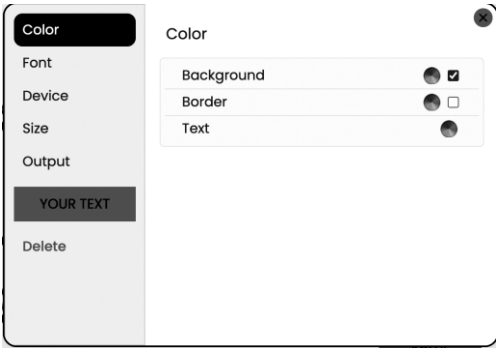


Рис. 2. Меню настроек элемента

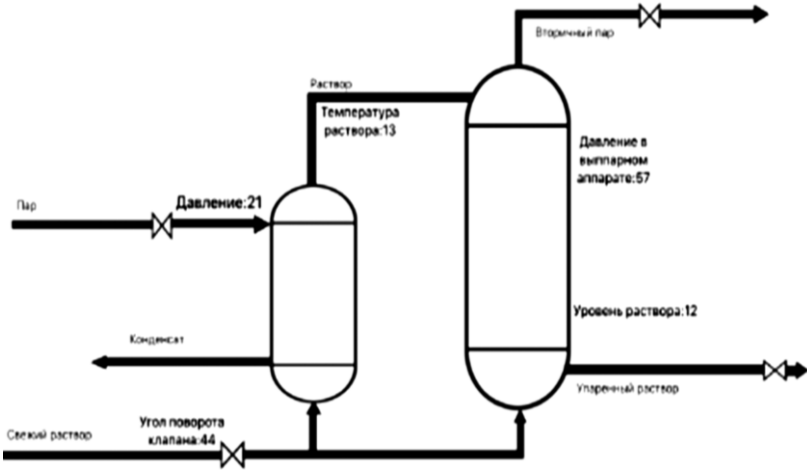


Рис. 3. Главный экран

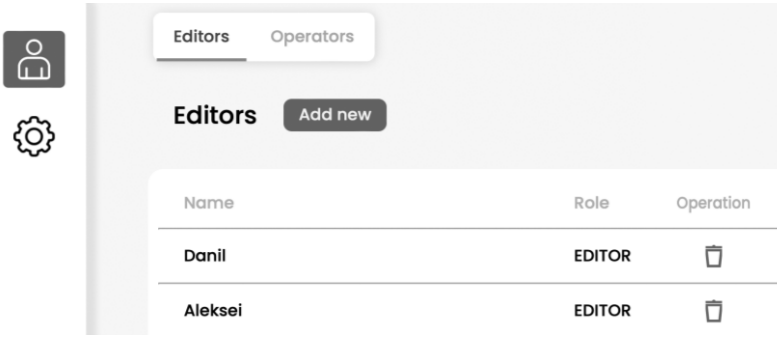


Рис. 4. Настройки системы

На главном экране расположены меню для создания объектов, а также различные настройки, пагинация для перехода между страницами и самое рабочее место, на котором можно располагать сами объекты.

В настройках проекта показано окно настроек системы, доступное только администратору. В нем есть возможность добавления и удаления пользователей с различными правами доступа, а также настройками подключения к ПЛК, такими как количество регистров или время опроса устройства.

Когда пользователь вводит свои данные, они отправляются на сервер, где в случае валидности пользователю возвращается JWT-токен. Если JWT-токен уже существует, то пользователь попадает на главный экран, где в случае внесения изменений, связанных с контроллером или данными на сервере, отправляется запрос на сервер. Если не возникает никаких ошибок, то пользователь увидит изменения на экране.

На рис. 5 изображена структурная схема работы клиента и сервера.

В ходе выполнения была создана система, реализующая обмен данными между контроллером и пользователем внутри локальной сети. В данной системе был реализован функционал для создания мнемосхем и изменения данных на контроллере в режиме реального времени.

В дальнейшем планируется добавить возможность написания пользователем собственных скриптов для мнемосхем, которые будут отрабатывать при определенных условиях.

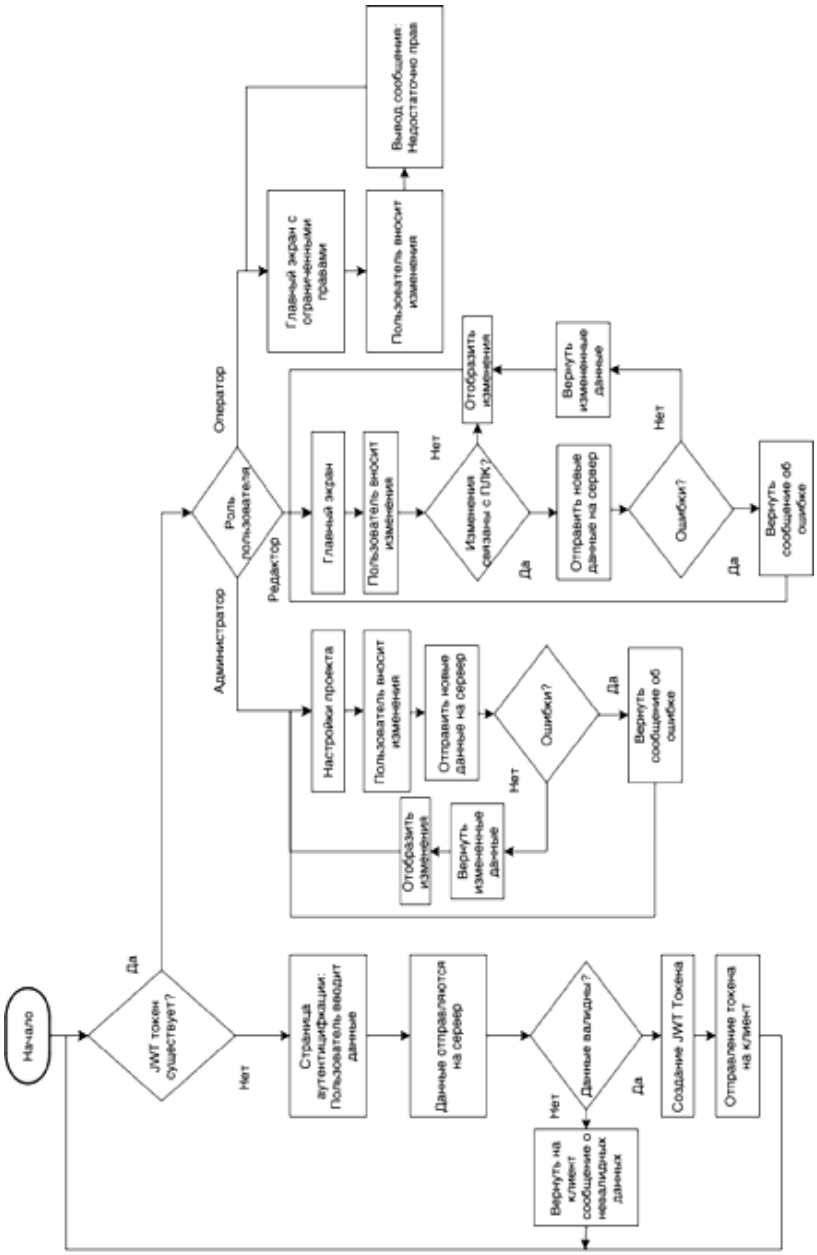


Рис. 5. Структурная схема веб-приложения

ЛИТЕРАТУРА

1. Официальная документация ExpressJs [Электронный ресурс]. – Режим доступа: https://expressjs.com/
2. Официальная документация ReactJs [Электронный ресурс]. – Режим доступа: https://ru.reactjs.org/
3. Официальная документация Node.js [Электронный ресурс]. – Режим доступа: https://nodejs.org/api/net.html

УДК 004.5

УЛУЧШЕНИЕ РАБОТЫ АЛГОРИТМОВ КЛАССИФИКАЦИИ МАШИННОГО ОБУЧЕНИЯ ПУТЕМ ПРИМЕНЕНИЯ МЕТРИК ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИ АНАЛИЗЕ СЕТЕВОГО ТРАФИКА

Я.А. Питько, студент

Научный руководитель А.В. Иванов, доцент каф. защиты информации, к.т.н.

г. Новосибирск, НГТУ, andrej.ivanov@corp.nstu.ru

Рассматриваются способы улучшения работы алгоритмов при решении задачи классификации в ходе определения нежелательного контента с использованием метрик эффективности классификации при анализе сетевого трафика. Для успешного функционирования данной модели необходимо добиться оптимальных результатов выявления нежелательного контента на моменте ее тестирования и не допустить возможность переобучения. В связи с чем в процессе обучения модели необходимо использовать определённые метрики, по результатам которых в исходный алгоритм вносятся правки, вследствие чего доля ошибки может быть снижена.

Представлен комплекс аналитических выражений, применение которых способствует снижению доли ошибки в ходе определения вида поступаемого трафика.

Ключевые слова: сетевой трафик, True-трафик, False-трафик, машинное обучение, нежелательный контент, ошибка первого рода, ошибка второго рода

В современном интернет-пространстве появляется все больше нежелательного контента, подвергающего опасности пользователей сети. Против подобного материала давно стали разрабатывать различные методы, позволяющие ограничить демонстрацию вредоносного контента в интернете, и продолжают до сих пор. Существующие методы, разработанные достаточно давно, уже нашли способы обхода программируемой системы со стороны злоумышленников и не могут считаться эффективными, используясь поодиночке. Более того, ком-

плексное использование также не может быть результативно оценено, поскольку большинство методов направлено на точечное выявление нежелательного контента на основе репутации страниц, ключевых слов/выражений, анализа содержащихся изображений, отклика пользователей, посетивших страницу, и т.п. Например, система «черных» и «белых» списков, способна производить контент-фильтрацию по обобщенной структуре, игнорируя большинство неочевидных сценариев, при которых получаемый контент может быть отнесен к нежелательному.

Под нежелательным контентом в данном контексте понимается не только некорректная реклама, но и демонстрация аудиовизуального материала, признанного нежелательным или запрещенным на территории того или иного государства, а также вредоносные программы, способные заполучить доступ к информации, хранящейся на компьютере пользователя. В интернете зачастую содержится информация, являющаяся запрещенной не «напрямую», так как определить степень ее опасности можно только по вторичным характеристикам, выявленным только в ходе просмотра сетевого трафика. В этом случае простые методы обучения, основанные на анализе страницы, не будут эффективны.

Информация, проходящая через компьютерную сеть, носит название «сетевой трафик». В нем фиксируется весь объем данных, получаемый в результате перехода с ресурса на ресурс. В настоящее время в системах контентной фильтрации при анализе сетевого трафика применяются следующие методы ограничения доступа к веб-ресурсу: по конкретному IP-адресу, по адресу URL, по протоколу или порту. Например, классификация и идентификация трафика в операционной системе, приложениях и клиентских браузерах может быть выполнена с использованием защищенного трафика по протоколу передачи гипертекста (HTTPS) [1]. Таким образом, для предотвращения демонстрации пользователю нежелательного контента необходимо в первую очередь оценить степень опасности поступающего сетевого трафика.

В данном случае стоит различать понятия «приемлемого» и «неприемлемого» трафика. Первый тип трафика не содержит вышеописанных характеристик нежелательного контента и является «чистым» с точки зрения вредоносной информации. Второй тип содержит элементы, по которым данный ресурс может быть заблокирован в связи со степенью опасности располагающейся на нем информации. Далее в данной работе первый и второй типы будут заменены на словосочетания «True-трафик» и «False-трафик» соответственно.

В последние годы исследователи предложили множество методов обнаружения False-трафика, основанных на машинном обучении, которые в целом можно разделить на классическое машинное обучение и глубокое обучение. Классическое машинное обучение, в свою очередь, можно разделить на две подгруппы: обучение с учителем и без учителя. В статье [2] авторы проводят обзор методов глубокого обучения, предназначенных для обеспечения кибербезопасности, среди которых рассматриваются сети глубокого убеждения, глубокие автоэнкодеры, RNN, CNN и др.

Авторы работы [3] представили результаты, полученные путем применения рекуррентного алгоритма глубокого обучения для классификации трафика через облачные системы интернета вещей. В [4] авторы провели всесторонний обзор большого количества классификационных показателей и сравнили их с помощью стандартных показателей, таких как скорость, точность и т.д. В [5] был предложен новый подход к обнаружению DDoS-атак в SDNS путем применения шести классификаторов (SVM, случайных лесов и машин с градиентным усилением) с использованием оптимального набора весов.

Автором рассматривается улучшение работы алгоритмов реагирования на нежелательный контент путем его распознавания при решении задачи классификации. Чтобы определить задачу классификации, человек начинает с представления данных в векторном пространстве их характеристик; затем он выполняет вычисления на основе этого представления данных и присваивает оценку, которая может быть переведена в определенный класс [6].

Целью данного исследования является построение комплекса аналитических выражений, применение которых увеличит точность распознавания нежелательного контента при сканировании сетевого трафика.

Математическая постановка задачи классификации. Рассматриваемый сетевой поток для итогового алгоритма может быть разделен на два класса: класс приемлемого контента, на который не должна срабатывать блокировка, и класс неприемлемого контента, при обнаружении которого необходимо сообщить пользователю о возможной опасности. Для машинного обучения разделение на два класса данных является задачей классификации, т.е. задачей, в которой классы заранее известны и данные могут быть разделены только на два этих класса.

Классическая задача классификации в терминах теории вероятностей основывается на множестве пар «объект, класс» $X \times Y$, которые представлены в виде вероятностного пространства с неизвестной вероятностной мерой P. Согласно данной мере генерируется конечная

обучающая выборка наблюдений: $X^m=\{(x_1,y_1),\ldots(x_m,y_m)\}$. Требуется построить алгоритм $a: X\to Y$, способный классифицировать произвольный объект $x\in X$ [7].

После реализации алгоритма полученные объекты тестовой выборки можно разделить на четыре непересекающихся множества.

- истинно положительные значения (true positive, TP);
- истинно отрицательные значения (true negative, TN);
- ложно положительные значения (false positive, FP) (ошибка первого рода);
- ложно отрицательные значения (false negative, FN) (ошибка второго рода).

Ложно положительные и ложно отрицательные значения, возникающие в процессе классификации сетевого трафика, являются одной из значимых проблем при работе алгоритмов обнаружения нежелательного контента. Данные ошибки оказывают негативное влияние на такие показатели качества алгоритма, как полнота и точность результата обнаружения, и приводят либо к большому числу ложных срабатываний систем обнаружения, либо к большому числу пропусков [8].

Из вышесказанного следует: чем меньше будет ошибок первого и второго рода при обнаружении нежелательного контента, тем более полным и точным будет алгоритм по его обнаружению.

Метрики оценки эффективности классификации при обнаружении нежелательного контента. Как было сказано в предыдущем пункте, метрики оценки эффективности алгоритмов классификации вычисляются исходя из полученных четырёх видов результатов: True Positive, True Negative, False Positive, False Negative. По данным параметрам рассчитываются следующие показатели: точность, полнота и F-мера.

Основными метриками классификации являются достоверность (accuracy) классификации (TPR – True Positive Rate – частота истинно положительных результатов) и ошибка (error), определяемые следующим образом:

$$\text{Accuracy=TPR}=\frac{\text{TP+TN}}{|S|}=\frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}, \quad (1)$$

$$\text{error}=1-\text{accuracy}, \quad (2)$$

$$\text{FPR}=\frac{\text{FP}}{\text{FP+TN}}. \quad (3)$$

Также, на практике используется параметр, противоположный параметру TPR – False Positive Rate (FPR) – частота ложно положительных результатов.

Для построения более выигрышного баланса между истинно положительным и ложно положительным результатом классификации используют метрики точности (precision), полноты (recall) и F-меры (F-score). Метрики определяются следующим образом.

Точность (precision) измеряет, какой процент объектов, для которых алгоритм предсказал класс 1, действительно относится к классу 1:

$$\text{precision} = TP/(TP + FP). \quad (4)$$

Полнота (recall) измеряет, для какого процента объектов класса 1 алгоритм предсказал класс 1:

$$\text{recall} = TP/(TP + FN). \quad (5)$$

На практике обе метрики рассчитываются параллельно Точность, в отличие от полноты, чувствительна к распределению данных. Данные метрики, как правило, рассчитываются параллельно, поскольку являются взаимодополняемыми. Полнота не отражает, сколько образцов помечены как положительные неверно, а точность не дает никакой информации о том, сколько положительных образцов помечены неправильно [8].

Рассчитывать и анализировать обе метрики зачастую не совсем неудобно, поэтому чаще всего применяется комбинация полноты и точности в так называемой F-мере. F-мера сочетает в себе вышеупомянутые две метрики и присваивает взвешенную важность либо точности, либо полноте, используя коэффициент β:

$$\text{F\_score} = \frac{(1 + \beta^2)*\text{recall}*\text{precision}}{\beta^2*\text{recall} + \text{precision}}. \quad (6)$$

Однако на практике чаще всего важность точности и полноты удобнее всего присваивать в равной степени. Поэтому формула (6) принимает вид среднего гармонического этих двух величин.

$$\text{F\_score} = 2 * \frac{\text{recall}*\text{precision}}{\text{recall} + \text{precision}}. \quad (7)$$

Из формулы (7) можно видеть, что значение F-меры напрямую зависит от значений обеих метрик. Иными словами, если хотя бы одна из двух метрик близка к 0, F-мера тоже будет близка к 0, что свидетельствует о низком качестве применённого алгоритма или отсутствии баланса входных обучающих данных.

Для оценки эффективности алгоритмов классификации используются и другие метрики, однако вышеперечисленные позволяют видеть предполагаемое значение классификации на выходе алгоритма и корректировать его с учетом полученных значений.

Заключение. Качество работы обученной модели зависит от многих факторов, начиная с исходных данных и заканчивая выбранным алгоритмом обучения. Задача классификации при исследовании сетевого трафика может быть решена на основе реальных датасетов, собранных с помощью программ-анализаторов трафика, однако за счёт сложной структуры современной сети более качественного разделения на приемлемый и неприемлемый контент можно добиться только на этапе обучения.

В данном исследовании был рассмотрен метод улучшения качества модели на этапе обучения, применение которого увеличит точность распознавания нежелательного контента при сканировании сетевого трафика. Описанные аналитические выражения позволяют более качественно подойти к оценке алгоритма классификации, снизив долю полученных ложно положительных (ошибка первого рода) и ложно отрицательных (ошибка второго рода) результатов.

По представленному алгоритму расчета метрик в настоящее время проводятся экспериментальные исследования для внедрения данного комплекса аналитических выражений в работу алгоритма, чтобы определить параметры входных данных, при которых разработанный комплекс для обнаружения нежелательного контента при анализе сетевого трафика будет предоставлять налучшие результаты.

ЛИТЕРАТУРА

1. Afeez Ajani Afuwape. Performance evaluation of secured network traffic classification using a machine learning approach / Afeez Ajani Afuwape, Ying Xu, Joseph Henry Anajemba, Gautam Srivastava // Computer Standards & Interfaces. – 2021. – Vol. 78. – Article 103545.

2. Berman D. A survey of deep learning methods for cyber security / D. Berman, A. Buczak, J. Chavis, C. Corbett. – 2019. – 37 p.

3. Patil S. Classification of traffic over collaborative IoT and Cloud platforms using deep learning recurrent LSTM / S. Patil, L.A. Raj // Comput. Sci. – 2021. – Vol. 22.

4. Alzahrani R.J. Survey of Traffic Classification Solution in IoT Networks / R.J. Alzahrani, A. Alzahrani // Int. J. Comput. – 2021. – Vol. 183. – PP. 37–45.

5. Maheshwari A. An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment / A. Maheshwari, B. Mehraj, M.S. Khan, M.S. Idrisi // Microprocess. Microsyst. – 2022. – Vol. 89. – Article 104412.

6. Belkadi O. ML-Based Traffic Classification in an SDN-Enabled Cloud Environment / O. Belkadi, A. Vulpe, Y. Laaziz, S. Halunga // Electronics. – 2023. – 18 p.

7. Шелухин О.И. Технологии машинного обучения в сетевой безопасности / О.И. Шелухин, С.Д. Ерохин, М.В. Полковников; под ред. О.И. Шелу-

хина. – М.: Горячая линия – Телеком, 2023. – 360 с. – Сер.: Интеллектуальные технологии информационной безопасности. – Вып. 1.

8. Микова С.Ю. Гибридный алгоритм обнаружения сетевых аномалий на основе системы голосования / С.Ю. Микова, В.С. Оладько, А.А. Мелких // Вестник УГАТУ. – 2016. – № 1 (71).

УДК 343.982.9

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ СЛУЧАЕВ МОШЕННИЧЕСТВА, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ SIP- И VOIP-ТЕЛЕФОНИИ

Р.С. Поляков, студент;

Р.М. Данилов, зав. каф. информационных технологий, к.т.н.

г. Хабаровск, ХИИК СибГУТИ,danilovroman@mail.ru

Рассмотрены некоторые особенности совершения мошенничества в сфере сотовой связи и IP-телефонии. Приведены примеры совершения преступлений. Описаны способы совершения мошеннических действий пользователями связи.

Ключевые слова: преступление, сотовая связь, IP-телефония, SIP, VoIP, протокол.

Преступления экономической направленности в России являются одними из наиболее часто регистрируемых при сообщении в органы внутренних дел о совершенном или готовящемся преступлении. Как следует из данных с января по октябрь 2022 г., предоставленных ресурсами МВД России, всего было зарегистрировано 1 677 066 преступлений [1]. Из них преступлений против собственности – 989 885, а касаемо объекта нашего исследования – мошенничества (ст. 159–159.6 УК РФ) – 2 822 698, что в процентном соотношении составляет 16,9% от всех зарегистрированных преступлений. Из них раскрыто и материалы находятся в производстве в отчетном периоде лишь 59 800 преступлений, что является довольно низким показателем, если сравнивать с показателями регистрации и раскрываемости других категорий преступлений.

Бурный технологический прогресс научно-технических знаний привнес не только удовлетворение потребностей населения в общении, в поиске литературы и сферы развлечений, но также обеспечил возможность удаленно с использованием информационных технологий осуществлять некоторые финансовые и юридически значимые действия, для которых ранее требовались физические носители информации, например, паспорт, свидетельство о регистрации и т.д. и

предоставление этих документов соответствующим органам с преодолением длинных очередей и множественных бюрократических особенностей ведения делопроизводства.

Однако вместе с тем такими же пользователями данных услуг являются и криминальные субъекты. Лица, которые, открыв для себя киберпространство, стали изобретать новые способы обогатиться на неосведомлённых в некоторых аспектах действий в этом самом пространстве лиц.

Так, в центре нашего внимания становится понятие «обман», выступающее способом совершения мошенничества, понимание которого мы можем почерпнуть из разъяснений Верховного Суда Российской Федерации, которое звучит следующим образом: «Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение» [2].

Обман – это в первую очередь умышленное искажение действительности, преднамеренное введение в заблуждение по факту тех обстоятельств, из которых злоумышленник намерен получить выгоду имущественного характера [3]. То есть мошенничество – это совершение хищения имущества потерпевшего, оставляя его в неведении об истинных мотивах действий преступника.

Суть данной разновидности экономических преступлений заключается не только в обмане потерпевшего, но также в том, что действия преступника направлены в первую очередь не непосредственно на имущество, а на склонение потерпевшего к их передаче.

Также стоит отметить, что мошенничество, совершенное с использованием средств связи, подразумевает, что злоумышленник и потерпевший не встречаются в реальности. Факт их встречи отражается в ином пространстве, а передача денежных средств производится путем перевода на электронные кошельки и иные накопители.

В таком случае возникает вопрос о доказательстве факта наличия обмана. Изучить способ его осуществления, местоположение абонентов и путь, по которому прошли денежные средства прежде, чем оказаться на счету злоумышленника, – это первоочередные задачи, с которыми сталкиваются правоохранительные органы при расследовании данной категории дел.

На сегодняшний день существует немало методов использования обмана. Одним из таких методов является «Фишинг» – суть которого

в использовании методов практической психологии, относящихся к социальной инженерии с целью получения логинов, паролей, данных карт, номеров телефонов, паспортов наиболее неподготовленных в теме пользователей, а также создание видимости, что действия человека, который указывает на серьезную проблему и вызывается помочь, являются искренними и малодушными [4]. Но на самом деле преступник уже «поймал на удочку» незадачливого потерпевшего.

Как правило, на данном историческом этапе, учитывая технологический прогресс, мошенник старается исключить знание потенциальной жертвы о его личности, включая особенности его внешности, персональные данные и сведения о местоположении. Самым простым и действующим методом является мошенничество с использованием средств телефонии, так как соблюдает указанные выше факторы, за исключением абонентского номера.

За последние несколько лет на территории России наблюдается рост числа такого способа совершения дистанционных преступлений, оставляя в неведении о личности преступника, как и потерпевшего, так и правоохранительные органы. Так, по данным Банка России, во втором квартале 2022 г. граждане Российской Федерации под воздействием третьих лиц перевели злоумышленникам денежные средства 211 тыс. раз, что в сумме составило 2,8 млрд рублей [5].

Во многом здесь играют роль методы социальной инженерии и использование специальных сервисов, сохраняющие анонимность преступника.

Понятие «социальная инженерия» не рассматривается ни одним нормативно-правовым актом, но неоднократно раскрыто многими учеными в области информационных технологий. Так, пионерами в этой области стали К.Д. Митник и В.Л. Саймон. По их мнению, социальная инженерия – это совокупность подходов прикладных социальных наук, приемов и технологий, ориентированных на создание организационных структур для регулирования и управления действиями человека [6].

Как правило, лица, совершающие мошенничество через телефонную связь, обращаются к потерпевшим от лица сотрудника банка. Они представляются, вежливо просят назвать имя кредитора или сами обращаются по имени, называют причину их звонка и предлагают свою помощь в решении сложившейся якобы проблемы.

Обычно сценарий следующий: злоумышленник производит звонок потерпевшему с целью подтверждения оформленного кредита. После того, как клиент сообщает, что не оформлял кредит, мошенник фиксирует данный момент и передает звонок в якобы ПХО. Далее

клиента перенаправляют на другую линию, где ему сообщают о мошеннических действиях с его банковской картой и предлагают перевести на резервный счет его денежные средства с целью избежать их утрату. На что клиент соглашается.

Типичный портрет мошенника – это, как правило, лицо от 25 лет, чаще всего с незаконченным высшим образованием. Эти лица, хорошо осведомлённые во многих областях, в том числе в сфере информационных технологий. Кроме этого, такой тип преступников обладает мастерскими навыками демагога или оратора, поэтому его речь всегда грамотна, четко поставлена и уверенна, что и создает видимость «искренности» намерений преступника, чем он и пользуется. Этот и другие сценарии аккумулирует Сбер на своем сайте [7].

Речь сама по себе, с точки зрения социальной инженерии, имеет ряд недостатков. Она связана с нашим субъективным восприятием фактов. Из-за этого термин «гипноз» считается не таким уж и шуточным и несерьезно воспринимаемым. Опускание ряда фактов, легендирование истории, искажение смысла излагаемого влечет неправильное понимание сути воспринимаемой информации. Это в совокупности с корыстной направленностью и целеустремленностью преступника является «оружием» мошенника, но изрядно устоявшимся и состаренным.

Поэтому ему на помощь приходят информационные технологии и технический прогресс. Особенную помощь в этом ему оказывают сервисы подмены номеров SIP-серверов.

SIP, или «протокол установления сеанса», – это протокол передачи данных, описывающий способ установления и завершения пользовательского сеанса связи. Мошеннические действия совершаются на основе пользовательских абонентских номеров телефона и виртуальных номеров, работающих посредством интернет-соединения.

Напомним, что абонентский номер – это номер, идентифицирующий оконечный элемент сотовой связи. Он состоит из 11 последовательных цифр: 1 – это число, определяющее принадлежность абонентского номера к коду страны. Так, в Российской Федерации используется устоявшаяся цифра «8» или «+7», разницы особенной действительно нет, если звонок совершается на территории Российской Федерации, но если за ее пределами, то очень важно использовать международный формат «+7», где «+» это международный формат совершения телефонного звонка, а «7» – код для России и Казахстана. Например, коды «+1» – это Северная Америка или «+44» – Великобритания.

2, 3, 4-я цифра – это уже набор цифр, который относится к региону (495, 499 – Москва, 421 – Хабаровский край), и оператору сотовой

связи, например, «МТС», «Билайн», «Теле2», «МегаФон». Но кроме того, существуют мобильные коды, в большинстве случаях, начинающихся с цифры 9xx («МегаФон» – 92x, 93x; МТС – 91x и 98x и т.д.). И уже остальные цифры после трехзначного являются номером клиента.

Сотовая связь завязана на использовании общих зон покрытия вышками – «Секторы». Образуемые зоной покрытия вышкой перекрываются другими вышками, так и образуется сеть. Такого рода процесс коммуникации между собеседниками существует уже очень давно, и его особенности вполне известны органам следствия.

Наиболее часто, абонентский номер предполагаемого злоумышленника начинается с «8-800…», и это не просто так. Как мы выяснили ранее, операторы закрепили за собой номера, которые после кода страны начинаются с цифры «9» и последующей за ней их кодом. В свою очередь, номер «8-800…» не принадлежит ни одному оператору сотовой связи и не требует для совершения звонка сотового аппарата и подключения к базовой станции. Все эти звонки совершаются через программное обеспечение на смартфоне или через программное обеспечение персональных компьютеров по протоколу IP.

Такого рода звонки осуществляются без физического носителя – SIM-карты, который содержит в себе электронный номер абонента и информацию об аккаунте, о чем известно мошенникам. Поэтому они используют различные сервисы или мессенджеры. Для потерпевшего звонок совершается как обычно, а для мошенника входящий вызов похож на звонок через, например, «WhatsApp» или «Skype». При совершении такого звонка невозможно отследить информацию о привязке номера к конкретной станции. Возможным остается получить сведения об использованных IP-адресах.

IP-адрес – это уникальный адрес, идентифицирующий устройство в интернете или локальной сети. IP-адреса существуют двух типов – «IPv4» и «IPv6». Первый является наиболее распространенным на данный момент, но при этом ограничен в своем количественном выражении – максимальное число таких адресов может достигать до 4,3 млрд. Такое ограниченное комбинаций, еще до изобретения «IPv6», смогла решить технология «преобразования сетевых адресов» – NAT. Данный ресурс предоставляет возможность обеспечить максимальное количество пользователей IP-адресами, вплоть до того, что один IP-адрес будет использоваться сразу несколькими клиентами, что может создать много проблем при расследовании уголовных дел.

Аббревиатура «IP» означает «интернет-протокол», т.е. это определенный набор правил, по которым осуществляется передача данных

через сеть. Он содержит в себе информацию о местоположении устройства и обеспечивает его доступность для связи, что и является важным для работы с интернетом. IP-адрес состоит из четырех чисел с диапазоном от 0 до 255, например, 144.178.1.38 [8].

Виртуальный номер – это основная услуга SIP-провайдеров, которая работает по принципу переадресации звонков через интернет. Такие звонки могут поступать на несколько компьютеров одновременно, при условии, что они подключены к одному аккаунту. По такому сценарию работают Call-центры, когда поступает звонок на несколько устройств, а отвечает любой из свободных представителей.

На сегодняшний день в связи с проведением специальной военной операции участились случаи мошенничества из стран Прибалтики, Германии или Украины, которые представляются сотрудниками Call-центра российского Банка и работают по вышеотработанному сценарию. Поиск таких сервисов особой сложности не вызывает. Форумы по их обсуждению, отысканию «лежат» в открытом доступе при наборе «SIP-сервисы по подмену номеров» в поисковой системе Google, где возможно найти некоторые названия таких сервисов.

Также, как правило, мошенник не использует номер телефона, схожий с абонентским, в котором указан, по крайней мере, код региона или города. Поэтому предварительно потерпевший должен понять, что если все-таки исходящий номер телефона ему не знаком, но внешне он похожий на обычный номер, вероятно, это виртуальный номер SIP-провайдера и на него ни в коем случае нельзя отвечать.

Зная этот номер, возможно получить следующую информацию: данные владельца номера, информацию об иных номерах, связанных с этим, реальный абонентский номер и адреса электронной почты. Проблема в том, что полностью всю эту информацию получить в одном документе или в одном предложении невозможно. Требуется использовать несколько сервисов, каждый из которых позволит по крупицам собрать все сведения.

Интернет-звонки совершаются по принципу VoIP-телефонии. VoIP преобразует стандартный телефонный сигнал в цифровой поток и наоборот, который может передаваться через интернет-сеть [9]. Они также, как и SIP-модули, могут быть установлены в качестве программного обеспечения на смартфон или, что характерно именно для этого вида, могут быть отдельным традиционным телефоном, предназначенным для вышеуказанных целей.

Итак, делая промежуточный вывод, мы можем с уверенностью сказать, что информационные технологии породили совершенно новые способы совершения мошенничества, в том числе с использованием средств связи и электронной телефонии. Эти средства позволя-

ют оставаться злоумышленнику незамеченным или, по крайней мере, скрытным от потерпевшего и правоохранительных органов. В этом ему помогают различные SIP-ресурсы, которые изначально должны были решить проблему ограниченного количества IP-адресов технологии «IPv4» до изобретения «IPv6», но теперь используется совместно с методами социальной инженерии в целях хищения имущества, оставляя всех в неведении о его местоположении, анкетных данных, внешности и т.д.

Посредством различных интернет-ресурсов возможно установить принадлежность абонентского номера к оператору связи, например, сервис КОДЫ.SU URL: https://www.kody.su/check-tel#text. Данный сайт позволяет определить не только сотового оператора связи, но также где он был зарегистрирован.

При оформлении запроса о держателе абонентского номера оператору связи в части требования следует указать: полные сведения о держателе абонентского номера, когда и на кого оформлен с указанием Ф.И.О., даты рождения, адреса, адреса подразделения, где зарегистрирован и обслуживается данный номер телефона, а также интересующую следствие выписку звонков абонента за конкретный промежуток времени.

Всё с той же целью по направлению запросов возможно с использованием интернет-ресурсов определить и IP-провайдера, если известен сам адрес IP. Для этого можно использовать сервис «Whoer» URL: https://whoer.net/ru/checkwhois, где в появившейся строке поиска нужно ввести четырехзначный номер IP, после чего он показывает информацию о регионе IP, о провайдере услуг связи, об организации и почтовый индекс.

Если известен IP-адрес, но требуется установить абонента и его контактные данные, то можно оформить запрос на получение информации о выходах в интернет. При этом нужно ссылаться на статьи Уголовно-процессуального кодекса РФ и ст. 64 Федерального закона от 07.07.2003 г. «О связи» № 126. Выдвигая требования, нужно указать IP-адрес лица, которое требуется установить, а также необходимые дату и время. Также нужно наиболее полно отразить, что потребуется предоставить оператору связи следователю, а конкретно: контактные данные абонента, логины, MAC-адреса сетевого оборудования, адрес фактического установления сетевого оборудования, номер договора на услуги использования сети передачи данных, способ подключения, а также сотовый номер мобильного телефона зарегистрированного абонента.

Возвращаясь к вопросу интернет-телефонии, стоит сказать следующее. Большинство звонков с подмененными номерами через SIP совершаются по VoIP-сетям и переводятся операторами без проверок принадлежности номера абонента. В настоящий момент порядок присоединения VoIP-сетей и телефонных сетей не урегулирован, как и не существует запрета на передачу IP-вызовов из сети и передачи данных на телефонную сеть. Отсутствие санкции за такое допущение является одной из причин совершения большинства мошеннических действий, несмотря на созданную банками систему «Антифрод» по оценке финансовых транзакций. Таким образом, нужно бороться не со следствием совершения мошенничества, а с условиями, порождающими причину совершения. Требуется на законодательном уровне предусмотреть ответственность для операторов связи за допущение подключения входящего интернет-звонка с сотовым телефоном без проверки на подлинность IP и абонентского номера вызывающего держателя.

Таким образом, вопрос установления личности преступника и его местоположения содержит в себе ряд технических и процессуальных аспектов для следователя. На сегодняшний день ему требуется быть не только юридически осведомленным по вопросам направления запросов в организации, но и также в техническом и информационном плане. При этом указанные способы не являются исчерпывающими и могут быть расширены возможностями технических подразделений МВД России при налаженных вопросах взаимодействия.

SIP-телефония является одним из средств совершения телефонных мошенничеств, которые на сегодняшний день остаются одними из самых не раскрытых и требующих большого количества времени для расследования этих категорий преступлений. Сервис по подмене абонентского номера и совершению звонков через интернет позволяет оставаться преступнику незамеченным, а в совокупности с умениями, подкрепленными знаниями о социальной инженерии, быть преуспевающим в своем деле.

Но след его действий в киберпространстве остается все так же четким. При должных умениях следователя в уголовно-процессуальной деятельности и знании законов, он способен по крупицам информации методом дедукции собрать полную, интересующую расследование информацию.

В заключение следует отметить, что при особенностях расследования мошенничества с использованием телефонной связи по протоколам VoIP и SIP такие звонки совершаются через преобразование подмененного номера в цифровом формате в сотовый. И что при до-

казывании факта хищения нужно обращаться не только на поиск злоумышленника, но также на доказывание факта хищения, который может быть выражен в информации, полученной от банков, операторов интернет и телефонной связи.

ЛИТЕРАТУРА

1. Краткая характеристика состояния преступности в Российской Федерации за январь – октябрь 2022 г. [Электронный ресурс]. – Официальный сай Министерства внутренних дел Российской Федерации: https: // xn--b1aew.xn--p1ai/reports/item/ 33913311/ (дата обращения: 02.01.2023).
2. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. – СПС «КонсультантПлюс».
3. Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 24.02.2023) [Электронный ресурс]. – СПС «КонсультантПлюс».
4. Kaspersky.Фишинг // [Электронный ресурс]. – URL: https://www. kaspersky. ru/resource-center/definitions/what-is-an-ip-address (дата обращения: 10.02.2023).
5. Сбербанк. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс]. – URL: http://www.cbr.ru/analytics/ib/review_2q_2022/ (дата обращения: 10.02.2023).
6. Митник К.Д. Искусство обмана / К.Д. Митник, В.Л. Саймон // Компания АйТи. – 2004. – 360 с.
7. Сайт Сбер. Как мошенники кол-центров общаются с потенциальными жертвами [Электронный ресурс]. – https://promo. sber.ru/kibrary#/ investigation/call-center (дата обращения: 12.02.2023).
8. Kaspersky. Определение IP-адреса [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-an-ip-address (дата обращения: 10.02.2023).
9. 3CX. Телефония [Электронный ресурс]. – URL: https://www.3cx.ru/voip-sip/voip-telephone/ (дата обращения: 16.12.2022).

УДК 621.396.41

МЕТОД НАХОЖДЕНИЯ ВЕКТОРОВ ХАРАКТЕРИСТИК JPEG ИЗОБРАЖЕНИЙ ДЛЯ ЗАДАЧИ СТЕГАНОАНАЛИЗА, ОСНОВАННЫЙ НА ПРИМЕНЕНИИ ЦЕПЕЙ МАРКОВА

А.В. Прокофьева, аспирант каф. ИБ ИКИТ СФУ

Научный руководитель А.Н. Шниперов, доцент каф. ИБ, к.т.н.

г. Томск, ТУСУР, prokofe-aleksandra@yandex.ru

Предложен метод нахождения вектора характеристик изображений, позволяющий эффективно детектировать наличие скрытой информации в JPEG-изображениях. Метод заключается в использовании матрицы переходных вероятностей и применении метода калибров-

ки изображения для повышения точности и уменьшения числа ложных срабатываний. Для каждого изображения из обучающей и тестовой выборки находится вектор характеристик, число элементов которого составляет 324. Далее на полученных данных из обучающей выборки обучается искусственная иммунная система. Для оценки качества классификации использовались следующие метрики: точность, величина ошибки первого и второго рода результатов бинарной классификации. Для встраивания скрытого сообщения использовался один из трех алгоритмов стеганографии: Steghide, OutGuess и nsF5. Предложенный подход нахождения вектора характеристик изображения позволяет детектировать наличие скрытого вложения в изображениях, полученных в результате применения неадаптивных методов стеганографии (Steghide, OutGuess и nsF5) с точностью более 95%.
Ключевые слова: стеганоанализ, Steghide, OutGuess, nsF5, бинарная классификация.

Традиционно множество методов стеганоанализа изображений разделяют на методы визуального поиска, сигнатурные, статистические и эвристические. Метод визуального поиска не предполагает средств автоматизации, аналитик просматривает изображения, выполняет различные преобразования (яркость, контрастность, цвет и т.д). Для работы с методами стеганографии, которые встраивают скрытое сообщение в поля формата файла (например, поле комментария) или оставляют специфические символьные последовательности, предназначены сигнатурные методы стеганоанализа. RS-стеганоанализ (Regular-Singular) и WS-стеганоанализ (Weighted Stego Image) [1] – примеры статистических методов, которые основаны на анализе статистических характеристик исследуемого изображения, а также гистограммный стеганоанализ [2] и другие подходы. Они в значительной степени зависят от метода стеганографии, который использовался для сокрытия сообщения, и против некоторых методов бывают нерезультативны. Эвристические методы стеганоанализа, напротив, не зависят от алгоритма стеганографии и зачастую основываются на применении методов машинного обучения (например, методы, предложенные в работах [3–5]), поэтому в большей степени применимы для использования на практике. Также можно привести пример атаки обратной совместимости [6], которая работает только для JPEG-изображений с качеством 99 и 100, но позволяет обнаруживать даже небольшие скрытые сообщения. В основе этой атаки лежит факт того, что изменения в квантованных коэффициентах дискретного косинусного преобразования (ДКП), появившиеся в результате встраивания скрытого

сообщения, увеличивают дисперсию гауссова распределения ошибок округления в пространственной области.

В работе [7] нами уже был представлен метод стеганоанализа изображений, в котором на этапе предобработки изображения вектор характеристик вычислялся с помощью вейвлет-преобразования Хаара. Его главным недостатком была недостаточная точность классификации изображений (75–80%): для применения в реальных информационных системах на практике этот показатель низкий и приводит к ложным срабатываниям и пропускам событий. Поэтому целью настоящей работы является повышение точности классификации изображения путем модификации метода предобработки и получения вектора характеристик изображения.

Получение вектора характеристик изображения. Предлагаемый метод основывается на нахождении матрицы переходных вероятностей изображения (subtractive pixel adjacency matrix), использовавшийся авторами в статьях [5, 9]. Вектор характеристик представляет собой марковский процесс как разницу между абсолютными значениями соседних коэффициентов ДКП, которому, как известно, подвергается каждый блок изображения при сжатии JPEG.

Итак, необходимо формализовать общую задачу метода стеганоанализа: пусть $I = C \cup S$ – множество изображений формата JPEG, S – множество заполненных стеганоконтейнеров, содержащих скрытое сообщение, C – множество пустых стеганоконтейнеров, два этих множества – взаимоисключающие: $S \cap C = \varnothing$. Каждое изображение $\text{img} \in I$ представлено вектором $\bar{D}$ его характеристик. Задача стеганоанализа изображения $\text{img} \in I$ заключается в решении задачи бинарной классификации о наличии скрытого вложения.

Суть предлагаемого метода заключается в том, что на основе матрицы коэффициентов ДКП изображения img размером $N \times M$, согласно (1), находятся четыре разностные матрицы соседних значений коэффициентов ДКП. На этом этапе они будут вычислены для четырех направлений: горизонтального, вертикального и диагонального направлений и направления побочной диагонали, которые обозначаются соответственно $F_h(u,v)$, $F_v(u,v)$, $F_d(u,v)$ и $F_m(u,v)$.

$$F_h(u,v) = F(u,v) - F(u+1,v), \quad F_v(u,v) = F(u,v) - F(u,v+1), \quad (1)$$
$$F_d(u,v) = F(u,v) - F(u+1,v+1), \quad F_m(u,v) = F(u+1,v) - F(u,v+1),$$

где $u \in [1, N-1]$, $v \in [1, N-1]$.

Далее на основе этих разностных матриц вычисляются матрицы переходных вероятностей согласно (2). Значение коэффициентов

ДКП изображения прогнозируется на основе соседних коэффициентов, а величина ошибки прогнозирования получается следующим образом: из значения исходного коэффициента вычитается значение предсказания. Затем полученное значение сравнивается с заранее заданным пороговым значением T (условимся, что $T = 4$). Число элементов вектора характеристик равно $4\times(2T + 1)^2$, следовательно, оно составляет 324.

Значения F_h, F_v, F_d и F_m округляются таким образом, чтобы они попадали в диапазон $[-T, T]$. По полученным значениям F_h, F_v, F_d и F_m рассчитываются матрицы вероятностей перехода $M_h(i, j)$, $M_v(i, j)$, $M_d(i, j)$ и $M_m(i, j)$. Приведем формулу расчета матрицы вероятностей перехода для горизонтального направления, для остальных направлений они получаются аналогичным образом:

$$M_h(i,j) = \frac{\sum_{v=1}^{N-1}\sum_{u=1}^{M-1}\delta\left[F_h(u,v)-i, F_h(u+1,v)-j\right]}{\sum_{v=1}^{N-1}\sum_{u=1}^{M-1}\delta\left[F_h(u,v)-i\right]}, \qquad (2)$$

где N, M – размеры изображения img, $i, j \in [-T, T]$.

Также предлагается использовать метод калибровки, который заключается в том, что изображение img с помощью ОДКП переводится в пространственную область, далее обрезается на четыре пикселя слева и снизу. Затем с помощью матрицы квантования исходного изображения img производится повторное сжатие. В результате получается изображение img′ формата JPEG, позволяющее получить отражение статистических свойств пустого стеганоконтейнера для анализируемого изображения. Для img′ находится вектор характеристик способом, рассмотренным выше. На следующем шаге каждую компоненту итогового вектора характеристик получаем как разность соответствующих компонент векторов откалиброванного и исходного изображений. На рис. 1 приведена общая схема получения вектора характеристик изображения.

Методика проведения эксперимента. Для обучения и тестирования методов классификации нами была использована база изображений IStego100K [8], состоящая из 208104 изображений размера 1024×1024. Среди них 200 тыс. изображений составляют обучающую выборку, а оставшиеся 8104 – тестовую выборку. Для каждого изображения коэффициенты качества JPEG различаются и находятся в диапазоне от 75 до 95. Встраивание производилось программно с помощью утилит Steghide, OutGuess для Linux и алгоритма nsF5 на языке Python.

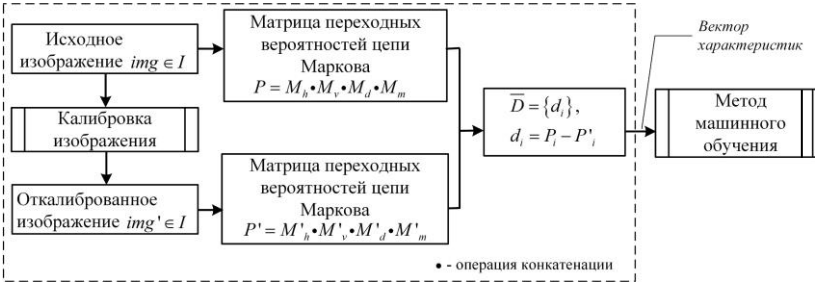


Рис. 1. Принцип нахождения вектора характеристик изображения

Алгоритмы Steghide, OutGuess и nsF5 [9] относятся к неадаптивным к содержимому изображения методам стеганографии, встраивание скрытого сообщения в изображение происходит последовательно. В алгоритме nsF5 встраивание не так сильно влияет на изменение гистограмм коэффициентов ДКП, поэтому данный метод не подвержен основным статистическим атакам и тем самым менее подвержен стеганоанализу. Алгоритмы J-UNIWARD [10] и UERD [11] являются на данный момент самыми надежными на сегодняшний день методами стеганографии с использованием минимальных искажений, в которых сообщение встраивается в наиболее зашумленные места изображения, и встраивание зависит от сложности текстуры.

Обучение и тестирование модели производилось на основе сочетания алгоритмов отрицательного и клонального отбора искусственной иммунной системы. Более подробно процесс классификации был описан в статье [7].

Результаты. Результаты сравнения работы данного метода нахождения векторов характеристик изображения и метода, основанного на нахождении вейвлет-преобразования Хаара, приведены в таблице.

Результаты сравнения точности классификации методов

Алгоритм стеганографии / Метод	Steghide	Outguess	nsF5
Точность обнаружения, %			
Вейвлет-преобразование Хаара [7]	71,1	74,5	74,9
Матрица переходных вероятностей	96,88	97,91	95,6
Величина ошибки I рода, %			
Вейвлет-преобразование Хаара [7]	26,3	16,5	17,1
Матрица переходных вероятностей	3,9	2,3	4,6
Величина ошибки II рода, %			
Вейвлет-преобразование Хаара [7]	31,5	34,5	32,9
Матрица переходных вероятностей	1,92	1,23	3,7

Видно, насколько более эффективно данный метод стал работать на неадаптивных алгоритмах стеганографии: точность обнаружения выросла более чем на 20%. Для заполненных контейнеров, полученных в результате встраивания сообщения одним из адаптивных методов (J-UNIWARD, UERD), показатели точности обнаружения не приведены в таблице, поскольку пока находятся в пределах 50–60%, что требует доработки в дальнейших исследованиях.

Заключение. В результате данной работы были улучшены показатели точности классификации изображения путем применения метода нахождения матрицы переходных вероятностей и метода калибровки изображения. Предложенный подход позволяет детектировать наличие скрытого вложения в изображениях, полученных в результате применения неадаптивных методов стеганографии (Steghide, OutGuess и nsF5) с очень высокой точностью более 95%. Также данный метод нахождения вектора характеристик позволяет классифицировать изображение за очень короткий промежуток времени (до 250 мс), что является вполне приемлемым для использования на практике.

ЛИТЕРАТУРА

1. Gulášová M. Steganalysis of stegostorage library / M. Gulášová, M. Jókay // Tatra Mountains Mathematical Publications. – 2016. – Vol. 67, No. 1. – PP. 99–116. DOI: 10.1515/tmmp-2016-0034.

2. Fridrich J.J. Steganalysis of JPEG Images: Breaking the F5 Algorithm / J.J. Fridrich, M. Goljan, D. Hogea // 5th International Workshop on Information Hiding. – 2002. DOI: 10.1007/3-540-36415-3.

3. Hendrych J. Advanced methods of detection of the steganography content / J. Hendrych, L. Ličev // Lecture Notes in Electrical Engineering. – 2020. – Vol. 554. – PP. 484–493. DOI: 10.1007/978-3-030-14907-9_47.

4. Yousfi Y. et al. Breaking Alaska: Color separation for steganalysis in JPEG domain // IH and MMSec 2019. – Proceedings of the ACM Workshop on Information Hiding and Multimedia Security. – 2019. – PP. 138–149. DOI: 10.1145/3335203.3335727.

5. Saito T. Second Level Steganalysis – Embeding Location Detection Using Machine Learning / T. Saito, Q. Zhao, H. Naito // 2019 IEEE 10th International Conference on Awareness Science and Technology, iCAST 2019. – Proceedings. IEEE, 2019. – PP. 1–6. DOI: 10.1109/ICAwST.2019.8923205.

6. Butora J. Reverse JPEG Compatibility Attack / J. Butora, J. Fridrich // IEEE Transactions on Information Forensics and Security. IEEE. – 2020. – Vol. 15. – PP. 1444–1454. DOI: 10.1109/TIFS.2019.2940904.

7. Shniperov A.N. Steganalysis Method of Static JPEG Images Based on Artificial Immune System / A.N. Shniperov, A.V. Prokofieva // Automatic Control and Computer Sciences. – 2020. – Vol. 54, No. 5. DOI: 10.3103/S014641162005 0077.

8. Yang Z. et al. IStego100K: Large-scale Image Steganalysis Dataset // Digital Forensics and Watermarking. IWDW 2019. Lecture Notes in Computer Science. – 2019. – Vol. 12022. doi.org/10.1007/978-3-030-43575-2_29

9. Fridrich J. Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities / J. Fridrich, T. Pevný, J. Kodovský // MM and Sec'07 – Proceedings of the Multimedia and Security Workshop 2007. – 2007. DOI: 10.1145/1288869.1288872.

10. Holub V., Fridrich J., Denemark T. Universal distortion function for steganography in an arbitrary domain / V. Holub, J. Fridrich, T. Denemark // Eurasip Journal on Information Security. – 2014. – Vol. 2014. DOI: 10.1186/1687-417X-2014-1.

11. Guo L. et al. Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited // IEEE Transactions on Information Forensics and Security. – 2015. – Vol. 10, No. 12. DOI: 10.1109/TIFS.2015.2473815.

УДК 004.49

ОЦЕНКА УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

С.В. Селигеев, магистрант каф. БИТ

Научный руководитель В.Г. Жуков, доцент каф. БИТ, к.т.н.

г. Красноярск, СибГУ им. М.Ф. Решетнева, seligeevsergei@gmail.com

Рассматривается практическая применимость методики оценки критичности уязвимостей ФСТЭК для решения задачи приоритезации в рамках управления уязвимостями программных, программно-аппаратных средств в информационной системе, а также анализируются существующие сложности расчёта.

Ключевые слова: уязвимость, CVSS, приоритезация.

В рамках оценки уровня критичности уязвимостей программных, программно-аппаратных средств в информационной системе можно выделить три основные проблемы:

1) низкая эффективность используемых подходов к приоритезации уязвимостей;

2) закрытие каналов обновлений программного обеспечения, сетевого оборудования и других элементов информационной системы и системы защиты информации в связи с геополитической обстановкой;

3) высокая гетерогенность информационных систем.

Наиболее наглядно первые две проблемы отражает отчет Positive Tecnologies «Итоги пентестов – 2022» [1]. При проведении исследования анализировалось 53 проекта в 30 организаций. В рамках анализа

на пентестеров не накладывались существенные ограничения, что позволило получить объективные оценки уровня защищенности. Стоит отметить, что рассмотренные организации занимаются различными отраслями, что позволяет рассмотреть общую картину. Проводились как внутренние, так и внешние пентесты. В итоге был получен следующий результат:

1) 96% протестированных организаций не защищены от проникновения внешнего злоумышленника;

2) 100% исследованных организаций не защищены от установления внутренним злоумышленником полного контроля над ИТ-инфраструктурой;

3) удалось подтвердить возможность реализации 89% недопустимых событий, обозначенных организациями;

4) в 7% организаций обнаружены следы компрометации.

Также из опроса Positive Technologies «Как изменилась работа с уязвимостями в 2022 году» [2], участие в котором принимали 200000 человек, стало известно, что 52% опрошенных доверяют оценке CVSS, в свою очередь, в отчете компании Kenna «Measuring and Minimizing Exploitability» [3], выпущенном совместно с институтом Cyentia, оценка CVSS не особо отличается от случайного устранения обнаруженных уязвимостей, снижая уровень уязвимостей в 2–6 раз. Так, например, использование данных о наличии эксплойта снижает уровень уязвимости в 22–29 раз.

Высокая гетерогенность информационных систем обусловлена тем, что во многих организациях они сложились со временем и их изменение может происходить постепенно для того, чтобы минимизировать влияние на бизнес-процесс. А также у многих организаций отсутствует финансовая возможность построения информационных систем на экосистемах известных вендоров для понижения гетерогенности.

Актуальность проблемы также показывает изменение подходов к управлению уязвимостями в течение 2022 г., которое можно увидеть в опросе [2]. Наблюдается сокращение доли компаний, не использующих специализированное программное обеспечение для работы с уязвимостями с 26% (2020 г.) до 11%. Так же 74% опрощенных изменили подход патч-менеджменту с февраля 2022 г.

Таким образом, существует потребность в практическом решении задачи приоритезации уязвимостей. Данные, полученные в ходе решения, должны позволять строить планы устранения уязвимостей с учетом ограниченного времени устранения и человеческого ресурса. В идеальной ситуации решение для приоритизации должно быть до-

ступно для применения в автоматезированном режиме, уменьшать охват необходимых к устранению уязвимостей, например, учитывать реальную статистику применения.

Методика оценки критичности ФСТЭК России. Исходя из высокой необходимости в инструментах приоритезации ФСТЭК России разработал и рекомендовал к применению методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств» [4]. Расчёт критичности уязвимости в соответствии с методикой происходит по следующей формуле:

$$V = I_{\text{CVSS}} \times I_{\text{inf}}\, r, \quad (1)$$

где I_{CVSS} – показатель, характеризующий уровень опасности уязвимости. Данный параметр численно представляет собой результат оценки уязвимости по контекстному вектору CVSS.

Показатель $I_{\text{inf}}\, r$ характеризует влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы. Данный показатель рассчитывается по следующей формуле:

$$I_{\text{inf}}\, r = k \times K + l \times L + p \times P, \quad (2)$$

где K – показатель, характеризующий тип компонента информационной системы, подверженного уязвимости; L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов); P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы; k, l, p – весовые коэффициенты показателей.

Расчет весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на информационную систему, проводится в соответствии с табл. 1.

В итоге полученная количественная оценка переводится из количественной в качественную в соответствии с табл. 2.

Сложности применения методики. Показатель Icvss предполагает использование оценки по контекстному вектору CVSS [5]. Методика в качестве варианта получения данной оценки предлагает применять калькулятор Банка данных угроз безопасности информации ФСТЭК России. Если расчет оценки для десятка уязвимостей не займет много времени, то расчет в реальных условиях для сотни или тысячи уязвимостей (даже при условии их группировки) является более трудоемкой задачей, так как на данный момент времени нет инструментов для автоматизации расчётов оценок по контекстному вектору CVSS.

Таблица 1

Оценки показателей

№ п/п	Показатель	Вес	Значение	Оценка	Итог
1	Тип компонента информационной системы, подверженного уязвимости (*K*)	0,4	Уязвимости подвержены компоненты информационной системы, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий	1	0,4
			Уязвимости подвержены серверы	0,8	0,32
			Уязвимости подвержено телекоммуникационное оборудование, система управления сетью передачи данных	0,8	0,32
			Уязвимости подвержены автоматизированные рабочие места	0,5	0,20
			Уязвимости подвержены другие компоненты	0,5	0,20
2	Количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов) (*L*)	0,2	Более 70% компонентов от общего числа компонентов в информационной системе	1	0,2
			50–70% компонентов от общего числа компонентов в информационной системе	0,8	0,16
			10–50% компонентов от общего числа компонентов в информационной системе	0,6	0,12
			Менее 10% компонентов от общего числа компонентов в информационной системе	0,5	0,10
3	Влияние на эффективность защиты периметра системы, сети (*P*)	0,4	Уязвимое программное, программно-аппаратное средство доступно из сети Интернет	1	0,4
			Уязвимое программное, программно-аппаратное средство недоступно из сети Интернет	0,5	0,2

Таблица 2

Перевод баллов в качественную оценку

Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
$7{,}0 \le V \le 10{,}0$	Критичный
$4{,}5 \le V < 7{,}0$	Высокий
$1{,}5 \le V < 4{,}5$	Средний
$V < 1{,}5$	Низкий

Стоит отдельно показать проблемы получения данных для временного и контекстного вектора CVSS. Во временном векторе необходимо получить данные о состоянии эксплойта, о состоянии исправления и о данные о подтверждении уязвимости. Для наглядности в табл. 3 приведены возможные значения метрик и их веса.

Таблица 3

Возможные значения временной группы метрик

Наименование метрики	Качественное значение метрики	Численное значение метрики
Exploit Code Maturity (состояние эксплойта)	Not Defined	1
	High	1
	Functional	0,97
	Proof of Concept	0,94
	Unproven	0,91
Remediation Level (состояние исправления)	Not Defined	1
	Unavailable	1
	Workaround	0,97
	Temporary Fix	0,96
	Official Fix	0,95
Report Confidence (данные о подтверждении уязвимости)	Not Defined	1
	Confirmed	1
	Reasonable	0,96
	Unknown	0,92

В лучшем случае подобная информация может быть изъята из отчетов сканеров безопасности путем их парсинга, но в данном случае вполне вероятно, что для большего числа известных уязвимостей подобных данных во внутренних источниках сканеров безопасности может не быть в полном объеме. Вторым вариантом будет использование агрегаторов данных об уязвимостях, таких как Prion Knowledge Base [6] или SCORES [7]. Информацию из данных источников можно получить вручную или с помощью API при использовании платных версий. Но для некоторых уязвимостей получить полный набор данных для временного вектора с помощью подобных сервисов тоже не

всегда возможно. В таких случаях для возможности наибольшей корректировки критичности необходимо вручную анализировать специализированные источники для получения значений метрик, а это значительно увеличивает время оценки уязвимости.

Для контекстной группы метрик также существует проблема автоматизированного получения данных. Оптимальным решением данной проблемы является модернизация карточек активов в системе менеджмента активов, а именно добавление пользовательских полей, содержащих значение метрик контекстного вектора. Данные метрики для наглядности приведены в табл. 4.

Таблица 4

Возможные значения контекстной группы метрик

Наименование метрики	Качественное значение метрики	Численное значение метрики
Modified Attack Vector (Модифицированный вектор атаки)	Network Adjacent Local Physical	0,85 0,62 0,55 0,2
Modified Attack Complexity (Модифицированная сложность атаки)	Low High	0,77 0,44
Modified Privilege Required (Модифицированные привилегии, необходимые для выполнения атаки)	None Low High	0,85 0,62 (0,68) 0,27 (0,50)
Modified User Interaction (Модифицированная необходимость взаимодействия с пользователем)	None Required	0,85 0,62
Modified C, I, A Impact (Модифицированное влияние на свойства безопасности информации)	High Low None	0,56 0,22 0
Security Requirements – C, I, A Requirements (Требования к информационной безопасности)	Not Defined High Medium Low	1 1,5 1 0,5

Выполнение этой процедуры для каждого компонента, подверженного уязвимостям, требует затрат значительных ресурсов и времени, а также периодического пересмотра, так как инфраструктура в течение времени может изменяться. Так, требования к свойствам безопасности можно интерпретировать из требований безопасности, которые устанавливаются к информационной системе. Модифицированные базовые метрики же складываются из особенностей размещения компонента в инфраструктуре и его конфигурации. Наиболее приближенной к реальности выглядит ситуация, в которой процедура модификации свойств выполнена для групп активов, а при оценке

критичности для конкретного актива вносятся необходимые корректировки.

Для дальнейших рассуждений и наглядности проведем расчет нескольких высокоэксплуатируемых уязвимостей. Данные о используемых уязвимостей взяты из отчета «A Year in Review 2022: 100 vulnerabilities you should prioritize» [8] компании Prion. Первые три уязвимости из списка принадлежат продуктам Microsoft, а именно CVE-2022-41040 (Windows), CVE-2022-41082 (Microsoft Exchange Server 2013), CVE-2022-30190 (Windows). Расчет контекстного вектора, а также оценка по методике приведены на рис. 1. Значения метрик были выбраны субъективно для демонстрации общей сути процесса контекстной оценки.

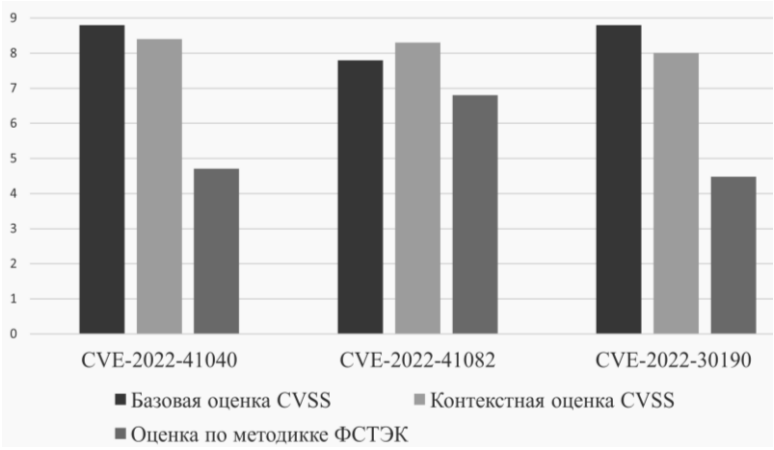


Рис. 1. Диаграмма оценок уязвимости

Также для большего понимания в табл. 5 приведены полные векторы CVSS v3 для каждой из приведенных уязвимостей, а в табл. 6 – значения метрик показателя I_{inf} *r*.

Теперь стоит поговорить о показателе I_{inf} *r*. Каждый компонент данного показателя стоит рассмотреть в отдельности.

Так, в компоненте K присутствует дифференциация только по уровню вхождения в сетевую инфраструктуру (критические системы, серверы, АРМы и т.д.). В данном случае методика не рассматривает дифференциацию по функционалу, выполняемому компонентами системы. Так, например, сетевое оборудование может использоваться на уровне ядра и быть особо критичным для организации, а в то же время другое оборудование будет обеспечивать уровень доступа для не-

значительных в рамках ИС рабочих мест. Но в любом случае в этих двух разных по критичности ситуациях по компоненте K будет получена одна и та же оценка. В качестве альтернативы можно использовать двумерную оценку по компоненте K при помощи матрицы, в которой по столбцам происходит дифференциация – по вхождению в сетевую инфраструктуру, а по строкам дифференциация по функционалу. Ячейки данной матрицы содержат оценки в соответствии с методикой от 0,2 до 0,4. Пример подобной матрицы с оценками, расставленными субъективно, приведен в табл. 7, данный пример стоит воспринимать только как иллюстрацию для большего понимания предлагаемой идеи.

Таблица 5

Векторы CVSS v3 для рассматриваемых уязвимостей

Код уязвимости	Вектор CVSS v3
CVE-2022-41040	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C /CR:M/IR:M/AR:M/MAV:A/MAC:L/MPR:L/MUI:N/MS: C/MC:H/MI:H/MA:H
CVE-2022-41082	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C /CR:M/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:R/MS: C/MC:H/MI:H/MA:H
CVE-2022-30190	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C /CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS: C/MC:H/MI:H/MA:H

Таблица 6

Значения метрик показателя I_{inf} *r*

Код уязвимости	Компонента K	Компонента L	Компонента P
CVE-2022-41040	0,2	0,16	0,2
CVE-2022-41082	0,32	0,1	0,4
CVE-2022-30190	0,2	0,16	0,2

Таблица 7

Пример матрицы компоненты *K*

	Сервер	Сетевое оборудование	АРМ	Иное оборудование (принтеры, контролёры и т.д.)
Критические процессы	0,4	0,4	0,35	0,25
Управление	0,4	0,35	0,3	0,25
Основные задачи	0,3	0,25	0,25	0,2
Удобство пользователей	0,2	0,2	0,2	0,2

В рамках второй компоненты *L* присутствует проблема корреляции с компонентой *K*. По логике компоненты чем больше активов подвержено уязвимости, тем она критичнее. Но рассмотрим обратную ситуацию, например, в инфраструктуре присутствует сервер, простой или выход из строя которого особо негативно скажется на бизнес-процессе, или же сетевое оборудование, образующее ядро локальной сети. Обычно подобных активов в сравнении с другими гораздо меньше, но присутствие уязвимости в них гораздо критичнее, чем, например, в рабочих местах пользователей, которые как раз могут составлять более 70 процентов активов. В приведенной ситуации данные активы имеют высокую оценку по компоненте *K* и низкую по компоненте *L*, тем самым происходит коллизия, приводя оценку к среднему значению.

Последняя компонента P фактически повторяет метрику Modified Attack Vector (MAV) в контекстном векторе CVSS, так как именно значение этой метрики учитывает доступность или невозможность использования уязвимости из сети Интернет. Рассмотрим влияние этой компоненты на примере CVE-2022-41040, меняя метрику MAV и компоненту *P*. Изменения оценок приведены на рис. 2.

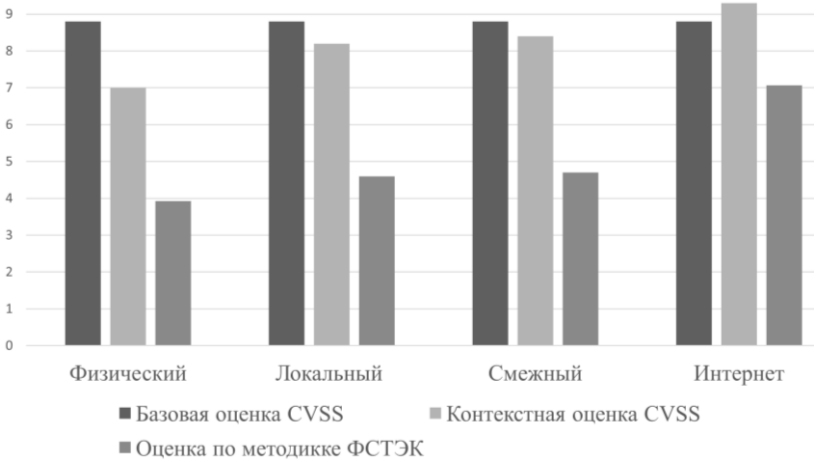


Рис. 2. Влияние компоненты *P*

В случаях, когда актив не доступен из сети Интернет, критичность уязвимости падает до высокого или среднего уровня. Но при этом фактически существуют данные о том, что эта уязвимость реально использовалась, и об этом написаны подробные технические отче-

ты, иначе говоря, опасность данной уязвимости принята сообществом. Но в соответствии с методикой на ее устранение выделяется от 7 дней до 4 недель. Выглядит так, будто этот показатель искусственно понижает критичность уязвимости.

С доступностью из сети Интернет другая ситуация. В данном случае MAV повышает опасность уязвимости, а компонента P снова ее понижает, оказывая большее влияние. В этом случае пропадает польза корректирующего воздействия контекстного вектора CVSS.

Сложности, описанные выше, касались логики расчета критичности. Но существуют проблемы и в дальнейших этапах процесса управления уязвимостями. Полученная критичность показывает опасность уязвимости для конкретной инфраструктуры и является входными данными для процесса построения плана устранения уязвимостей. Помимо критичности, при построении плана устранения учитываются и другие данные, такие как критичность актива, наличие эксплойта, сведения о реальных атаках и другие факторы. И только после построения плана специалист приступает к непосредственному устранению. Однако методика предлагает принятие мер защиты, отталкиваясь лишь от критичности, полученной в рамках расчётов.

Для критичных уязвимостей рекомендуется принятие по их устранению в течение часов (до 24 ч). В качестве путей устранения предлагается установка обновления программного обеспечения, программно-аппаратного средства или принятия компенсирующих организационных и технических мер защиты информации. При этом обновления для зарубежных программных, программно-аппаратных средств или программного обеспечения с открытым исходным кодом должно быть проведено тестирование обновления в соответствии с методикой тестирования обновлений безопасности программных, программно-аппаратных средств [9], утвержденной ФСТЭК России от 28 октября 2022 г.

Соответственно, для оперативного устранения критических уязвимостей (в идеальной ситуации) необходимо проводить сканирования раз в 12 ч для получения достаточного временного окна для устранения. Количество времени на расчёт критичности в рамках примера будет прямо зависеть от количества уязвимостей в отчете сканеров, и при числе в 100 уязвимостей подобный расчет даже в полуавтоматическом режиме может занять длительное время. Следующим шагом является проверка наличия обновления и информации по его тестированию. Если обновление не протестировано, то этот процесс также займет значительное количество времени. Остаются компенсирующие меры, но так как они могут также повлиять на бизнес-

процесс (что касается и обновлений), необходимо согласование их применения, на что также необходимо время.

В итоге устранение критических уязвимостей, даже если опустить сканирование раз в 12 ч, выглядит сложной, невыполнимой задачей.

Заключение. Так как данная методика подлежит применению операторами информационных систем при принятии ими мер по устранению уязвимостей программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, а также иными нормативными правовыми актами и методическими документами ФСТЭК России, не применять ее в автоматизированном режиме затруднительно. Но исходя из рассмотренных проблем сложно сказать о том, что результаты, полученные в ходе расчётов, являются показательными и объективными оценками критичности. Однако стоит отметить, что формализация подхода к приоритезации является позитивным шагом в развитии данного направления, так как валидация результатов расчётов критичности упрощается, в отличие от проверки подходов, созданных специалистами самостоятельно в ходе жизненного цикла управления информационной безопасностью.

ЛИТЕРАТУРА

1. Итоги пентестов – 2022 [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/ (дата обращения: 01.03.2023).

2. Как изменилась работа с уязвимостями в 2022 году [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/kak-izmenilas-rabota-s-uyazvimostyami-v-2022-godu/ (дата обращения: 01.03.2023).

3. Measuring and Minimizing Exploitability [Электронный ресурс]. – Режим доступа: https://learn-cloudsecurity.cisco.com/kenna/prioritization-to-prediction-volume-8#page=1 (дата обращения: 01.03.2023).

4. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/3458 (дата обращения: 01.03.2023).

5. Common Vulnerability Scoring System version 3.1 Specification Document Revision 1 [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (дата обращения: 01.03.2023).

6. Prio-n Knowledge Base [Электронный ресурс]. – Режим доступа: https://kb.prio-n.com/ (дата обращения: 01.03.2023).

7. SCORES (Seconize Contextual Risk Enumeration Sys-tem) [Электронный ресурс]. – Режим доступа: http://www.ngtp.ru/rub/4/31_2014.pdf (дата обращения: 01.03.2023).

8. A Year in Review 2022: 100 vulnerabilities you should prioritize [Электронный ресурс]. – URL: https://riskscore.info/ (дата обращения: 01.03.2023).

9. Методика тестирования обновлений безопасности программных, программно-аппаратных средств [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/3456 (дата обращения: 01.03.2023).

ПОДСЕКЦИЯ 4.2

ЦИФРОВЫЕ СИСТЕМЫ РАДИОСВЯЗИ И СРЕДСТВА ИХ ЗАЩИТЫ

*Председатель – **Голиков А.М.**, доцент каф. РТС, к.т.н.*

УДК 621.376

ЗАЩИЩЕННАЯ ЦИФРОВАЯ СИСТЕМА ТРАНКИНГОВОЙ РАДИОСВЯЗИ DMR НА БАЗЕ БЕСПИЛОТНОЙ АЭРОПЛАТФОРМЫ

В.В. Барсуков, магистрант;
О.В. Лемзя, М.М. Муруева, студенты каф. РТС
Научный руководитель А.М. Голиков, к.т.н., с.н.с., доцент каф. РТС
Проект ГПО РТС-2201. Проектирование автономной системы сотовой связи и передачи данных Private Networks 3G/4G/5G
г. Томск, ТУСУР, rts2_golikov@mail.ru

Проведена разработка технического предложения для создания защищенной цифровой транкинговой системы радиосвязи DMR на базе мобильной быстроразворачиваемой беспилотной аэроплатформы. Рассмотрены ключевые аспекты сети, преимущества и развитие стандарта DMR. Проведен анализ рынка оборудования, необходимого для создания проектируемого комплекса стандарта DMR на базе беспилотной аэроплатформы. Разработана MatLab-модель для исследования модуляции M-FSK, обеспечивающей работу сети на низких уровнях сигнала. Рассчитана зона покрытия, позволяющая узнать радиус действия мобильной станции. Проведен энергетический расчёт «зон видимости», подтверждающий работоспособность модуля полезной нагрузки в части оборудования сотовой связи.
Ключевые слова: DMR, TDMA, модуль полезной нагрузки, базовая станция, сотовая связь, помехоустойчивость, FSK, криптошлюз.

Создание DMR (Digital Mobile Radio), бесспорно, явилось очередным этапом в усовершенствовании средств высокопрофессиональной двухсторонней радиосвязи. Стандарт ETSI DMR обеспечивает ряд неоспоримых преимуществ всем пользователям профессиональных систем связи.

Проведено моделирование сигналов DMR (рис. 1–3).

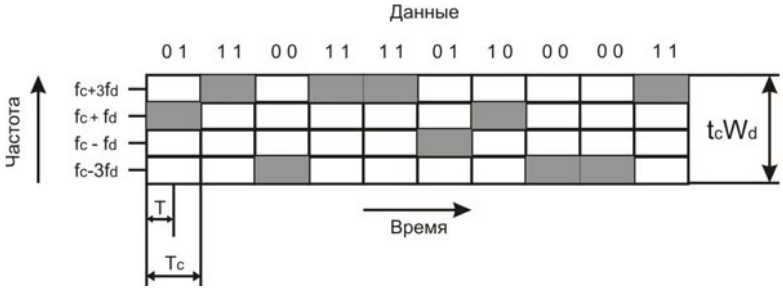


Рис. 1. Использование частоты схемой MFSK (M = 4)

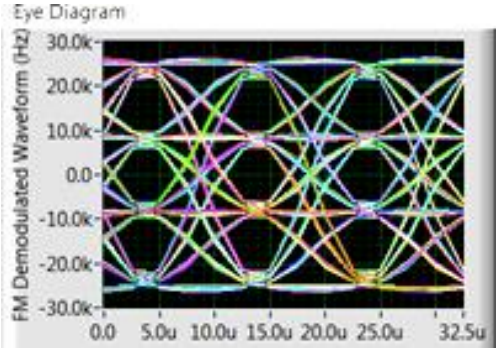


Рис. 2. Глазковые диаграммы при уровне модуляции M = 4

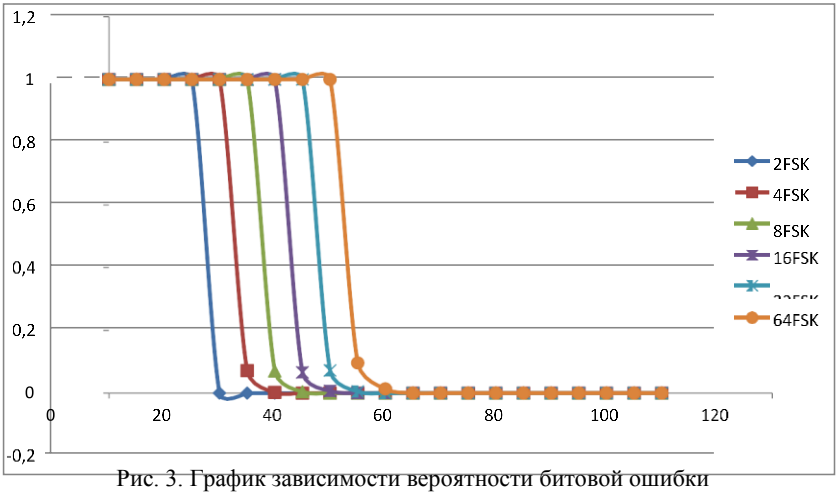


Рис. 3. График зависимости вероятности битовой ошибки
от отношения сигнал/шум для разных видов модуляций FSK

Было разработано предложение по аппаратной реализации цифровой системы транкинговой радиосвязи DMR на базе беспилотной аэроплатформы, для этого был изучен рынок производителей оборудования и программного обеспечения для реализации данных сетей. Защита информации проводится с использованием криптошлюза.

ЛИТЕРАТУРА

1. Голиков А.М. Цифровые системы связи и передачи данных: учеб. пособие [Электронный ресурс]. – Томск: ТУСУР, 2022. – 422 с. – Режим доступа: https://edu.tusur.ru/publications/10135

УДК 621.376

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ЦИФРОВЫХ РАДИОРЕЛЕЙНЫХ СИСТЕМ

В.И. Верхоланцев, студент каф. РТС

Научный руководитель А.М. Голиков, к.т.н., с.н.с., доцент каф. РТС

Проект ГПО РТС-2205. Проектирование линейки цифровых систем сотовой связи и передачи данных на базе мобильной быстроразворачиваемой беспилотной аэроплатформы

г. Томск, ТУСУР, rts2_golikov@mail.ru

Проведено проектирование и исследование ЦРРЛ, пролегающей между двумя газовыми месторождениями, относящимися к газопроводу «Сила Сибири», – ПАО «Газпром». В ходе проектирования было использовано оборудование МИК-РЛ Н500.

Ключевые слова: МИК-РЛ Н500, ЦРРЛ, Radio Mobile.

Система радиорелейной связи МИК-РЛ Н500 полностью внутреннего размещения – флагман семейства систем «МИК-РЛ», в котором воплотились самые передовые достижения инженерной мысли для создания магистральных многоствольных линий связи с максимальной надежностью и устойчивостью. Размещение внутри отапливаемых помещений позволяет круглый год комфортно и оперативно обслуживать аппаратуру и обеспечивать высочайший коэффициент готовности ЦРРЛ.

Ключевые характеристики МИК-РЛ Н500:

- Диапазон частот, 4,40…8,40 ГГц.
- Пропускная способность 89,6…448,0 Мбит/с.
- Мощность передатчика 35 Вт.

В процессе выполнения работы с помощью ПО Radio Mobile была построена линия связи с использованием системы МИК-РЛ Н500, предназначением которой было обеспечение стабильной связи между

Ковыктинским и Чаяндинским газовыми месторождениями. По итогам моделирования мы можем сделать вывод, что для установки стабильной связи между месторождениями потребуется 11 ретранслирующих станций между приемником и передатчиком, расположенными непосредственно на самих месторождениях. Также в некоторых местах возможно снижение высоты антенн для создания полузакрытых трасс без потери качества связи.

На рис. 1 изображен общий план сети.

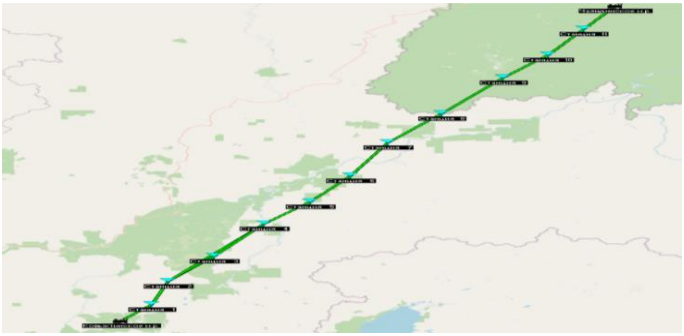


Рис. 1. ЦРРЛ газопровода «Сила Сибири»

Общая протяженность сети около 700 км. Передающая и принимающая станции расположены на месторождениях, между ними с интервалом в 50 км с учетом рельефа расположены ретранслирующие станции. Интервал варьируется в зависимости от сложности рельефа. Высота каждой из станций едина – 150 м.

На протяжении всей линии связи был отдельно рассмотрен каждый участок трассы, а также собрана статистика каждого из радиоканалов. Так, на рис. 2 мы можем видеть профиль канала связи между Ковыктинским месторождением и первым ретранслятором.

На данных изображениях мы также можем видеть основные параметры системы.

Как упоминалось ранее, ПО Radio Mobile позволяет не только оценить качество сигнала и графически изобразить профиль рельефа, но и показать статистику по отдельно выбранному радиоканалу, как показано на рис. 3.

Так, в ходе работы было проведено исследование каждого из участков системы связи, также стоит заметить, что местоположение каждой из антенн было выбрано с учетом данных карты высот (SRTM), загружаемой в приложение.

Таким образом, в результате проведения проектирования и исследования была построена рабочая модель сети, проведено исследование стабильности передаваемого и принимаемого сигнала. Это поз-

волит с помощью ПО Radio Mobile проектировать сети для различных областей применения.

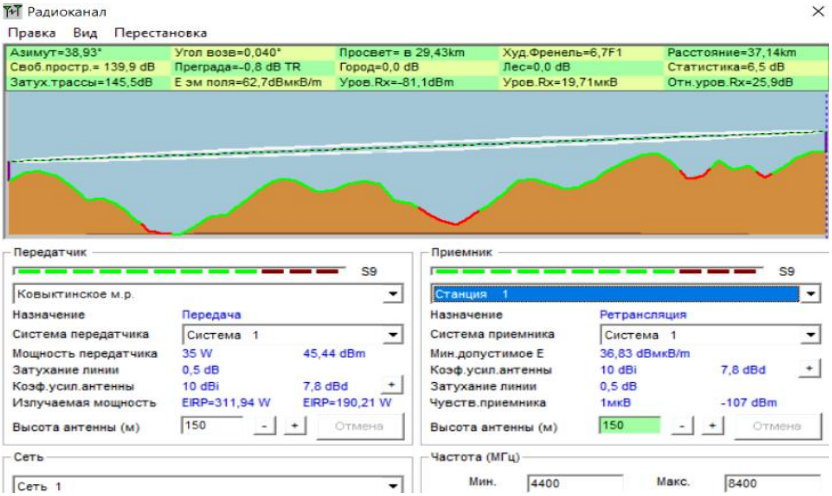


Рис. 2. Канал связи между Ковыктинским месторождением и первым ретранслятором

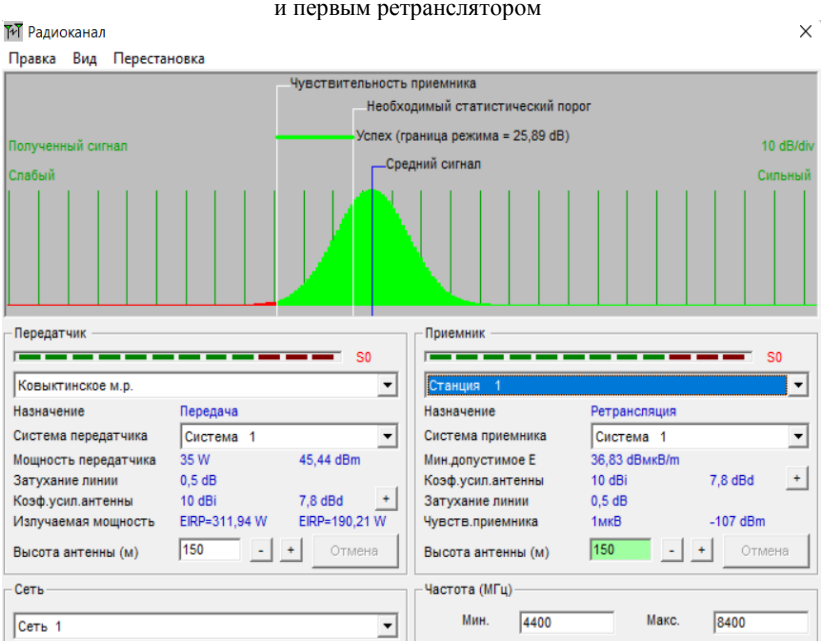


Рис. 3. Статистические данные трассы

ЛИТЕРАТУРА

1. Голиков А.М. Цифровые системы связи и передачи данных: учеб. пособие [Электронный ресурс]. – Томск: ТУСУР, 2022. – 422 с. – Режим доступа: https://edu.tusur.ru/publications/10135

УДК 621.376

МОДЕЛЬ LORA-МОДУЛЯТОРА ДЛЯ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ

А.М. Петров, магистрант каф. РТС

Научный руководитель А.М. Голиков, с.н.с., доцент каф. РТС, к.т.н.

г. Томск, ТУСУР, rts2_golikov@mail.ru

Разработана Matlab-модель модулятора LoRa для сети LoRaWAN. Проведено исследование помехоустойчивости модулятора для различных типов каналов передачи данных. Исследованы зависимости BER от E_b/N_0 для разных коэффициентов расширения (SF) в различных типах каналов передачи.

Ключевые слова: LoRa, LoRaWAN, модуляция, интернет вещей, помехоустойчивость, E_b/N_0.

LoRaWAN – открытый протокол сетей с большим радиусом действия, большим количеством устройств и низким потреблением. Данный протокол разработан LoRa Alliance. Одной из ключевых особенностей протокола является применение LoRa-модуляции, позволяющей передавать сигнал ниже уровня шума [1]. На рис. 1 представлена структурная схема глобальной IoT-сети с использованием LoRa.

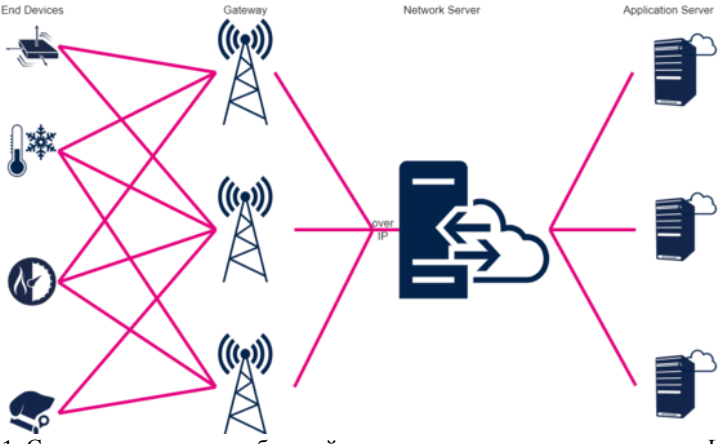


Рис. 1. Структурная схема глобальной сети с использованием технологии LoRa

Модуляция LoRa является подвидом линейной частотной модуляции (ЛЧМ). Каждый символ кодируется циклическим сдвигом чирпа (гармонического сигнала с линейно возрастающей частотой) во времени. Параметрами LoRa-модуляции являются полоса пропускания и коэффициент расширения SF. Коэффициент расширения определяет число N чирпов для передачи символа: $N = 2^{SF}$ [2]. На рис. 2 представлен спектр одиночного ЛЧМ-импульса, или чирпа.

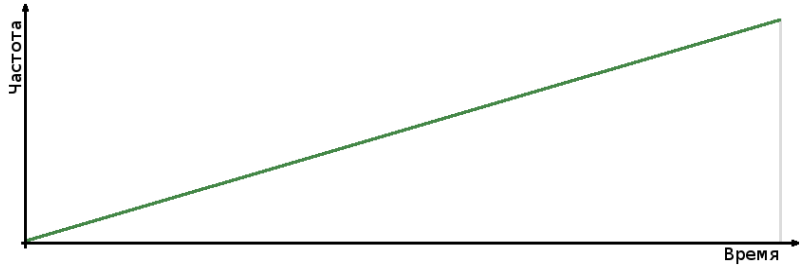


Рис. 2. Спектр одиночного ЛЧМ-импульса (чирпа)

Для исследования помехоустойчивости LoRa-модулятора была разработана Matlab-модель. Блок-схема разработанного алгоритма представлена на рис. 3.

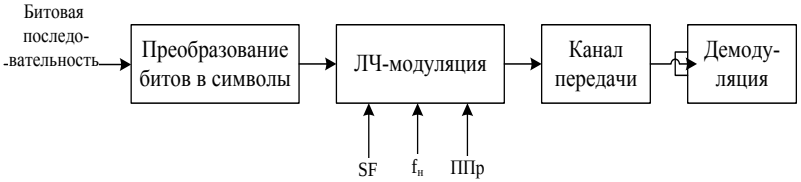


Рис. 3. Блок-схема алгоритма

Помимо измерения помехоустойчивости, был также изучен спектр сигнала с LoRa-модуляцией при разных коэффициентах расширения. Полученные спектры представлены на рис. 4.

В ходе исследования были получены водопадоподобные кривые помехоустойчивости сигнала с LoRa-модуляцией с различными SF. Данные кривые представлены на рис. 5.

Итогом работ стала разработка блок-схемы алгоритмов для исследования LoRa-модулятора, а также программного кода для ПО MatLab. Из графиков видно, что при увеличении коэффициента расширения увеличивается помехоустойчивость модулированного сигнала.

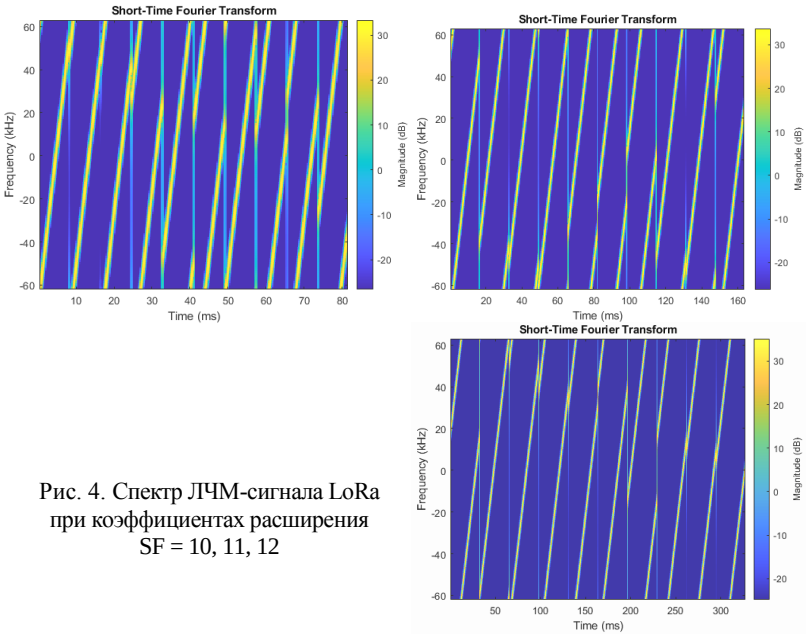


Рис. 4. Спектр ЛЧМ-сигнала LoRa при коэффициентах расширения SF = 10, 11, 12

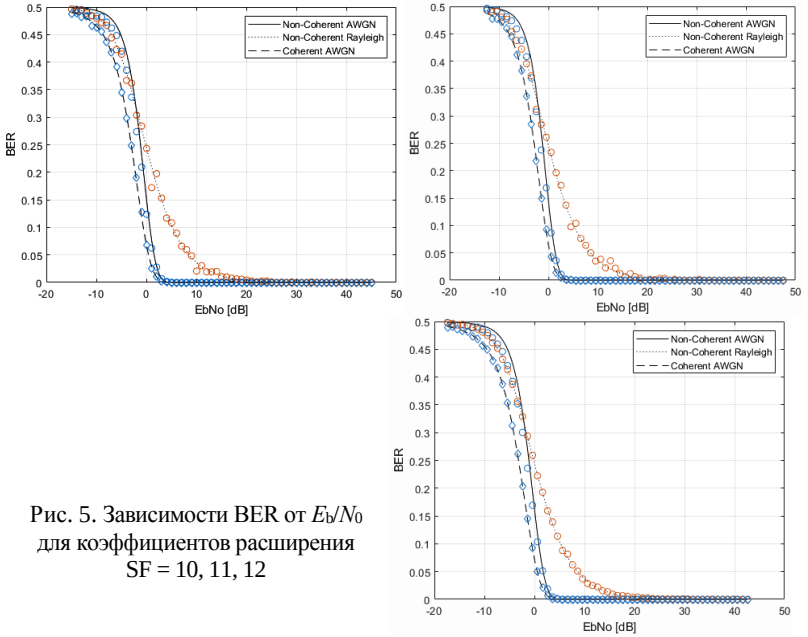


Рис. 5. Зависимости BER от E_b/N_0 для коэффициентов расширения SF = 10, 11, 12

ЛИТЕРАТУРА

1. Голиков А.М. Системы цифровой радиосвязи: учеб. пособие. – М.: Ай Пи Ар Медиа, 2022. – 340 с.

2. A technical overview of LoRa and LoRaWAN [Электронный ресурс]. – Режим доступа: https://lora-alliance.org/wp-content/uploads/2020/11/what-is-lorawan.pdf

УДК 621.376.9

АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ МНОГОПОРОГОВОЙ ДЕМОДУЛЯЦИИ

А.В. Романов, магистрант каф. РТС

Научный руководитель Ю.П. Акулиничев, д.т.н., проф. каф. РТС

г. Томск, ТУСУР, garfil09@list.ru

Описана эффективность использования многопороговой демодуляции. Представлены результаты влияния числа порогов на возможность увеличения количества передаваемой информации и улучшения помехозащищенности.

Ключевые слова: многопороговая демодуляция, порог, кодирование.

На текущий день существует потребность в увеличении количества передаваемой информации без увеличения ширины спектра и мощности, поскольку в некоторых случаях это является существенным удорожанием стоимости конечного проекта.

Однако, в свою очередь, требуется обеспечить возможность восстановления информации, которая может исказиться в процессе передачи информации. Для этого информацию кодируют избыточными кодами, что обычно уменьшает количество энергии, приходящейся на символ.

Ввиду этого противоречия появляется потребность в более детальном исследовании декодеров с мягким входом (SoftInput), использующих метод максимального правдоподобия, например, алгоритм Чейза [1].

Различают два основных подхода: использование окна стирания и многопороговой схемы демодуляции. В данной работе будет исследован последний тип демодуляции.

В ряде источников сообщается, что наиболее эффективно использовать схему с семью порогами, поскольку при дальнейшем увеличении числа порогов прирост информации невелик, но многократно возрастает вычислительная сложность демодуляции [2, 3].

В результате работы такого демодулятора с оптимальным числом порогов на вход кодера будет отправляться 3-битовое слово или не-

двоичное значение, описывающее интервал и достоверность данного символа.

Условные плотности вероятностей для двух равновероятных гипотез (0 или 1) и пример расположения порогов представлены на рис. 1.

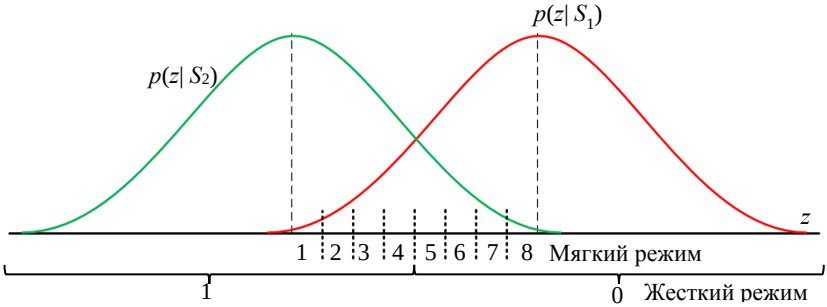


Рис. 1. Распределение вероятностей

В тех же источниках приводится информация, что при использовании мягкого режима демодуляции и при декодировании сверточных кодов алгоритмом Витерби имеется выигрыш в 2 дБ [2, 3], а при применении кодов Рида–Соломона и алгоритма Чейза выигрыш составляет 3 дБ [4].

Однако, если определить границы Варшамова–Гилберта и Хэмминга для кодового расстояния недвоичных кодов, то выяснится, что требуется меньшее количество избыточных символов при той же длине сообщения [5].

Поскольку при увеличении числа порогов уменьшается предельный уровень шума для верного декодирования информации, то возникает потребность оценки необходимого числа порогов и дополнительного выигрыша информации.

Так, проведя ряд исследований по определению количества информации по Шеннону, была получена таблица.

Количество информации по Шеннону

Кол-во порогов	SNR, дБ						
	–10,00	–5,00	0,00	2,40	4,00	6,00	10,00
7	0,02	0,07	0,19	0,23	0,21	0,14	0,01
6	0,02	0,07	0,19	0,23	0,21	0,14	0,01
5	0,02	0,07	0,19	0,23	0,21	0,14	0,01
4	0,02	0,07	0,19	0,23	0,21	0,14	0,01
3	0,02	0,07	0,19	0,22	0,20	0,13	0,01
2	0,02	0,07	0,18	0,21	0,18	0,11	0,01
1	0,02	0,05	0,14	0,14	0,10	0,05	0,00

Как видно из таблицы, при SNR 2,4 дБ количество дополнительной информации, которую можно извлечь из символа при использовании режима мягкой демодуляции, достигает своего максимума. В то же время выясняется особенность, что использование больше четырех порогов становится не актуальным, поскольку прирост дополнительной информации становится незначительным.

Выводы. Можно прийти к выводу, что использование многопороговых схем демодуляции и мягких декодеров способно увеличить количество полезной информации с одновременным улучшением помехозащищенности сигнала от шумов, что может быть весьма актуальным для применения в БШПД и РРЛ, использующих преимущественно лицензионные и арендуемые каналы связи, что уже является экономически обоснованным.

Далее совершенно очевидно, что равномерное расположение порогов не является наилучшим, особенно при малом и большом отношениях сигнал/шум. Но этот вопрос в имеющихся публикациях практически не освещен.

ЛИТЕРАТУРА

1. Chase D. A Class of Algorithms for Decoding Block Codes with Channel Measurement // Information, IEEE Trans. Inform. Theory. – 1972. – Vol. 18. – PP. 170–181.

2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение поиск / пер. с англ.; под ред. А. В. Назаренко. – М.: ИД «Вильямс», 2003. – 1114 с

3. Heller J.A., Jacobs I.W. Viterbi Decoding for Satellite and Space Communication // IEEE Trans. Commun. Techol. – October, 1971. – Vol. COM19, No. 5. – PP. 835–848.

4. A soft decoding algorithm and hardware implementation for the visual prosthesis based on high order soft demodulation / Nannan Quan, Jingjing Bu, Xueping Li, Ningmei Yu // BioMedical Engineering OnLine. – 2016. – Article number: 110.

5. Кларк Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, Дж. Кейн / пер. с англ. – М.: Радио и связь, 1987. – 392 с.

УДК 621.391

РАСПРЕДЕЛЕНИЕ РЕСУРСА СИСТЕМЫ МОБИЛЬНОЙ СВЯЗИ СОГЛАСНО СТРАТЕГИИ PROPORTIONAL FAIR

А.А. Бровкин, аспирант каф. ТОР;
Я.В. Крюков, Д.А. Покаместов, доценты каф. ТОР
г. Томск, ТУСУР, soldierbrovkin@gmail.com

Рассмотрена процедура распределения ресурсов систем связи согласно стратегии proportional fair (PF). Данная стратегия является

компромиссным вариантом планирования и позволяет поддерживать баланс между двумя конкурирующими интересами: максимизации пропускной способности и справедливого планирования. В рамках работы проведено моделирование влияния временного интервала оценки среднего объёма передаваемых данных *a* стратегии PF на справедливость распределения и пропускную способность системы связи.
Ключевые слова: распределение ресурса, справедливое планирование, proportional fair.

Одной из центральных и сложнейших проблем в сетях мобильной связи является проблема распределения системных ресурсов базовой станции (БС) между абонентскими каналами. В настоящее время распределение радиоресурсов в многоканальных системах связи осуществляется согласно различным стратегиям планирования. Каждая стратегия планирования представляет собой набор правил по приоритезации предоставления доступа абонентам системы и распределения общего ресурса связи между ними.

Для того чтобы эффективно осуществлять распределение ресурсов, БС собирает информацию о состоянии канала (CSI – Channel State Information) каждого абонента. Индекс CSI определяет пропускную способность канала передачи абонента. В общем случае разработчики каждой системы связи стремятся максимизировать эффективность использования ресурсов системы.

Для систем мобильной связи стратегия, направленная на максимизацию спектральной эффективности, приводит к снижению объема предоставляемых системных ресурсов абонентам с низким индексом CSI, вплоть до полного отказа в обслуживании. В то же время каждый абонент системы хотел бы, чтобы распределение системных ресурсов было одинаково справедливо для всех абонентов системы независимо от характеристики их каналов передачи. Для того чтобы удовлетворить каждую из сторон, был предложен компромиссный вариант, названный стратегией proportional fair (PF) [1, 2].

Стратегия PF основана на поддержании баланса между двумя конкурирующими интересами: попыткой максимизировать общую пропускную способность сети и справедливого планирования. Порядок обслуживания абонентов согласно стратегии PF определяется на основании весового коэффициента стратегии – отношения пропускной способности абонента R к среднему объёму данных, переданных абонентом T за некоторый предшествующий временной интервал a. В каждый момент времени t планировщик определяет одного абонента, обладающего наибольшим весовым коэффициентом, которого будет обслуживать система связи:

$$\omega(t) = \arg\max_{k} \left(R_k(t) / T_k(t-1) \right), \quad (1)$$

где k – номер абонента.

Для того чтобы определить приоритет доступа, алгоритм PF отслеживает средний объём переданных данных каждого абонента системы на некотором временном интервале a. Изменение приоритета абонента осуществляется на основании предоставленного объёма ресурса согласно

$$T_k(t) = \begin{cases} (1-1/a) \cdot T_k(t-1) + 1/a \cdot (R_k(t)), & \text{если } k = \omega(t), \\ (1-1/a) \cdot T_k(t-1), & \text{если } k \neq \omega(t). \end{cases} \quad (2)$$

Когда БС осуществило обслуживание одного из абонентов, его приоритет уменьшается, при этом приоритет других абонентов возрастает. Величина изменения приоритета зависит от пропускной способности каждого абонента и интервала оценки a.

В рамках работы проведено моделирование влияния временного интервала a на справедливость распределения и пропускную способность системы связи. Моделирование проводилось на базе системы с одной несущей с изменяющимся во времени каналом. Распределение ресурса осуществлялось во временном домене, длительность сигнала во времени ограничена 1000 фреймами. Распределению подвергаются n = 50 абонентов, пропускная способность каждого абонента определялась по теореме Шеннона–Хартли. Расчёт среднего значения характеристик распределения ресурса, рассматриваемых в данной работе, осуществляется методом Монте–Карло с количеством итераций, равным 100. На рис. 1, *а* представлена справедливость планирования, определяемого на основании Jain's fairness index [3]:

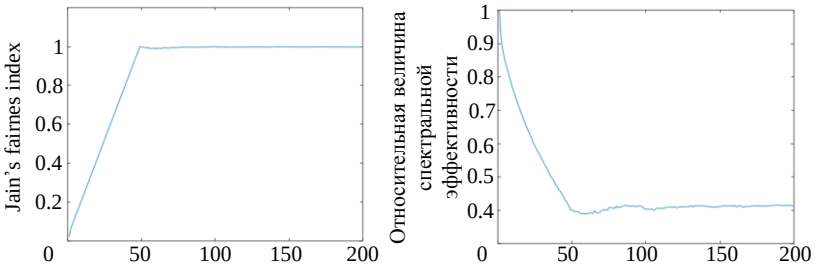
$$j = \left(\sum_{k=1}^{n} x_k \right)^2 \Big/ \left(n \cdot \sum_{k=1}^{n} x_k^2 \right), \quad (3)$$

где j – Jain's fairness index системы связи; x_k – количество временных слотов, предоставленных БС k-му абоненту.

На рис. 1, *б* представлено изменение спектральной эффективности, выраженное в относительных единицах.

Результаты моделирования демонстрируют, что чем больше временной интервал a, тем сильнее PF стремится обеспечить справедливое планирование, и наоборот, чем он меньше, тем сильнее PF стремится к увеличению общей системной скорости.

Исследование выполнено за счет гранта Российского научного фонда № 22-79-10148, https://rscf.ru/project/22-79-10148/.



а)*а* *б* б)

Рис. 1. Результаты моделирования: *а* – зависимость Jain's fairness index от *а*; *б* – относительное изменение спектральной эффективности от *а*

ЛИТЕРАТУРА

1. Thi Thuy Nga Nguyen. Proportional-Fair Scheduling of Mobile Users based on a Partial View of Future Channel Conditions. Automatic Control Engineering. INSA de Toulouse, 2020. English. ffNNT: 2020ISAT0023ff. fftel-03351962v2f [Электронный ресурс]. – Режим доступа: https://theses.hal.science/tel-03351962/document, свободный (дата обращения: 28.02.2023).

2. Tolga G. Proportional Fair Scheduling Algorithm in OFDMA-Based Wireless Systems with QoS Constraints / G. Tolga, Z. Chenxi, A. Jonathan, E. Anthony // Journal of Communications and Networks – JCN. – Vol. 12. – PP. 30–42 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/252063676, свободный (дата обращения: 1.03.2023). DOI: 10.1109/JCN.2010.5710556.

3. Katila C. Neighbors-Aware Proportional Fair scheduling for future wireless networks with mixed MAC protocols / C. Katila, C. Buratti, M. Abrignani et al. // J. Wireless Com Network. – 2017. – Vol. 93 [Электронный ресурс]. – Режим доступа: https://doi.org/10.1186/s13638-017-0875-6, свободный (дата обращения: 3.03.2023).

ПОДСЕКЦИЯ 4.3

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

*Председатель – **Кузьмина Е.А.**, директор Международной цифровой академии, к.т.н.;*
*зам. председателя – **Колтайс А.С.**, ст. преп. каф. ЭБ*

УДК 331.108

СОБЛЮДЕНИЕ СОТРУДНИКОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.В. Иванова, Е.Д. Часовских, В.А. Браун, Я.А. Пчелкин, студенты
Научный руководитель С.В. Глухарева, ст. преп. каф. ЭБ
г. Томск, ТУСУР, gsv@fb.tusur.ru

Рассмотрены причины несоблюдения требований информационной безопасности сотрудниками на рабочем месте, а также возможные меры, которые можно принять для улучшения ситуации.
Ключевые слова: информационная безопасность, риск, система кадровой безопасности предприятия, уровень благонадежности, фишинг, конфиденциальная информация.

Информационная безопасность [1] является критически важным аспектом работы любой компании. Одной из главных причин несоблюдения требований информационной безопасности является недостаточная осведомленность сотрудников о правилах работы с конфиденциальной информацией и рисках, связанных с ее неправильным использованием. Кроме того, некоторые сотрудники могут игнорировать правила безопасности, случайно или намеренно раскрывать конфиденциальную информацию.

Для улучшения ситуации необходимо проводить регулярные обучающие программы для персонала, в которых будут рассматриваться основные правила работы с конфиденциальной информацией [2]. Также стоит уделить внимание мониторингу и контролю за действиями сотрудников [3]. Внедрение системы авторизации и аутентификации может уменьшить вероятность несанкционированного доступа к конфиденциальной информации.

Система кадровой безопасности предприятия (СКБП) поможет не только определить компетентность сотрудника, но и повысить уровень знаний в области информационной безопасности.

Тест по информационной безопасности позволит руководству предприятия получить данные об уровне осведомленности сотрудника о комплексах мер по информационной безопасности [4]. База вопросов требует постоянного обновления. В период проверки знаний сотруднику выдаются 5 случайных вопросов. Успешное прохождение тестирования может повысить уровень благонадежности сотрудника.

Помимо тестовой проверки, СКБП реализует несколько методов для проверки сотрудников на соблюдение требований информационной безопасности:

1. Проверка на подключение внешних USB-устройств [5] направлена предотвращение утечек внутренних документов. Реализуется через скрипт, который сообщает о подключении к компьютеру несанкционированного устройства и блокирует его работу, при этом сохраняя данные о подключении.

2. Блокировка прямого доступа к внутренней системе через открытые сети [6]. Сотрудники, при попытке использования такой сети, получают уведомление о невозможности выполнения действия.

3. Проверка бездействия пользователя посредством введения контрольного кода, который поможет определить сотрудника, оставившего рабочее место доступным для всех, и избежать утечек с помощью автоматического выхода из системы по истечении установленного времени.

4. Проверка на переходы по посторонним ссылкам [7] (фишинг сайты) направлена на предотвращение утечек данных. Реализация осуществляется самой организацией с целью выявить неблагонадежных сотрудников посредством отслеживания переходов с устройств работников.

5. Проверка на внешние звонки [8] направлена на предотвращение возможного раскрытия конфиденциальной информации третьим лицам. Реализуется посредством выдачи корпоративных сим-карт и билинга телефона.

Таким образом, дополнительные функции в нашей системе делают работу более эффективной и позволят наиболее точно определить уровень благонадежности сотрудника. Соблюдение сотрудниками требований информационной безопасности является важной частью кадровой безопасности. Проведение обучающих программ, установление четких правил и процедур, контроль действий персонала важны в процессе работы всей компании для обеспечения безопасности.

ЛИТЕРАТУРА

1. Информационная безопасность в организации [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-organizatsii/viewer , свободный (дата обращения: 24.02.2023).
2. Инструменты для анализа данных [Электронный ресурс]. – Режим доступа: https://kurl.ru/AePEx, свободный (дата обращения: 24.02.2023).
3. Контроль персонала: задачи, принципы, методы [Электронный ресурс]. – Режим доступа: https://dasreda.ru/media/for-managers/kontrol-personala/, свободный (дата обращения: 27.02.2023).
4. Указ Президента РФ от 5 декабря 2016 г. № 646. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/, свободный (дата обращения: 27.02.2023).
5. Служба обнаружения новых устройств [Электронный ресурс]. – Режим доступа: https://ritorika.com.ua/informacija/14/sluzhba-obnaruzhenija-novyh-ustrojstv-usb-kak, свободный (дата обращения: 02.03.2023).
6. Разграничение доступа в локальной сети с использованием базовых настроек сетевого оборудования [Электронный ресурс]. – Режим доступа: https://kurl.ru/EtdIv, свободный (дата обращения: 3.03.2023).
7. Анализ внешних и внутренних ссылок [Электронный ресурс]. – Режим доступа: https://pr-cy.ru/link_extractor/, свободный (дата обращения: 3.03.2023).
8. Проверка переадресации вызовов на другие номера [Электронный ресурс]. – Режим доступа: https://kurl.ru/plQRR, свободный (дата обращения: 3.03.2023).

УДК 338

АНАЛИЗ СОВРЕМЕННЫХ ПРОГРАММНЫХ ПРОДУКТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ФИЗИЧЕСКОГО ЛИЦА И СУБЪЕКТА РФ

П.А. Воронцова, К.С. Орлова, Д.С. Филиппова, Д.Д. Зайцев, студенты

Научные руководители: П.А. Шелупанова, зав. каф. ЭБ, к.э.н.; Ю.Е. Лабунец, ст. преп. каф. ЭБ, к.э.н.

Проект ЭБ-2303. Применение современных программных продуктов для анализа составляющих экономической безопасности (на разных уровнях)

г. Томск, ТУСУР, saintundead1111@mail.ru

Выполнен обзор функционала действующего программного обеспечения экономической безопасности на различных уровнях. Проведен анализ возможности обеспечения решения исследуемыми

программными продуктами проблем оценки экономической безопасности.
Ключевые слова: проблемы оценки, экономическая безопасность, программное обеспечение, решение, риск, угроза, уровень безопасности.

Программные продукты являются одним из основных элементов современного механизма оценки экономической безопасности. Развитие и совершенствование функционала программного обеспечения направлены, главным образом, на решение основных проблем оценки экономической безопасности на различных уровнях (на уровне физического лица и субъекта РФ).

В настоящей работе нами проведен контент-анализ актуальных проблем оценки экономической безопасности. Сформирована классификация по значимым классификационным признакам:

1) по объекту экономической безопасности;

2) по содержанию;

3) по структурному признаку.

Для нашего исследования современных программных продуктов изучение проблем оценки экономической безопасности проводилось с учетом применения вышепредставленной классификации. В частности, мы рассмотрели теоретические и практические проблемы оценки финансовой компоненты экономической безопасности на примере физического лица и субъекта РФ с целью дальнейшей оценки возможностей программного оборудования решать данные проблемы.

Теоретический обзор научных исследований по оценке экономической безопасности позволил нам определить следующие актуальные проблемы:

А) На уровне проблем экономической безопасности физического лица:

– усиление расслоения общества;

– стихийность рыночной конъюнктуры;

– теневой сектор, криминализация общества.

Б) На уровне проблем экономической безопасности субъекта РФ:

– дисбаланс производства и потребления;

– катастрофическое старение производственного аппарата и инфраструктуры систем;

– структурные и институциональные диспропорции.

По результатам изучения рынка программного обеспечения экономической безопасности мы определили следующие программные продукты:

– на уровне физического лица: Statistica [1];

– на уровне субъекта РФ: Deducer [2], Jamovi [3];

– на уровне физического лица и субъекта РФ: PSPP [4].

Следует отметить, что в целом функционал выбранного нами для исследования программного оборудования достаточно универсален в области проведения различных процедур анализа и обработки данных.

Мы также провели анализ возможностей данного программного обеспечения для решения актуальных проблем оценки экономической безопасности на уровне физического лица и субъекта РФ.

Оценка осуществлялась эмпирическим методом с учетом полных данных о функционалах программных продуктов. Оценка выполнялась с применением шкалы баллов, где 1 балл присваивался программному обеспечению, если его применение способствовало решению определенной актуальной проблемы оценки экономической безопасности; 0,5 балла устанавливалось, если программное обеспечение способно частично решить ту или иную проблему оценки экономической безопасности; 0 баллов – в случае, если программное обеспечение не решает актуальную проблему оценки экономической безопасности. Результаты проведенной нами оценки представлены в таблице.

Анализ возможности обеспечения ПО решения проблем оценки экономической безопасности физического лица и субъекта РФ (в баллах)

№ п/п	Наименование проблемы	Наименование программного обеспечения и его оценка (в баллах)			
		PSPP	Statistica	Deducer	Jamovi
1	Усиление расслоения общества	0,5	0	0	1
2	Стихийность рыночной конъюнктуры	1	0,5	0	0,5
3	Теневой сектор, криминализация общества	0,5	0,5	0	0
4	Дисбаланс производства и потребления	0,5	0	0,5	0,5
5	Катастрофическое старение производственного аппарата и инфраструктуры систем	0,5	0	0,5	0
6	Структурные и институциональные диспропорции	0,5	0,5	0,5	0,5
Итого		3,5	1,5	1,5	2,5

Таким образом, проведен анализ возможности программного обеспечения решения исследуемыми программными продуктами проблем оценки экономической безопасности на уровне физического ли-

ца и субъекта РФ, наиболее приемлемыми и универсальными продуктами являются PSPP и Jamovi.

ЛИТЕРАТУРА

1. Программный продукт Statistica [Электронный ресурс]. – Официальный сайт «StatSoft Russia». – URL: http://statsoft.ru/products/STATISTICA_Base/ (дата обращения: 03.03.2023).

2. Дедуктор: графический интерфейс для R [Электронный ресурс]. – Официальный сайт «Deducer». – URL: https://deducer.org/ (дата обращения: 03.03.2023).

3. Открытое статистическое программное обеспечение для настольных компьютеров и облачных вычислений [Электронный ресурс]. – Официальный сайт «Jamovi». – URL:https://www.jamovi.org (дата обращения: 03.03.2023).

4. GNU PSPP / [Электронный ресурс]. – Официальный сайт «GNU». – URL: www.gnu.org/software/pspp (дата обращения: 03.03.2023).

УДК 338

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: АНАЛИЗ ФУНКЦИОНАЛА И ВОЗМОЖНОСТЬ ЕГО ПРАКТИЧЕСКОГО ВНЕДРЕНИЯ В УЧЕБНЫЙ ПРОЦЕСС

П.А. Карпушкина, В.Е. Коленкова, М.А. Семенова, Д.Д. Зайцев, студенты

Научные руководители: П.А. Шелупанова, зав. каф. ЭБ, к.э.н.; Ю.Е. Лабунец, ст. преп. каф. ЭБ, к.э.н.

Проект ЭБ-2303. Применение современных программных продуктов для анализа составляющих экономической безопасности (на разных уровнях)»

г. Томск, ТУСУР, saintundead1111@mail.ru

Выполнен анализ сильных и слабых сторон отдельных программных продуктов для обеспечения экономической безопасности предприятия. Методом анкетирования проведена оценка возможности внедрения данных программных продуктов в учебный процесс кафедры экономической безопасности факультета безопасности ФГБОУ ВО ТУСУРа.

Ключевые слова: экономическая безопасность, программное обеспечение, предприятие, учебные процесс, внедрение.

В эпоху цифровизации применение различных программных продуктов является необходимым элементом учебного процесса и методического обеспечения обучения студентов вузов.

Экономическая безопасность предприятия является основой стабильного развития государства. Следовательно, постоянный мониторинг и внедрение программного обеспечения экономической безопасности предприятия актуальны для развития учебного процесса кафедры экономической безопасности в рамках действующих положений ФГОС «Экономическая безопасность» [1].

Нами был проведен обзор современных программных продуктов для обеспечения экономической безопасности предприятия по двум направлениям: перспективность для образовательных программ и целесообразность для внедрения в учебный процесс [2].

Определены следующие критерии отбора перспективных программных продуктов: 1) соответствие требованиям профессиональных стандартов, составляющих основу ФГОС «Экономическая безопасность»; 2) многофункциональность программного продукта, а также возможность модификации формул и алгоритмов; 3) универсальность программного продукта – возможность применения для предприятия любого масштаба и вида деятельности; 4) адаптивность программного продукта для любого пользователя; 5) бесплатный доступ; 6) удобный интерфейс; 7) простота настройки.

Согласно данным критериям, были определены наиболее перспективные для учебного процесса программные продукты: Discoverit [3], БОСС Кадровик [4], ABACUS Professional [5].

Нами изучены функциональные характеристики данных программных продуктов. Результаты представлены в табл. 1.

Таблица 1

Функциональные характеристики выбранных программных продуктов по обеспечению экономической безопасности

№ п/п	Наименование программного обеспечения	Описание функционала
	Discoverit	Комплексное решение для повышения эффективности сотрудников и процессов предприятия
2	БОСС Кадровик	Автоматизация бизнес-задач, связанных с управлением персоналом
3	ABACUS Professional	Бухгалтерский и налоговый учет с учетом отраслевой специфики и масштаба бизнеса

По целесообразности внедрения нами было проведено сравнение программного обеспечения БОСС Кадровик, ABACUS Professional, Discoverit с их аналогами. Определены сильные и слабые стороны данных программных продуктов (табл. 2).

Таблица 2

Оценка сильных и слабых сторон программных продуктов

Наименование программного обеспечения	Слабые стороны	Сильные стороны
БОСС Кадровик	Сложность в настройке и понимании интерфейса	Наличие встроенных модулей системы управления персоналом; готовая интеграция с SAP и другими ERP-системами
ABACUS Professional	Расчет только на большой штат бухгалтерии	Для корпоративной сети, возможность создать политику расходов в масштабе всей компании
Discoverit	Много бесплатных аналогов	Выявление точек неэффективности замедления процессов; повышение точности анализа и оперативности принятия процессных управленческих решений

Кроме того, было проведено анкетирование целесообразности внедрения программных продуктов БОСС Кадровик, ABACUS Professional, Discoverit в учебный процесс кафедры экономической безопасности факультета безопасности ФГБОУ ВО ТУСУРа. В анкетировании приняли участие 15 преподавателей кафедры экономической безопасности, при этом 9 отметили возможность применения Кадровик, ABACUS Professional, Discoverit.

Таким образом, по результатам исследования внедрение в учебный процесс данных программных продуктов представляется нам перспективным и целесообразным, требует организации и проведения лабораторных работ, а также дальнейшего формирования (обновления) методических пособий.

ЛИТЕРАТУРА

1. Приказ Министерства науки и высшего образования РФ от 14 апреля 2021 г. № 293 «Об утверждении федерального государственного образовательного стандарта высшего образования – специалитет по специальности 38.05.01 Экономическая безопасность».

2. Программные средства, используемые в деятельности экономических и бухгалтерских служб организации: анализ преимуществ и возможностей использования [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/programmnye-sredstva-ispolzuemye-v-deyatelnosti-ekonomicheskih-i-buhgalterskih-sluzhb-organizatsii-analiz-preimuschestv-i/viewer (дата обращения: 09.03.2023).

3. Discoverit. Документация, содержащая информацию, необходимую для эксплуатации экземпляра ПО [Электронный ресурс]. – Режим доступа: https://docs.b1-it.ru/docs/discoverit/use.pdf (дата обращения: 09.03.2023).

4. БОСС Кадровик: основные преимущества HRM-системы [Электронный ресурс]. – Режим доступа: https://bsc-consulting.ru/advantages/boss-kadrovik/ (дата обращения: 09.03.2023).

5. ABACUS Professional – программный комплекс автоматизации бухгалтерского и налогового учета [Электронный ресурс]. – Режим доступа: https://www.omega.ru/ap.html (дата обращения: 09.03.2023).

УДК 331.103

ПРОБЛЕМЫ КАДРОВОЙ БЕЗОПАСНОСТИ ФЕДЕРАЛЬНОЙ НАЛОГОВОЙ СЛУЖБЫ РОССИИ

А.С. Макарова, студентка

Научный руководитель С.В. Глухарева, ст. преп. каф. ЭБ

г. Томск, ТУСУР, anastaysha.makarova@gmail.com

Рассматриваются проблемы, возникающие в ФНС России, связанные с кадровой безопасностью, а также пути их решения.

Ключевые слова: кадровая безопасность, сотрудник, Федеральная налоговая служба.

Кадровая безопасность является важной составляющей обеспечения экономической безопасности в любой организации. Существует большое количество определений кадровой безопасности, при этом под данным понятием будем подразумевать систему предприятия, связанную с эффективной работой персонала и функционированием организации (предприятия) в условиях безопасности и направленную на развитие самой организации в целом и каждого сотрудника в отдельности [1].

При этом следует подчеркнуть особую важность кадровой безопасности в сфере государственной гражданской службы, в частности, в Федеральной налоговой службе Российской Федерации (далее – ФНС РФ). В Законе РФ «О налоговых органах Российской Федерации» сказано, что ФНС РФ является исполнительным органом власти, главной функцией которого является контрольно-надзорная функция с целью установления соблюдения законодательства РФ о налогах и сборах [2]. Таким образом, в данном случае грамотное обеспечение кадровой безопасности необходимо не только для функционирования конкретного предприятия или организации, но и государства в целом, что определяет важность темы исследования.

На работу в данный орган принимаются сотрудники, имеющие высшее экономическое или юридическое образование. Помимо этого, очень важно, чтобы работник знал основы налогового законодатель-

ства и судопроизводства, а также умел ориентироваться в современных информационных технологиях.

В ФНС РФ предусмотрены определенные квалификационные требования к кандидатам в зависимости от конкретной должности, а также ограничения, которые закреплены в ст. 16 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» (далее – 79-ФЗ) [4]. В данной статье закреплено большое количество ограничений, связанных с гражданской службой, среди которых можно выделить наличие неснятой или непогашенной судимости, наличие заболевания, препятствующего поступлению на гражданскую службу, предоставление подложных документов.

Для поступления в налоговую службу кандидату необходимо предоставить характеристику, справку об отсутствии судимости. Помимо перечисленного, кандидат проходит анкетирование, интеллектуальное тестирование, а также психологическое исследование.

Психологическое исследование состоит из нескольких этапов: первый – знакомство (формируется общее представление о личностных качествах); второй – наблюдение (создается поведенческий «портрет»); третий – психологическое обследование (тестирование); четвертый – обработка данных, интерпретация результатов и подготовка итогового заключения; пятый – заключительное собеседование (происходит уточнение ранее полученных сведений); шестой – оформление итогового заключения (описание интеллектуальной, эмоционально-волевой, коммуникативной, поведенческой, характерологической составляющих). Используется также большое количество различных диагностических методов, что позволяет подобрать кандидатов с высоким уровнем благонадежности, тем самым обеспечив необходимый уровень кадровой безопасности.

После увольнения со службы гражданин, в соответствии с ч. 3 ст. 17 79-ФЗ, не вправе разглашать сведения конфиденциального характера, ставшие ему известными в связи с исполнением должностных обязанностей. При этом с таким гражданином в случае увольнения проводится соответствующая беседа, в ходе которой он подписывает соглашение о неразглашении указанной информации в течение трех или пяти лет (конкретный срок зависит от должности).

Можно заметить, что кандидат на должность в ФНС РФ подвергается тщательной проверке, что не может положительно не сказаться на кадровой безопасности. Однако в обеспечении кадровой безопасности ФНС РФ есть и существенные минусы.

Так, уже после принятия на должность не проводится какой-либо мониторинг работы и психологического состояния кадров. Это не предусмотрено ни федеральными законами, ни приказами ФНС РФ.

Существует только оперативное воздействие на кадры в случае возникновения каких-либо экстраординарных ситуаций.

Данный факт негативно сказывается на состоянии кадровой безопасности, поскольку не происходит никакого контроля кадров во время работы. В связи с этим повышается риск возникновения конфликтных ситуаций как со стороны налоговой службы к сотруднику, так и наоборот. Помимо этого, при работе сотрудника часто возникают проблемы в работе с налогоплательщиками, постоянное переобучение в связи с обновлениями программ и обязательное повышение квалификации раз в три года, а также множественные ограничения работника, связанные с гражданской службой. У государственных служащих уровень дохода значительно ниже по сравнению с частными компаниями.

Таким образом, в ФНС РФ в течение многих лет отмечается старение кадров, отсутствие обновления и прибытия «новой крови». Очевидно, что психологическому состоянию человека свойственно меняться под воздействием различных факторов: как естественных, так и стрессовых. Без периодического проведения психологического мониторинга кадров невозможно оперативно выявить указанные изменения конкретных лиц, что может привести к возникновению различных экстраординарных ситуаций: конфликтов в коллективе, появлению на рабочем месте определенных лиц в состоянии алкогольного или наркотического опьянения, противоправному поведению психически нестабильных лиц, а также проблем, связанных с коррупцией, потерей или утечкой данных, злоупотреблением должностью работника и т.п.

В связи с этим представляется, что необходимо расширить функционал сотрудников кадрового подразделения, которым необходимо проводить оценку и анализ для оперативного выявления проблем и рисков, связанных с сотрудниками, а также планировать меры по обеспечению кадровой безопасности и приводить прогноз по реализации данной меры, а также координировать дальнейшую работу.

ЛИТЕРАТУРА

1. Глухарева С.В. Методика подбора персонала на должности, связанные с обработкой конфиденциальной информации // Безопасность информационного пространства 2017: матер. XVI Всерос. науч.-практ. конф. студентов, аспирантов, молодых ученых, Екатеринбург, 12 декабря 2017 г. – Екатеринбург: Изд-во Урал. ун-та, 2018. – С. 154–158.

2. Закон РФ от 21.03.1991 № 943-1 (ред. от 28.12.2022) «О налоговых органах Российской Федерации» // СПС «КонсультантПлюс».

3. О государственной гражданской службе: Федеральный закон от 27.07.2004 № 79-ФЗ // СПС «КонсультантПлюс».

УДК 331.108

НЕОБХОДИМОСТЬ ВНЕДРЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ В ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

А.И. Середенко, студент каф. ЭБ
Научный руководитель С.В. Глухарева, ст. преп. каф. ЭБ
г. Томск, ТУСУР

Анализируется проблема необходимости внедрения кадровой безопасности в общеобразовательные учреждения. Несоблюдение или частичное соблюдение требований законодательства участниками образовательного процесса, а также непрофессионализм сотрудников школы приводят к негативным последствиям. Данная проблема особо актуальна в наши дни, так как участились несчастные случаи в образовательных учреждениях.
Ключевые слова: кадровая безопасность, «человеческий фактор», безопасность образовательной организации, угрозы безопасности.

Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ установлено, что в России образовательные организации обязаны обеспечивать безопасность образовательной среды [1]. Согласно данному закону для обеспечения комфортной и безопасной среды обучающихся и сотрудников общеобразовательного учреждения должны соблюдаться установленные законом требования по обеспечению безопасности. Согласно Федеральному закону «О безопасности» от 28.12.2010 № 390-ФЗ**,** основными принципами обеспечения безопасности являются соблюдение и защита прав и свобод человека и гражданина, законность и др. [2].

Для выявления уровня безопасности в школе и актуальных проблем был проведен опрос среди педагогов одной из школ г. Томска, который показал, что из 20 опрошенных педагогов 8 человек не всегда чувствуют себя безопасно в школе. Основные причины, согласно опросу: семейные факторы (дети из неблагополучных семей, под опекой и т.д.) – 55% опрошенных (11 человек); неподобающее поведение со стороны учеников – 50% опрошенных (10 человек); отсутствие поддержки со стороны родителей – 35% опрошенных (7 человек).

Как показывает практика, не все учителя могут найти подход к «трудным» ученикам. Не всегда родители идут навстречу учителям и оказывают поддержку со своей стороны. Впоследствии возникают конфликтные ситуации по следующим причинам: отсутствие заинтересованности со стороны родителей (опекунов) жизнью ребенка, в том числе в школе, а также неэтичное поведение педагога.

Неэтичное поведение педагога подразумевает недопустимое поведение по отношению к ученику: крик, агрессия, унижение и т.п. Причинами такого поведения могут служить: отсутствие стрессоустойчивости, терпения, толерантности, халатность – все то, что можно отнести к пресловутому «человеческому фактору».

Под кадровой безопасностью будем понимать «систему предприятия, связанную с эффективной работой персонала и функционированием организации (предприятия) в условиях безопасности и направленную на развитие самой организации в целом и каждого сотрудника в отдельности» [3]. Одним из важных элементов кадровой безопасности является подбор кадров с высоким уровнем благонадежности. Исходя из обязанностей и функций сотрудников образовательного учреждения, регламентированных трудовым договором и должностной инструкцией, вытекают их квалификационные обязанности, которые должны выполняться.

Кроме профессиональной подготовки, не менее важными являются личные качества сотрудников. В опросе было предложено выбрать 6 самых важных качеств, которыми должен обладать педагог. Согласно опросу, одними из важнейших качеств педагоги считают: профессионализм (18 человек – 90% опрошенных), ответственность (14 человек – 70% опрошенных), терпение (14 человек – 70% опрошенных), уважение к детям (13 человек – 65% опрошенных), дисциплинированность (12 человек – 60% опрошенных), умение донести материал (12 человек – 60% опрошенных).

Вопросами подбора и трудоустройства кадров в общеобразовательных учреждениях занимается администрация школы. При приеме на работу администрации школы необходимо всесторонне осуществлять проверку кандидатов с целью выявления их неблагонадежности и в целом для того, чтобы снизить уровень риска. Неблагонадежность сотрудника в общеобразовательном учреждении обусловлена отрицательными личными качествами (безответственность, конфликтность, агрессия, недисциплинированность, негативное отношение к детям и т.п.); плохой репутацией педагога (негативные характеристики с места учебы, прошлого места работы и т.п.); наличием в прошлом судимости и т.д.

Специфика работы учителя заключается в том, чтобы найти общий язык с детьми, быстро сориентироваться в сложившейся ситуации, найти правильное решение. В последние годы в российском образовании меняются стандарты, программы, формы и методы образования, разрабатываются новые технологии. В связи с этим каждый педагог должен быть обучаем, уметь адаптироваться в новых про-

граммах обучения и применять новые методы. В опросе было предложено выбрать несколько форм и методов, которые педагоги используют в своей работе с учениками: организация групповой, парной и индивидуальной работы (18 человек – 90% опрошенных); организация самостоятельной деятельности учащихся (18 человек – 90% опрошенных); индивидуальные беседы (14 человек – 70% опрошенных); игровые формы (12 человек – 60% опрошенных); классные часы (10 человек – 50% опрошенных); экскурсии, поездки (8 человек – 40% опрошенных); научно-исследовательская деятельность детей (8 человек – 40% опрошенных) и т.д.

На данный момент времени актуальной является и проблема дефицита кадров. Департаментом образования Томской области был проведен мониторинг форм поддержки и сопровождения молодых учителей, в том числе мониторинг по кадровой обеспеченности общеобразовательных учреждений. Так, согласно информации из распоряжения Департамента образования Томской области «Об организации работы по поддержке и сопровождению молодых педагогов в общеобразовательных учреждениях г. Томска» по состоянию на 01.11.2021 г., в школах работают 4329 педагогических работников (увеличение с прошлым учебным годом на 78 человек, что составляет 1,8%). На 17.08.2021 г. общее количество педагогических работников, прибывших за летний период в общеобразовательные учреждения, составило 169 человек (в 2020 г. – 183), со статусом «молодой специалист» – 47 человек. На 17.08.2021 г. в образовательных учреждениях было открыто 276 вакансий.

Таким образом, в 2021 г. от общей численности педагогических работников до 35 лет выбывшие из системы образования составляют 7,3% (114 человек), в 2020 г. – 6,1% (89 человек). Причин этому несколько: смена места жительства, переезд в другой регион, смена профессии, отсутствие в учреждении программы по работе с молодыми учителями, недостаточное материальное стимулирование наставников, «слабые» меры поддержки молодых учителей в возрасте до 35 лет, недостаточное методическое сопровождение образовательными организациями молодых учителей с целью устранения профессиональных дефицитов и др.

Опрос, проводившийся в школе, показал, что 85% опрошенных (17 человек) не удовлетворены уровнем своей заработной платы, но на все необходимое ее хватает, 15% опрошенных (3 человека) не устраивает уровень их заработной платы. Приблизительно каждый 7-й сотрудник работает по внутреннему совместительству.

Большая часть сотрудников общеобразовательных учреждений не довольна уровнем заработной платы, многие молодые специалисты после окончания педагогических вузов уезжают в другие регионы, часть уходит из системы образования. Периодически в школах возникают чрезвычайные ситуации различного характера. Так, в последнее время участились случаи ложных сообщений на электронные почты школ о минировании и нахождении подозрительных предметов. Все это свидетельствует о снижении уровня кадровой безопасности общеобразовательных учреждений.

Таким образом, можно сделать вывод о необходимости внедрения кадровой безопасности в общеобразовательные учреждения.

ЛИТЕРАТУРА

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_140174/ (дата обращения: 15.01.2023).

2. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/247e2ca8fe0f9d1d821eae037dd70806804b0d3c/ (дата обращения: 21.01.2023).

3. Глухарева С.В. Методика подбора персонала на должности, связанные с обработкой конфиденциальной информации // Безопасность информационного пространства – 2017: матер. XVI Всерос. науч.-практ. конф. студентов, аспирантов, молодых ученых, Екатеринбург, 12 декабря 2017 г. – Екатеринбург: Изд-во Урал. ун-та, 2017. – С. 155–158 [Электронный ресурс]. – URL: http://elar.urfu.ru/bitstre am/10995/65616/1/978-5-7996-2404-0_2018-50.pdf (дата обращения: 03.03.2023).

УДК 338.23

ЭКОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ КАК ОДНА ИЗ СОСТАВЛЯЮЩИХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Д.И. Тарасова, студентка

Научный руководитель Е.Б. Дворядкина, проф. каф. РиМЭУ, д.э.н.

г. Екатеринбург, УрГЭУ, d.i.office@yandex.ru

Обоснована актуальность вопросов экологической безопасности как одной из компонентов экономической безопасности. В качестве теоретической основы выступает теория зеленой экономики, в рамках которой приоритет отдается экологическому контексту.

Ключевые слова: экономическая безопасность, экологическая безопасность, зеленая экономика.

Современная обстановка с её активностью изменений, доминированием многоукладности в экономике, постоянно меняющимся мировым настроением, растущим количеством санкций ставит необходимым фактором стабилизации ситуации позиции субъектов Российской Федерации. Вопросы стабилизации экономики и увеличения безопасности приобретают первостепенное значение. В связи с этим анализ возникающих рисков безопасности должен, прежде всего, основываться на выявлении причин ограничений развития производства, влияющих на комплексное развитие экономики. С одной стороны, интенсивное развитие производства повышает благосостояние населения, с другой – негативно сказывается на окружающей среде [3]. С развитием производства, в частности промышленности, ежегодно уничтожается более 1 млн га леса, выброс углекислого газа в атмосферу составляет 20 млрд т, рост объемов пластикового мусора составляет – 300 млн т в год. Сейчас как никогда очень актуально развитие «зеленой» экономики, которая способствует росту производства без ущерба окружающей среде.

Таким образом, задача нашего исследования – обосновать актуальность решения задач в области экологической безопасности для устранения риска в этом направлении и, как следствие, развития экономики страны.

Экологическая безопасность напрямую взаимосвязана с развитием зеленой экономики. Научный мир до сих пор не дал единой трактовки понятию «зеленая экономика». ООН, излагая программу по окружающей среде, раскрывает определение зеленой экономики – «такая экономика, которая повышает благосостояние людей и обеспечивает социальную справедливость и при этом существенно снижает риски для окружающей среды и ее обеднение».

А. Завалеева вкладывает в это понятие следующие составляющие: бережное отношение к ресурсам планеты, их воспроизводство; «повышение качества жизни людей, их здоровья и благополучия»; усиление экономической позиции страны [3].

Р. Перник трактует понятие через разработку, производство и эксплуатацию «технологий и оборудования», которые обеспечат не только контроль, но и уменьшат выбросы вредных веществ, позволят проводить мониторинг и прогнозировать изменения [4].

В.С. Бочко понимает зеленую экономику как перевод производства на технологии, в результате применения которых создаются экологически чистые товары [1, с. 115].

Исходя из этого, существуют задачи, решение которых способствует переходу к зеленой экономике. Рассмотрим некоторые из них:

1. Установление четких норм в области экологии и стандартов «зеленой экономики» для ведения бизнеса. Особое значение данные нормы имеют для промышленных предприятий, которые наносят экологический (а значит, и экономический) ущерб окружающей среде. Налоговые льготы, дополнительные финансовые возможности для предприятий, внедряющих экологически чистые технологии, маркировка продукции, выпускаемой на «зеленом» производстве, – это часть инструментов, позволяющих стимулировать диверсификацию экономики для устранения рисков.

2. Диверсификация отечественной промышленности, вектор которой направлен на создание и реализацию экологически безопасных, ресурсосберегающих производств для создания конкурентоспособных товаров, работ, услуг. В разрезе экономической безопасности данный фактор оказывает влияние на состояние основных фондов. Большинство ученых определяют норму износа основных фондов не более 60%. По состоянию на 2021 г. степень износа основных фондов в РФ составила 53% (+0,9% по сравнению с 2020 г.).

3. Актуализация экологических проблем и выявление путей нейтрализации рисков. Показатели состояния экологии могут быть рассмотрены через совокупность данных об уровне загрязнения окружающей среды, истощение природных ресурсов, количество ЧС природного и техногенного характера. Природный потенциал задает вектор развития региона, подразумевает использование природных ресурсов (недра, вода, климатические особенности, земельные и лесные ресурсы) развитием производств. Вместе с широкими возможностями потребления и использования в производстве природный потенциал требует восстановления, воссоздания нарушенных природных связей. Поэтому приоритетом в решении этого фактора становится обеспечение рационального природопользования в условиях экологической безопасности, что благоприятно сказывается на устойчивой экономической безопасности региона.

4. Повышение уровня жизни населения через улучшение экологического состояния региона. Высокий уровень жизни населения привлекает трудоспособное население. Конкурентоспособность трудовых ресурсов и их научно-технический потенциал определяются закономерностями развития народонаселения и эффективностью демографической политики государства и региона. Эффективное использование трудового потенциала субъекта существенным образом влияет на создание экономической устойчивости региона.

Таким образом, мы видим, что все задачи, которые способствуют переходу к зеленой экономике и повышению уровня экологической

безопасности, напрямую влияют на уровень экономической безопасности, а значит, и на устойчивость экономического развития субъектов экономики.

ЛИТЕРАТУРА

1. Бочко В.С. Зеленая экономика: вторая вечная проблема человечества // Вестник УрФУ. Сер.: Экономика и управление (Екатеринбург). – 2014. – № 3. – С. 113–119.

2. Завалеева А. Зеленая экономика // HPBS, 2021 [Электронный ресурс]. – Режим доступа: https://hpb-s.com/news/zelenaya-ekonomika/, свободный (дата обращения: 06.03.2023).

3. Шмидт О. Что такое зеленая экономика // Совкомблок. – 2021 [Электронный ресурс]. – Режим доступа: https://sovcombank.ru/blog/esg/chto-takoe-zelenaya-ekonomika?utm_referrer=https%3A%2F%2Fyandex.ru%2F, свободный (дата обращения: 06.03.2023).

4. Pernick R. It's All in the Count: The Vexing but Critical Challenge of Green Jobs Accounting // Cleean Edge [Электронный ресурс]. – Режим доступа: www.cleanedge. com/views, свободный (дата обращения: 06.03.2023).

УДК 004.912; 004.622

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПОДГОТОВКИ ДОКУМЕНТОВ ДЛЯ ПРОХОЖДЕНИЯ ВСЕХ ВИДОВ ПРАКТИК

Э.Э. Белозерцев, П.Ю. Давыдченко, студенты каф. КИБЭВС;
М.Д. Татаринов, студент каф. БИС
Научный руководитель С.В. Глухарева, ст. преп. каф. ЭБ
г. Томск, ТУСУР, eduard.belozercev@gmail.com

Проект ГПО КИБЭВС-2101. Автоматизированная информационная система для подготовки документов для прохождения всех видов практик

Рассматривается возможность внедрения автоматизированной информационной системы для подготовки документов для прохождения студентами практик в аспекте экономической безопасности.

Ключевые слова: экономическая безопасность, автоматизированная система, система электронного документооборота, практическая подготовка.

В условиях тенденции цифровизации многих сфер деятельности различных организаций нельзя не отметить активную трансформацию инструментов управления [1] процессами, к которым относятся в том числе процессы обработки документов (создание, хранение, передача,

согласование). В связи с этим многие организации внедряют в свою работу системы электронного документооборота (СЭД), например, «1С:Документооборот 8» компании «1С», «ТЕЗИС» компании Haulmont, «Е1 ЕВФРАТ» компании Cognitive Technologies.

Проблема оптимизации документооборота присутствует и в вузах. Одним из трудоемких процессов, требующих заполнения внушительного количества документов, является организация прохождения студентами практик, являющихся видом учебной деятельности [2]. Повысить эффективность работы с документами, сэкономить время на их заполнение, проверку, подтверждение, обеспечить согласованность данных этапов позволяет разрабатываемая автоматизированная информационная система (АИС) для подготовки документов для всех видов практик.

Оптимизация документооборота и создание единого массива электронных файлов для всех документов по прохождению студентами практик может иметь важное значение и с точки зрения экономической безопасности.

Внедрение в систему управления обучением АИС для подготовки документов для прохождения всех видов практик окажет влияние на совокупность факторов экономической безопасности:

1. Сокращение издержек на содержание бумажных носителей информации и ручную обработку документов, что приведет к экономии бюджетных средств; уменьшение времени на обработку документов позволит снизить затраты на проведение практик, снизив объемы финансовых затрат студентов и организаций, привлекающих стажеров.

2. Уменьшение количества ошибок в документах, корректность составления которых крайне важна, поможет избежать финансовых рисков, связанных с возможными санкциями и штрафами, вызванными ошибками в документах. Ошибки, совершаемые пользователями при ручной работе с документами, сказываются и на времязатратности и трудоемкости контроля за их обработкой, согласованием, исполнением. По данным опроса, проведенного среди студентов факультета безопасности (ФБ) осенью 2022 г., большинство из них допускали ошибки в заполняемых вручную документах для прохождения практики (результаты представлены на рис. 1).

3. Создание единого электронного хранилища всех документов по прохождению практик с повышенным уровнем защиты и управление им позволит избежать возможности утечки конфиденциальной информации, что является важным аспектом экономической безопасности. Защиту данных, хранимых в системе, можно реализовать с помощью применения криптографических методов шифрования данных,

авторизации пользователей, а также механизмов защиты от несанкционированного доступа.

Рис. 1. Оценка частоты возникновения ошибок при заполнении документов

4. Создание единой информационной среды для работы студентов и работодателей улучшает процесс взаимодействия и повышает качество информационной поддержки студентов. Информация о приобретаемых в процессе прохождения студентами практик и стажировок навыках и компетенциях в совокупности с данными об их обучении могут формировать цифровой след студента [3]. Это может в дальнейшем повысить их конкурентоспособность на рынке труда.

5. Сбор и анализ статистических данных по взаимодействию вуза с различными компаниями (например, успешность прохождения студентами практик и стажировок в профильных организациях, их выходные навыки и умения) для организации дальнейшего успешного сотрудничества.

Текущая разработка АИС для подготовки документов для прохождения всех видов практик предусматривает возможность дальнейшей интеграции с внешними системами: базами данных (общими хранилищами данных студентов, преподавателей), системами управления документами (являющихся частью системы управления обучением), электронной почтой (возможность оповещений, рассылок, подтверждение действий) и другими приложениями.

Таким образом, возможности разрабатываемой автоматизированной информационной системы, которые предоставит полная реализа-

ция ее функционала, обеспечат экономическую безопасность, обусловленную:

– улучшением эффективности работы сотрудников с документами;

– повышением уровня защиты информации;

– снижением рисков, связанных с возможными финансовыми потерями.

Для пользователей система может стать удобным интерфейсом для организации работы с большим количеством данных, которые посредством нее могут быть структурированы, надежно сохранены, а затрачиваемые на их обработку ресурсы сведены к минимуму.

ЛИТЕРАТУРА

1. Обеспечение экономической безопасности при внедрении систем электронного документооборота в условиях цифровой трансформации бизнеса / Н.В. Викторова, Д.В. Каримова, А.В. Камнева, В.С. Перминов // Вопросы инновационной экономики. – 2020. – Т. 10, № 1. – С. 57–70 [Электронный ресурс]. – URL: https://doi.org/10.18334/vinec.10.1.41532

2. Положение о практической подготовке в форме практики обучающихся, осваивающих образовательные программы высшего образования в ТУСУРе: введено приказом ректора от 19.10.2020 № 830 [Электронный ресурс]. – Режим доступа: regulations.tusur.ru/documents/1073, свободный (дата обращения: 22.11.2021).

3. Чуркина Н.А. «Цифровой след» в аспекте электронного обучения. Методология и технология профессионального образования // Междунар. науч.-исслед. журнал. – 2022. – № 11 (125) [Электронный ресурс]. – URL: https://doi.org/10.23670/IRJ.2022.125.35 (дата обращения: 27.02.2023).

УДК 336.717.061

СКОРИНГОВАЯ ОЦЕНКА КРЕДИТОСПОСОБНОСТИ ФИЗИЧЕСКОГО ЛИЦА В БАНКОВСКОЙ СФЕРЕ

М.Е. Исаева, студентка каф. БИС

Научный руководитель С.В. Глухарева, ст. преп. каф. экономической безопасности

г. Томск, ТУСУР, d13.h@mail.ru

Описана разработка собственной методики скоринга заемщиков физических лиц. Актуальность связана с тем, что банки ежедневно принимают решения о рассмотрении кредитных заявок с помощью методик скоринга, в связи с чем применяемые банками методики требуют постоянной доработки. Предложенная методика опирается на исследования социально-психологических особенностей заемщиков – физических лиц.

Ключевые слова: кредитоспособность, скоринг, банковская сфера, заемщик, физическое лицо.

Для создания собственной методики был проанализирован ряд исследований на тему влияния параметров заемщика - физического лица на возврат кредитов.

При рассмотрении бальной оценки возраста были учтены исследования [1–4], где авторы пришли к выводу, что заемщики более старшего возраста исправнее исполняют свои обязательства перед банком.

Отсутствие у супруга регулярного стабильного дохода увеличивает финансовую нагрузку на заемщика [1–3]. В данном случае, супруг заёмщика может условно считаться иждивенцем.

Авторы источников [2–5] отмечают, что чем выше уровень образования заемщиков, тем ниже уровень невозврата кредитов, и, наоборот, чем ниже уровень образования заемщиков, тем выше уровень невозврата кредитов.

Авторы источников [1–3, 5] отмечают, что чем больше у заемщика иждивенцев, тем выше риск невыплаты кредита, и наоборот, чем меньше у заемщика иждивенцев, тем ниже риск невыплаты кредита.

Наличие автомобиля или недвижимости напрямую не может говорить об исполнении или неисполнении заемщиком своих долговых обязательств, однако наличие автомобиля или недвижимости у заемщика свидетельствует о его возможном достатке и дает банку возможность взять данное имущество под залог.

Отсутствие или наличие факта просрочки платежей по кредиту свидетельствует о платежной дисциплине заемщика. Заемщик без просрочек платежей по кредиту получает максимальный балл.

Созданная методика представлена на рис. 1, 2.

Предлагаемая методика содержит вопросы для вычисления дополнительных параметров оценки платежеспособности заемщика.

В соответствии с набранным итоговым баллом потенциального заемщика можно отнести к следующим группам:

– От 19 до 22 баллов – надёжный заёмщик.

– От 15 до 18 баллов – хороший заемщик.

– От 11 до 14 баллов – стандартный заемщик.

– От 8 до 10 баллов – ненадёжный заемщик.

– Менее 8 баллов – безнадёжный заемщик.

Таким образом, созданная методика подходит для оценки платёжеспособности заемщика – физического лица и при необходимости может быть дополнена необходимыми, по мнению экспертов, параметрами. При составлении методики не учитывалась какая-либо банковская стратегия или политика кредитования.

Показатель	Значение	Балл
Возраст клиента (рассматривается во всех авторских методиках)	До 21 года	0
	От 21 до 35	1
	От 35 до 45	2
	От 45 до 60	3
	От 60 и выше	1
Семейное положение клиента (рассматривается во всех авторских методиках)	Женат/Замужем	1
	Холост/ Разведен(-а)/Овдовел(-а)	0
Имеет ли супруг стабильный ежемесячный доход? (Добавлен. Оценивается как 1 иждивенец)	Да, имеет.	0,5
	Нет, не имеет/ Супруг отсутствует.	0
Образование клиента (рассматривается во всех авторских методиках)	Ученая степень/второе высшее	1,5
	Высшее образование	1
	Среднее специальное	0,5
	Среднее/Неоконченное высшее	0
Наличие иждивенцев (рассматривается в большинстве авторских методик)	Отсутствуют	2
	1	1,5
	2	1
	3	0,5
	Более 3	0
Наличие недвижимости (рассматривается в большинстве авторских методик)	Отсутствует	0
	Имеется	1,7
Наличие автомобиля (рассматривается в авторской методике)	Имеется	1,5
	Отсутствует	0
Имеется ли у Вас факт просрочки платежей по кредитам? (рассматривается в большинстве авторских методик)	Да	0
	Нет	2,2
	Не брал(-а) кредит	1,1
Величина среднемесячного дохода клиента (рассматривается во всех авторских методиках)	Менее 10 000 рублей	0
	От 10 000 до 20 000 рублей	1
	От 20 000 до 30 000 рублей	2
	От 30 000 до 60 000 рублей	3
	От 60 000 до 100 000 рублей	4
	Свыше 100 000 рублей	5
Остаток от среднемесячного располагаемого дохода клиента после выплаты платежа по кредиту, в % (Добавлен. Считается на основе дополнительных сведений. Свободный остаток баллов)	Менее 35%	0
	От 35% до 50%	1,2
	От 50% до 70%	2,4
	Более 70%	3,6
Максимальная сумма по таблице	22	
Минимальная сумма по таблице	0	
Дополнительные сведения для проверки финансового состояния клиента		
Средний ежемесячный доход, в рублях		-
Алименты, иные расходы, на аренду		-
Участие в программе личного страхования, годовая сумма взноса		-
Наличие прочих регулярных доходов		-
Годовая плата за учебу		-
Платежи по текущим займам		-

Рис. 1. Методика скоринга заемщиков физических лиц

Параметр	Формула расчета
Прожиточный минимум в регионе кредитования	Определяется регионом = ПМ
Количество иждивенцев	= И
Средний ежемесячный доход, в рублях	= Ср. мес. доход
Ежемесячная сумма прочих регулярных доходов	= Пр.доходы
Итоговый среднемесячный доход	Ср. мес. Доход + Пр.доходы = Итог.Дох
Расходы на содержание	И * ПМ = Расход
Алименты, иные расходы, на аренду	= А
Годовая плата за учебу	= У
Годовая сумма взноса по программе личного страхования	= С
Сумма платежей по текущим займам	= З
Среднемесячный расход	Расход + А + З + (У/12) + (С/12) = Ср.мес. расход
Среднемесячный располагаемый доход	Итог.Дох – Ср.мес. расход = Ср.мес.доход.
Доля ежемесячного платежа	Месяч. платеж по кредиту/Ср.мес.доход = ДП
Остаток от среднемесячного располагаемого дохода клиента после выплаты платежа по кредиту, в %	100*(1 – ДП) = Остаток от Ср.мес.доход, в %

Рис. 2. Дополнительные параметры для оценки платежеспособности

ЛИТЕРАТУРА

1. Improving credit scoring model of mortgage financing with smote methods in sharia banking / Wibowo Hariz Eko, Mulyati Heti, Saptono Imam Teguh // Russian Journal of Agricultural and Socio-Economic Sciences. – 2019. – No. 8 (92). – PP. 56–67.

2. Пикалова М.Д. Скоринговая система как метод оценки кредитоспособности заемщика – физического лица / М.Д. Пикалова, И.А. Чеховская // Управление. Бизнес. Власть. – 2016. – № 1 (10). – С. 76–79.

3. Капелюш А.К. Социально-демографическая структура российской банковской клиентуры // Финансы и кредит. – 2007. – № 7 (247). – С. 10–18.

4. Гагарина М.А. Социально-психологические особенности и уровень финансовой грамотности должников / М.А. Гагарина, А.А. Шанцева // Журнал «Review of business and economic studies». – 2017. – Т. 5, № 2. – С. 5–22.

5. Ниворожкина Л.И. Статистическая оценка рисков потребительского кредитования / Л.И. Ниворожкина, З.А. Морозова, Т.Г. Синявская // Вестник Ростовского гос. экономического ун-та (РИНХ). – 2012. – № 4 (40). – С. 66–76.

УДК 303.022

РЫНОК ОНЛАЙН-ОБРАЗОВАНИЯ КАК ПОТЕНЦИАЛЬНАЯ УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Г.Р. Егле, А.В. Осипенко, Е.И. Васильев, студенты каф. БИС

Научный руководитель А.С. Колтайс, ст. преп. каф. ЭБ

г. Томск, ТУСУР, germanegle@mail.ru, pstskaa@yandex.ru, egg.or.no@gmail.com

Проект ГПО ЭБ-2301. Разработка электронного курса по профессии «Системный аналитик»

Проводятся анализ онлайн-курсов, их плюсы и минусы, а также сравнение с обучением в высшем учебном заведении. Рассматриваются резуль-

таты опроса выпускников онлайн-школ, разбирается причина сокращения количества студентов, обучающихся в университетах, а также влияние онлайн-курсов на экономическую безопасность страны в связи с переходом абитуриентов от традиционного обучения в дистанционное с использованием онлайн-курсов.
Ключевые слова: онлайн-курсы, обучение, угроза, анализ, потери, экономическая безопасность.

В настоящее время большую популярность обретают онлайн-курсы, которые, по мнению авторов, позволяют получить качественное образование в сроки от 3 до 12 месяцев, а также сразу после обучения трудоустроиться и получать высокий оклад [1]. По данной причине тема уровня и качества получаемого образования от онлайн-курсов стала весьма актуальной.

Онлайн-обучение – это удобный метод, используемый в качестве альтернативы традиционному обучению и позволяющий людям успешно совершенствоваться. Однако, на сегодняшний день существует большое количество немаловажных аспектов, над которыми, с целью увеличения преимуществ онлайн-курсов в ходе преподавания и обучения, необходима доработка.

В таблице рассмотрены плюсы и минусы онлайн-образования в сравнении с традиционным обучением в вузе.

Преимущества и недостатки онлайн-курсов

Плюсы	Минусы
Экономия времени и сокращение расходов на дорогу	Необходимо техническое оснащение в виде компьютера и стабильного интернет-соединения
Развитие навыка самообразования, материал усваивается лучше, когда приходится разбираться в нём самому	Потеря самодисциплины
Разнообразие учебных программ, собранных в одном месте	Проблемы со здоровьем из-за сидячего образа жизни и постоянного использования компьютера
Возможность самостоятельного распределения времени для обучения	Устанавливаются жесткие дедлайны к выполнению заданий. В случае невыполнения работ возможна доплата за продление временного ограничения
Привлечение практикующих специалистов	Недостаточный объем практических заданий, что впоследствии особенно негативно сказывается на профессиях технической направленности

Главным же недостатком онлайн-обучения является высокая цена за неполную базу знаний в изучаемой области. Так, по данным сайта

«Sravni.ru», стоимость прохождения курса в области IT-безопасности варьируется от 10 до 170 тыс. руб., самые популярные курсы стоят около 100 тыс. руб. [1].

Таким образом, в связи с высокими показателями выручки, делается вывод, что главной целью любого коммерческого онлайн-продукта является заработок денежных средств. Для получения наибольшей прибыли для каждого клиента используется следующая политика – выдаётся неполная база знаний, после чего предлагается следующий курс для получения недостающего материала. Следовательно, для приобретения фундаментальных знаний в определенной области необходимо пройти 2–3 курса, последовательно предложенных авторами. С учетом средней цены в 100 тыс. руб. за курс получение образования стоит порядка 300 тыс. руб.

По данным проведенного опроса 50 выпускников онлайн-курсов, 8 человек проходили два и более курса, а 42 – в связи с высокой ценовой политикой остановились на прохождении одного. Полученные данные свидетельствуют о том, что после прохождения онлайн-обучения большая часть людей не может устроиться на работу по причине нехватки должных компетенций.

В свою очередь, высшее образование позволяет получить необходимые навыки, необходимые для высокого качества выполнения дальнейших трудовых функций по специальности.

Тем не менее в последние годы существенная часть молодежи считает, что значение высшего образования переоценено, и оно является необязательным для построения успешной карьеры [2]. Абитуриенты выбирают более быстрый и простой способ получения образования в виде прохождения онлайн-курсов. По данным Высшей школы экономики, за последние 15 лет количество поступающих снизилось на 59% – с 7 млн человек в 2006 г. до 4 млн в 2022 г., из которых на платной основе обучается 2,1 млн человек [3].

Так как количество людей, получающих высшее образование, падает, то и количество денег, получаемых государством, тоже сокращается. На сегодняшний день получение образования на очном отделении бакалавриата стоит порядка 150 тыс. руб. в год. Следовательно, с каждого студента, решившего сделать выбор в сторону онлайн-курсов, государство теряет около 600 тыс. руб. [4].

После анализа онлайн-курсов были получены данные, что большая их часть зарегистрирована как «ООО» (общество с ограниченной ответственностью), а следовательно, лишь 20% от прибыли данных организаций отчисляются в налоговую службу. Если рассматривать среднюю цену в 100 тыс. руб. за курс и 12 месяцев обучения, то госу-

дарство получает 10 тыс. в год с одного онлайн-учащегося, что составляет всего 6,67% от суммы, перечисляемой государству от студента вуза. В будущем данный факт может стать существенной угрозой для экономической безопасности страны.

ЛИТЕРАТУРА

1. Онлайн-курсы – полный список лучших обучений онлайн в каталоге образования [Электронный ресурс]. – Режим доступа: https://www.sravni.ru/kursy/ (дата обращения: 03.03.2023).

2. Большинство молодых россиян считают высшее образование переоцененным [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/3702004 (дата обращения: 03.03.2023).

3. Как в России устроена система высшего образования [Электронный ресурс]. – Режим доступа: https://journal.tinkoff.ru/statistic-univercitites/ (дата обращения: 04.03.2023).

4. Стоимость обучения в России [Электронный ресурс]. – Режим доступа: https://studyinrussia.ru/study-in-russia/cost-of-education-in-russia (дата обращения: 04.03.2023).

СЕКЦИЯ 5

ЭКОНОМИКА, УПРАВЛЕНИЕ, СОЦИАЛЬНЫЕ И ПРАВОВЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ

ПОДСЕКЦИЯ 5.1

МОДЕЛИРОВАНИЕ В ЭКОНОМИКЕ

Председатель секции – ***Мицель А.А.****, проф. каф. АСУ, д.т.н.;*
зам. председателя – ***Грибанова Е.Б.****, доцент каф. АСУ, к.т.н.*

УДК 519.816

НЕЧЕТКАЯ МОДЕЛЬ ВЫБОРА АЛЬТЕРНАТИВ ОБУЧЕНИЯ СОТРУДНИКОВ В РЕСТОРАНЕ

А.А. Захарова, проф., доцент, д.т.н.; П.А. Куминов, студент
г. Томск, ТУСУР, каф. АСУ, pavekum@mail.ru

Представлены выработка и оценка альтернатив решения проблемы, связанной с низкой оборачиваемостью столов при оказании услуг в ресторане на основе методов системного анализа.
Ключевые слова: системный анализ, теория систем, моделирование, принятие решений.

Ресторан – важная часть общества. Для одних – это быстрое место для приема пищи, для других – источник гастрономического и эстетического удовольствия.

Объектом исследования является ресторан, а предметом исследования – процесс оказания услуг.

Цель ресторанного бизнеса – получение прибыли путем организации питания и досуга или без досуга [1].

Низкая текучесть клиентов в ресторане не только создает заминки в главном зале, но также влияет на работу кухни.

Таким образом, выделяется проблема – низкая оборачиваемость столов: за единицу времени за столом пребывает недостаточное количество посетителей.

Исходя из предмета исследования, ресторан стоит разделить на две части: зал и кухню. Рассмотрим проблему с точки зрения работы кухни.

Если смена людей происходит недостаточно быстро, то проблема заключается в быстроте работы официантов – надо увеличить скорость их работы. Для повышения скорости работы официантов нужно повысить эффективность работы с клиентом.

Наилучшим вариантом повышения навыков сотрудников является создание эффективной системы обучения персонала. Рассмотрим 5 альтернатив:

1. Курсы повышения квалификации – улучшение компетенций сотрудников в соответствии с профессиональными требованиями.
2. Мастер-классы – несколько занятий в малой группе, где демонстрируется, как применять на практике новую технологию.
3. Менторство – обучение младшего сотрудника через взаимодействие со старшим в процессе работы.
4. Тренинг – интенсивное обучение для решения определенной проблемы.
5. Инструктаж – базовый вид обучения, где сотруднику разъясняются и демонстрируются приемы работы.

Для оценки альтернатив использовалось нечеткое многокритериальное оценивание на основе Гауссовой функции принадлежности лингвистической переменной [2]. В общем виде функции принадлежности имеют следующий вид:

$$\mu_{X_1} = \begin{Bmatrix} 1 \text{ при } x \le a_1, \\ e^{-(x-a_1)^2/2\sigma_{11}^2} \text{ при } x \ge a_1, \end{Bmatrix};$$

$$\mu_{X_2} = \begin{Bmatrix} e^{-(x-a_1)^2/2\sigma_{21}^2} \text{ при } x \le a_2, \\ e^{-(x-a_1)^2/2\sigma_{22}^2} \text{ при } x > a_2, \end{Bmatrix};$$

$$\mu_{X_n} = \begin{Bmatrix} e^{-(x-a_n)^2/2\sigma_{nn-1}^2} \text{ при } x \le a_n, \\ 1 \text{ при } x > a_n, \end{Bmatrix}.$$

При обучении наиболее важными являются такие критерии, как количество сотрудников, которые могут попасть на один поток обучения (КПО), количество сотрудников, улучшивших показатели (КУП) среди прошедших обучение. Для оценки альтернатив была введена выходная лингвистическая переменная – эффективность (Э).

Необходимо составить нечеткие множества лингвистических переменных для данных критериев: {Низкий, Средний, Высокий}. Элементам множеств будут соотноситься элементы множества четких значений, выраженные в процентах {0, 50, 100}. Параметры функции Гаусса представлены в табл. 1.

Таблица 1

Параметры функции Гаусса

Базовые значения	Доминирующее значение нечеткого мн-ва	Пограничные значения соседних термов y_{kj}	Степень принадлежности пограничных значений μ_k
Низкий	0	$y_{k1} = 45$ $y_{k2} = 80$	$\mu_1 = 0,5$ $\mu_2 = 0,5$
Средний	50		
Высокий	100		

Для определения степени принадлежности лингвистических переменных была построена следующая система правил:

1. ЕСЛИ КУП = «Низкий» И КПО = «Низкий» ТО Э = «Низкий».
2. ЕСЛИ КУП = «Низкий» И КПО = «Средний» ТО Э = «Низкий».
3. ЕСЛИ КУП = «Средний» И КПО = «Низкий» ТО Э = «Низкий».
4. ЕСЛИ КУП = «Средний» И КПО = «Средний» ТО Э = «Средний».
5. ЕСЛИ КУП = «Низкий» И КПО = «Высокий» ТО Э = «Средний».
6. ЕСЛИ КУП = «Высокий» И КПО = «Низкий» ТО Э = «Средний».
7. ЕСЛИ КУП = «Средний» И КПО = «Высокий» ТО Э = «Высокий».
8. ЕСЛИ КУП = «Высокий» И КПО = «Средний» ТО Э = «Высокий».
9. ЕСЛИ КУП = «Высокий» И КПО = «Высокий» ТО Э = «Высокий».

Экспертные оценки критериев для каждой альтернативы и их эффективность представлены в табл. 2.

Таблица 2

Экспертные оценки критериев

Альтернатива	Экспертная оценка		Эффективность альтернативы
	КУП	КПО	
Курсы повышения квалификации	70	70	0,575
Мастер-классы	50	30	0,44
Менторство	90	15	0,8
Тренинг	60	50	0,56
Инструктаж	20	30	0,32

Наибольшее значение имеет альтернатива № 3 – менторство, из чего следует вывод, что данный способ обучения сотрудников является наиболее эффективным.

ЛИТЕРАТУРА

1. ГОСТ 30389–2013. Услуги общественного питания [Электронный ресурс]. – Режим доступа: https://internet-law.ru/gosts/gost/57023 (дата обращения: 10.03.2023).

2. Силич М.П. Основы теории систем и системного анализа: учеб. пособие / М.П. Силич, В.А. Силич. – Томск: ТУСУР, 2013. – 342 с.

УДК 519.816

ВЫБОР АЛЬТЕРНАТИВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОЦЕССА РАЗРАБОТКИ КОРПОРАТИВНОГО САЙТА В WEB-СТУДИИ

А.А. Захарова, проф., доцент, д.т.н.; А.А. Лузинсан, студентка

г. Томск, ТУСУР, каф. АСУ, luzinsan@mail.ru

Текущая глобальная ситуация ставит задачу создания инструментов для рационального принятия решений в процессе разработки корпоративных веб-сайтов и других информационных продуктов. Представлены результаты исследования альтернативных вариантов решения проблемы превышения бюджета на разработку корпоративных веб-сайтов.

Ключевые слова: системный анализ, корпоративный сайт, web-студия, превышение бюджета, метод группового парного сравнения.

В современном мире Web-студии предоставляют обширный список услуг, в числе которых доступны: разработка веб-приложений, создание корпоративных сайтов и порталов, разработка интернет-магазина, веб-сервисы и решения для электронной коммерции. Предмет интереса в данном случае представлен корпоративным сайтом. Корпоративный сайт считается интернет-ресурсом, на котором представлена подробная информация о деятельности организации или предприятия. От одностраничного приложения (SPA) или лендинга корпоративный сайт отличается многоуровневой структурой и большими объёмами информации, а также возможностью интеграции системы во внутреннюю корпоративную сеть, ведением документооборота и бухгалтерии, управлением и визуализацией бизнес-процессов, а также кластеризацией веб-ресурса [1]. В конечном итоге целью функционирования Web-студии является получение прибыли за счёт реализации и интеграции корпоративного сайта, выступающего в роли информационной платформы для успешного развития бизнеса заказчиков.

Среди конечных причин в ходе анализа возможного неудовлетворительного состояния Web-студии были выделены только некото-

рые из них [2, 3]: некомпетентность привлечённых специалистов для обработки узкоспециализированной информации, отсутствие чётко поставленных целей и задач, отсутствие участия заказчика на некоторых этапах исполнения проекта, неинициативность команды разработчиков по отношению к заказчику, санкции в IT-сфере, организационные и структурные изменения со стороны заказчика, смена команды разработчиков. Построив дерево причин и проведя оценку коренных причин методом парного сравнения [4], была выявлена наиболее весомая причина – санкции в IT-сфере.

На следующем этапе было построено дерево целей [4] с листьями, представленными следующими задачами: привлечение экспертов со стороны заказчика, помощь в определении целей и задач заказчика, назначение фиксированного расписания встреч команды разработчиков с заказчиком, проведение анализа доступных вендоров и оценка рисков, составление матрицы заинтересованных сторон, анализ конкурентов.

Конечная цель в виде анализа доступных вендоров и оценки рисков» была определена на основе метода анализа иерархий [4]. Выделенная цель может быть достигнута посредством реализации одной из следующих альтернатив [5]: создание списка потенциальных вендоров исходя из предоставленной информации специализированных организаций, заимствование вендора компании конкурента, изучение списка популярных изданий в сети Интернет, обращение к TRF-компании и анализ индустриального фокуса, предоставленного вендора, обращение к финансовым аналитикам в банки и инвестиционные компании и функциональный анализ.

В качестве метода, использованного для нахождения наилучшей альтернативы достижения поставленной цели, использовался метод группового парного сравнения [4] с системой оценок 1/0. Метод парного оценивания представляет собой процедуру установления предпочтения объектов при сравнении всех возможных пар. При этом результаты сравнения всех пар объектов представляются в виде матрицы с булевыми значениями, построение которой производится по следующей формуле:

$$w_{ij} = \begin{cases} 1, \text{ если } x_i > x_j \text{ или } x_i \equiv x_i; \\ 0, \text{ если } x_i < x_j \text{ при } i, j \equiv \overrightarrow{1, n} \end{cases},$$

где n – количество альтернатив.

Данная матрица обязана быть согласованной, т.е. должны быть выполнены условия: по главной диагонали расположены единицы; если элемент i-й строки и j-го столбца равен единице, то элемент j-й

строки и *i*-го столбца должен быть равен 0, и наоборот; должна выполняться транзитивность. Так как в качестве метода используется оценка группового парного сравнения, то высчитывается матрица парных сравнений для каждого эксперта. После этого строится обобщённая матрица парных сравнений, которая заполняется таким образом, что элемент обобщённой матрицы равен 1 только в том случае, если половина или больше экспертов посчитали этот элемент равным 1. Пример обобщённой матрицы представлен в таблице. Здесь же вычисляются ранги объектов, где наиболее предпочтительный объект получает ранг 1, а наименее предпочтительный – максимальный ранг.

Пример обобщённой матрицы

	x_1	x_2	x_3	x_4	x_5	Сумма элементов	Ранг альтернативы
x_1	1	1	1	1	1	5	1
x_2	0	1	0	0	0	1	5
x_3	0	1	1	0	0	2	4
x_4	0	1	1	1	0	3	3
x_5	0	1	1	1	1	4	2

Таким образом, в результате расчётов наилучшей альтернативой выступила альтернатива «Создание списка потенциальных вендоров исходя из предоставленной информации специализированных организаций, и оценки рисков на основе годового оборота, прибыльности и клиентской базы вендора».

ЛИТЕРАТУРА

1. Корпоративный сайт: требования // Комсомольская правда. – URL: https://www.kp.ru/guide/korporativnyi-sait.html

2. 7 причин, по которым веб-проекты не доводятся до конца, и как с этим бороться // SEO блог в Worksolutions [Электронный ресурс]. – URL: https://worksolutions.ru/blog/7-reasons-projects-fail/

3. Сложности, с которыми сталкиваются клиенты веб-студий // Обзор на исследование в журнале CNS Magazine [Электронный ресурс]. – URL: https://cmsmagazine.ru/journal/research-difficulties-faced-by-web-studio-clients/

4. Силич М.П. Основы теории систем и системного анализа: учеб. пособие / М.П. Силич, В.А. Силич. – Томск: ТУСУР, 2013. – 342 с.

5. Эффективный ИТ-отдел. – Ч. 5: Как правильно выбирать вендора. Шаг 2. – Статья Г. Галкина на информационном портале intelligent [Электронный ресурс]. – URL: https://www.iemag.ru/master-class/detail.php?ID=15705

УДК 618.518 (075.8)

МОДЕЛИРОВАНИЕ ЗАДАЧИ О НАЗНАЧЕНИЯХ ПРИ РАСПРЕДЕЛЕНИИ ЗАДАЧ МЕЖДУ СОТРУДНИКАМИ IT-КОМПАНИИ

Р.Р. Мустакимов, аспирант

Научный руководитель А.А. Мицель, проф. каф. АСУ, д.т.н.

г. Томск, ТУСУР, каф. АСУ, mustakimov.ruslan97@gmail.com

Обосновывается важность проблемы распределения рабочего времени сотрудников в IT-компаниях. Рассматривается способ решения проблемы с помощью задачи о назначениях, который заключается в его модификации и добавлении в модель новых переменных и ограничений.

Ключевые слова: IT, сотрудники, распределение рабочего времени, задача о назначениях.

Проблема учёта и распределения рабочего времени сотрудников в настоящий момент имеет большую значимость в организациях, занимающихся разработками и исследованиями в сфере IT [1]. Задачи учёта и распределения рабочего времени актуальны как для так называемых «продуктовых» организаций – IT-организаций или подразделений, выполняющих работы для или в рамках организации, занятой в другой отрасли, так и для «аутсорс» и «аутстафф» организаций, специализирующихся на выполнении работ в рамках заказов от компаний-заказчиков. Значимость проблемы обусловливается необходимостью оптимизации распределения ресурса – рабочей силы. Оптимизация распределения рабочей силы позволяет сократить затраты, ускорить реализацию проектов и положительно влияет на существование и развитие компании [2].

Одним из возможных способов решения указанной проблемы является моделирование и решение задачи о назначениях [3]. Математически такие задачи относятся к задачам линейного программирования, суть которых заключается в оптимизации функции вида (1) [4].

$$f(x)=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{ij}x_{ij}\rightarrow\min. \qquad (1)$$

При решении задачи о назначениях предполагается, что $c_{i,j}$ – приносимый доход либо время, необходимое при выполнении каждым работником той или иной задачи. В случае использования времени целевая функция должна минимизироваться – необходимо минимизировать затраты на выполнение той или иной задачи работником предприятия.

При распределении задач необходимо также учитывать фактор важности той или иной задачи, фактор необходимой квалификации для реализации задачи, а также уровень квалификации сотрудников. Важность задач можно отобразить в отдельной матрице, обозначив её *w*. Тогда важность *j*-й задачи будет обозначаться как w_j. При определении важности воспользуемся методом ранжирования, где каждой задаче присваивается ранг от 1 – самой важной задачи до *n* – наименее важной задачи.

Для отображения уровня квалификации сотрудников и необходимого уровня квалификации при решении задачи можно обратиться к общепринятой в IT-компаниях системе оценки компетенций «junior, middle, senior» [5]. Эта система предполагает оценку компетенций в соответствии с тремя уровнями:

– junior – сотрудник знаком с технологией или методом решения, имеет небольшой опыт, при работе может столкнуться с трудностями;

– middle – сотрудник уверенно владеет технологией или методом решения, опыт от двух лет, возникающие при работе трудности решает самостоятельно за короткое время;

– senior – сотрудник отлично владеет технологией, разбирается в нюансах, может разработать и предложить собственный метод решения, опыт от 3 лет и более, скорость решения подобных задач минимальна по сравнению с другими сотрудниками.

Чтобы использовать описанную выше систему оценки квалификации, необходимо:

– задать матрицу необходимых квалификаций для выполнения задач, обозначим её **L**, элементы – l_k;

– расширить матрицу **C**, создав для неё 3 «сечения» в соответствии с количеством уровней компетенции, назовём эти сечения **C**(1), **C**(2) и **C**(3).

Матрицы **C**(*k*) будут содержать предполагаемые данные о времени, затрачиваемом на реализацию той или иной (*j*-й) задачи определенным (*i*-м) сотрудником. Если квалификация сотрудника ниже, чем требуется для определенной задачи, то время выполнения такой задачи будет на порядок выше, чем у сотрудника с соответствующей квалификацией.

С учётом всех введенных обозначений сформируем функцию задачи о назначениях (2), которую необходимо минимизировать:

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{o} C(k)_{i,j}\ w_j l_k\ x(k)_{i,j} \to \min, \qquad (2)$$

где *n* – количество сотрудников; *m* – количество задач; *o* – количество уровней компетенций (3, но может быть и другим); $C(k)_{i,j}$ – количество

часов, затрачиваемое i-м сотрудником на выполнение j-й задачи в разрезе компетенций уровня k; w_j – уровень важности j-й задачи; l_k – уровень требуемых компетенций для решения задачи; $x(k)_{i,j}$ – 1 или 0, выполняется ли i-м сотрудником j-я задача для уровня компетенций k.

Необходимо также ввести ограничения следующего формата:

– j-ю задачу должно выполнять количество сотрудников не меньше $a1_j$ и не больше $b1_j$;

– i-й сотрудник может выполнять не меньше $a2_i$ и не больше $b2_i$ задач в рамках любого уровня компетенций;

– затрачиваемые на реализацию задач k-го уровня ресурсы не могут быть меньше $a3_k$ и больше $b3_k$.

Тогда сформированная задача о назначениях будет выглядеть следующим образом (3):

$$\begin{cases} \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{o} c(k)_{i,j}\ w_j l_k\ x(k)_{i,j} \to \min, \\ a1_j \le \sum_{i=1}^{n} \sum_{k=1}^{o} c(k)_{i,j}\ x(k)_{i,j} \le b1_j, \\ a2_j \le \sum_{k=1}^{o} \sum_{i=1}^{m} c(k)_{i,j}\ x(k)_{i,j} \le b2_j, \\ a3_k \le \sum_{i}^{n} \sum_{j}^{m} c(k)_{i,j}\ x(k)_{i,j} \le b3_k. \end{cases} \quad (3)$$

Решение сформированной задачи о назначениях методом Монте–Карло показало хорошие результаты на тестовых данных.

ЛИТЕРАТУРА

1. Пот, слезы и учет времени – как мы повышали рентабельность компании [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/457582/, свободный (дата обращения: 02.02.2023).

2. Хитрова Т.И. Проблемы распределения работ в процессе реализации инновационных задач / Т.И. Хитрова, А.С. Низовцева // Baikal Research Journal. – 2020. – Т. 11, № 2. DOI: 10.17150/2411-6262.2020.11(2).15

3. Хитрова Т.И. Методы формирования состава исполнителей IT-проекта / Т.И. Хитрова, С.С. Ованесян, А.С. Низовцева // Baikal Research Journal. – 2020. – Т. 11, № 4. DOI: 10.17150/2411-6262.2020.11(4).

4. Мицель А.А. Исследование операций и методы оптимизации. – Ч. 1: Лекционный курс: учеб. пособие. – Томск: ТУСУР, 2019. – 167 с.

5. Джуниор, мидл и сеньор. Как определить грейд специалиста [Электронный ресурс]. – Режим доступа: https://friend.work/blog/junior_middle_and_senior, свободный (дата обращения: 10.03.2023).

УДК 004.8

НЕЙРОСЕТЕВАЯ МОДЕЛЬ ПРОГНОЗИРОВАНИЯ РЕНТАБЕЛЬНОСТИ ФИРМ, ОРИЕНТИРОВАННЫХ НА РОЗНИЧНЫЙ РЫНОК

Е.Б. Грибанова, доцент каф. АСУ ТУСУРа, к.т.н.;
Л.Ю. Спицына, доцент ОСГН ШБИП НИ ТПУ, к.э.н.;
И.А. Лызин, ассистент ОИТ ИШИТР НИ ТПУ
г. Томск, ТУСУР, НИ ТПУ, geb@asu.tusur.ru,
s_luba_07@mail.ru, lyzin@tpu.ru

Рассматривается решение задачи прогнозирования рентабельности с использованием машинного обучения. Приводятся описание регрессионной модели и нейросетевой модели, а также результаты моделирования.

Ключевые слова: рентабельность, машинное обучение, нейросетевая модель, панельные данные.

Задача предсказания эффективности деятельности предприятия является актуальной для инвесторов и собственников компаний. Рентабельность – это один из основных показателей, который характеризует успешность бизнеса.

В литературе одним из наиболее популярных инструментов для прогнозирования рентабельности являются методы машинного обучения. При этом выполняется как прогнозирование величины рентабельности (задача регрессии) [1], так и прогнозирование признака, является ли предприятие рентабельным (задача классификации) [2]. В качестве объекта рассматривается группа предприятий, относящихся к какой-либо отрасли или классу: отели [3], магазины «у дома» [2], банки и т.д.

Для исследования были отобраны компании, осуществляющие деятельность в сфере производства и обслуживания и ориентированные на розничный рынок. В выборку входит 265 компаний пищевой промышленности, ИТ-сектора и др. Данные были собраны за 2016–2020 гг. с использованием систем СПАРК и Seranking и разделены на две части:

1. Обучающая выборка (2017–2019 гг.) используется для обучения моделей и выявления взаимосвязей между переменными. Представляет собой панельные данные и включает 795 наблюдений (265 предприятий, 3 г.).

2. Тестовая выборка (2020 г.) используется для предсказания рентабельности фирм. Включает значения переменных за 2020 г.

Были определены следующие входные данные модели: натуральный логарифм выручки (Size), доля основных средств в общих акти-

вах (FATA), коэффициент текущей ликвидности (CALC), возраст организации (age), оборачиваемость активов (Turnover), финансовый рычаг (Leverage), интернет-трафик (trorg1), рентабельность в предыдущий момент времени (ROAt-1), рост продаж (Growth), три дамми-перменные, учитывающие различия рентабельности между предприятиями разных отраслей (Dummy1, Dummy2, Dummy3). Выходная величина – рентабельность предприятия (ROA).

Для анализа панельных данных была использована регрессионная модель со случайными эффектами. Полученное регрессионное уравнение имеет следующий вид:

$$ROA = 8{,}97 + 0{,}13^* Size - 1{,}1^* FATA + 1{,}12^* CACL - 4{,}07^* Leverage + 2{,}17^* Turnover - 0{,}13^* Age + 2{,}55^* Growth + 0{,}78^* Traffic + 1{,}21^* Growth^* Traffic + 5{,}98^* ROAt\text{-}1 + 0{,}16^* Dummy1 - 2{,}17^* Dummy2 - 1{,}05^* Dummy3.$$

Структура нейронной сети включает входной слой, два скрытых слоя и выходной слой (рис. 1).

Реализация моделей выполнена на языке Python.

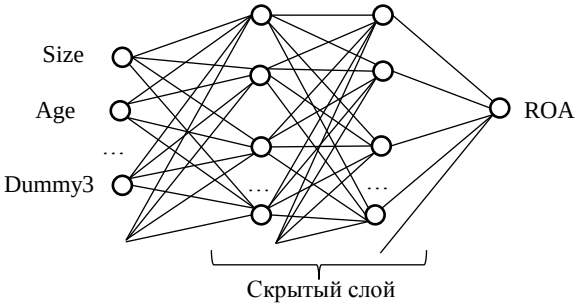


Рис. 1. Структура нейронной сети

В таблице приведены результаты моделирования, расчёт стандартных характеристик выполнен с использованием тестовой выборки.

Оценка точности прогноза

Модель	mae	mse	R^2	rmse
Регресионная	6,6	107,7	0,57	10,4
Нейросетевая	5,8	90,5	0,64	9,5

Согласно полученным результатам, нейросетевая модель обеспечивает более высокую точность погнозирования. На рис. 2 представлены реальные и прогнозные значения рентабельности для 20 предприятий.

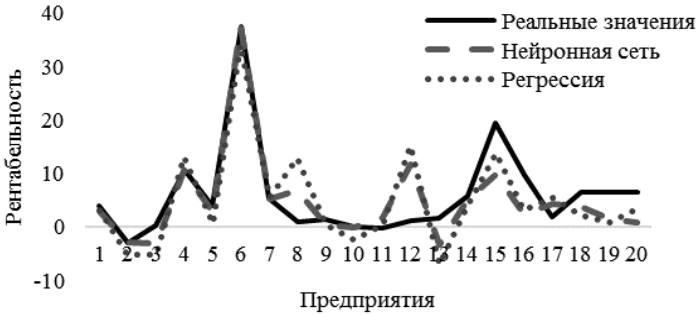


Рис. 2. Реальные и предсказанные значения рентабельности

Исследование выполнено за счет гранта Российского научного фонда № 22-28-01795, https://rscf.ru/project/22-28-01795.

ЛИТЕРАТУРА

1. Lee J. Deep Learning-Based Corporate Performance Prediction Model Considering Technical Capability / J. Lee, D. Jang, S. Park // Sustainability. – 2017. – № 9. – PP. 1–12.

2. Lado-Sestayo R. Hotel profitability: a multilayer neural network approach / R. Lado-Sestayo, M. Vivel-Bua // Journal of Hospitality and Tourism Technology. – 2019. – Vol.11, No. 1. – PP. 35–48.

3. Goyeneche D. Predicting Profitability of Neighbourhood Stores in Colombia // Review of Integrative Business and Economics Research. – 2022. – Vol. 11, No. 2. – PP. 1–24.

УДК 519.246.8

ДИНАМИЧЕСКАЯ МОДЕЛЬ УПРАВЛЕНИЯ BSF-ПОРТФЕЛЕМ

Е.В. Викторенко, аспирант каф. экономики;
А.А. Мицель, проф. каф. АСУ, д.т.н.
г. Томск, ТУСУР, maa@asu.tusur.ru, elena.v.viktorenko@tusur.ru

Рассматривается портфель ценных бумаг, который включает в себя рисковый актив, безрисковый актив, а также депозит. Структура цен рискового актива имеет биномиальную структуру. Модель относится к классу моделей динамического программирования. Представленная модель принадлежит группе моделей динамического программирования. Для определения наиболее подходящей стратегии управления с обратной связью по квадратичному критерию применен линейный закон управления.

Ключевые слова: оптимальное управление, динамическое программирование, инвестиционный портфель, биномиальная структура цен рискового актива.

Динамические модели управления инвестиционным портфелем (ИП) достаточно подробно исследовались рядом авторов, такими как В.В. Домбровский, В.А. Гальперин, Т.Ю. Пашинская. Результаты работ перечисленных авторов используются для решения таких задач оптимизации ИП, как оптимизация при ограничениях на объемы торговых операций, оптимизация управления с обратной связью по квадратичному критерию, а также оптимизация при условии включения в портфель рисковых бумаг со случайной волатильностью. В работе [1] построена модель управления ИП с линейным критерием качества, имеющая динамическую структуру. В работах Е.Р. Колясниковой, Е.Р. Бронштейн проводится исследование BSF-портфелей с древовидной структурой цен рискового актива. Данными авторами рассматривается модель ИП, состоящего из рискового, безрискового актива, а также потока платежей по ним. Способам учета влияния тенденций рынка на динамику изменения цен рисковых активов посвящены работы В.В. Давнис, А.М. Федосеева.

В данной работе предлагается динамическая модель управления BSF-портфелем с квадратичным критерием качества, состоящим из безрискового, рискового активов и депозита. В отличие от работ В.В. Домбровского, В.А. Гальперина, Т.Ю. Пашинской, цены рискового актива изменяются случайным образом по древовидной структуре.

Расчеты были осуществлены в среде MatCad.

Рассмотрим портфель, состоящий из безрискового актива (БА), рискового актива (РА) и депозита (Д). Будем рассматривать дискретные моменты времени 0, 1, 2, …, n. Обозначим за $r_1(t)$ ставку доходности БА. Цена БА известна в каждый момент времени. Цена РА изменяется случайным образом, причём она может принимать одно из двух возможных значений, т.е. цены РА имеют структуру бинарного дерева (рис. 1). За p обозначим вероятность того, что цена РА увеличилась на случайную величину η, а за $q=1-p$ обозначим вероятность того, что цена актива уменьшилась на случайную величину η.

Обозначим за x долю БА, а за y – долю РА. Вершины с номерами (t+1, 2i–1) и (t+1, 2i) являются зависящими от (t,i)-й вершины или так называемыми наследниками. Цена РА в вершине с номером (t,i) равна $C''_{t,i}$ (при соответствии вершины моменту времени t). Цены РА в вершинах с номерами (t+1, 2i–1) и (t+1,2i) равны $C''_{t+1,2i-1}=C''_{t,i}\cdot(1+\eta_i)$ и $C''_{t+1,2i}=C''_{t,i}\cdot(1-\eta_i)$ соответственно (при соответствии вершин моменту времени t+1). Цена БА в вершине с номером (t, i), соответствующей моменту времени t, равна $C'(t)$, а це-

на БА в вершинах с номерами (t+1, 2i–1) и (t+1, 2i), соответствующими моменту времени t+1, равна $C'(t+1)$.

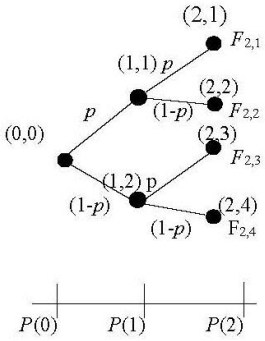


Рис. 1. Двухпериодное дерево РА

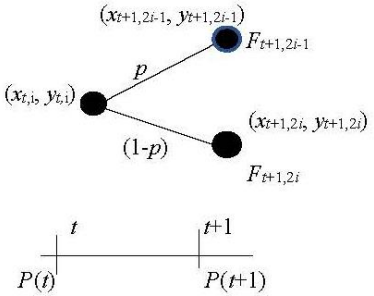


Рис. 2. Терминальные вершины дерева РА

Значение потока платежей $P(t)$ задаем для каждого момента времени t.

Будем полагать, что в начальный момент времени весь капитал помещен в БА и заемные средства не используются, а также что оба вида активов в ИП можно быстро продать или купить [2, 3]. Обратим внимание, что поток платежей, в свою очередь, является неликвидным инструментом, платежи по которому определены заранее.

Если рассматривать путь от начальной вершины дерева цен до его конечной вершины, то нужно иметь в виду, что этот путь является случайным.

Стратегия оптимального управления ИП состоит в определении в каждой вершине дерева цен количества БА x_i и РА y_i при выполнении следующих условий [2,3]:

а) на множестве терминальных вершин дерева задана платёжная функция $F_{t,i} \geq 0$ ($i = 1, 2, ..., 2^t$) – сумма, которую хотел бы получить инвестор при попадании цен активов в соответствующую вершину дерева цен после продажи активов и выплаты или поступления средств по потоку платежей;

б) за займы активов предусмотрена плата. Например, при займе x единиц безрисковых активов в следующий момент времени следует вернуть λx единиц БА. При займе y единиц рисковых активов следует вернуть μx единиц акций ($\lambda \geq 1$, $\mu \geq 1$). Имеют место следующие соотношения:

$$v_{t,i} = x_{t,i}, \text{ если } x_{t,i} \geq 0;\ v_{t,i} = \lambda x_{t,i}, \text{ если } x_{t,i} < 0, \quad (1)$$

$$u_{t,i} = y_{t,i}, \text{ если } y_{t,i} \geq 0;\ u_{t,i} = \mu y_{t,i}, \text{ если } y_{t,i} < 0, \quad (2)$$

при $i = 1, 2, ..., 2^t$;

в) рынок является самофинансируемым [4], т.е. инвестор может покупать и продавать активы, обеспечивая выплаты и поступления. Запишем это математически:

$$C'(t+1)\lambda x_{t,i} + C''_{t+1,2i-1}\mu y_{t,i} + P(t+1) = C'(t+1)x_{t+1,2i-1} + C''_{t+1,2i-1}y_{t+1,2i-1}, \quad (3)$$

$$C'(t+1)\lambda x_{t,i} + C''_{t+1,2i}\mu y_{t,i} + P(t+1) = C'(t+1)x_{t+1,2i} + C''_{t+1,2i}y_{t+1,2i}, \quad (4)$$

при $i = 1, ..., 2^t$.

В конечных вершинах (на рис. 2 данные вершины определены как терминальные) должны выполняться следующие неравенства:

$$C'(t+1)\lambda x_{t,i} + C''_{t+1,2i-1}\mu y_{t,i} - P(t+1) \geq F_{t+1,2i-1}, \quad (5)$$

$$C'(t+1)\lambda x_{t,i} + C''_{t+1,2i}\mu y_{t,i} - P(t+1) \geq F_{t+1,2i}. \quad (6)$$

В работе был предложен алгоритм построения динамической модели управления портфелем, состоящим из безрискового, рискового активов и депозита. В отличие от работ В.В. Домбровского, В.А. Гальперина, Т.Ю. Пашинской, цены рискового актива изменяются случайным образом по древовидной структуре.

ЛИТЕРАТУРА

1. Мицель А.А. Динамическая модель управления инвестиционным портфелем с линейным критерием качества / А.А. Мицель, Н.П. Красненко // Доклады ТУСУР. – 2014. – № 4 (34). – С. 176–182.

2. Бронштейн Е.М. Модель (B,S,F)-рынка и хеджирующие стратегии / Е.М. Бронштейн, Е.Р. Колясникова // Управление риском. – 2010. – № 2. – С. 55–64.

3. Бронштейн Е.М. Приближенные хеджирующие стратегии в модели (B,S,F)-рынка / Е.М. Бронштейн, Е.Р. Колясникова // Математическое моделирование. – 2010. – Т. 22, № 11. – С. 29–38.

4. Ширяев А.Н. Основы стахостической финансовой математики: в 2 т. – Т. 1: Факты. Модели. – М.: Фазис, 1998. – 512 с.

ПОДСЕКЦИЯ 5.2

ИНФОРМАЦИОННЫЕ СИСТЕМЫ В ЭКОНОМИКЕ

*Председатель секции – **Исакова А.И.**, доцент каф. АСУ, к.т.н.; зам. председателя – **Григорьева М.В.**, доцент каф. АСУ, к.т.н.*

УДК 004.42

ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ОТДЕЛА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АО «СИБИРСКАЯ ГОРНО-МЕТАЛЛУРГИЧЕСКАЯ КОМПАНИЯ»

С.С. Домрачева, студентка

Научный руководитель А.А. Захарова, д.т.н., проф. каф. АСУ

г. Томск, ТУСУР, каф. АСУ, ssdomracheva@yandex.ru

Описаны бизнес-процесс деятельности отдела информационных технологий АО «СГМК» по учету вычислительной техники и этапы его автоматизации.

Ключевые слова: вычислительная техника, учет, SADT-модель, информационная система.

В данной работе рассмотрим организацию АО «Сибирская горно-металлургическая компания» (СГМК). Она является одной из ведущих компаний на рынке России, а также лидером среди предприятий горно-металлургической отрасли в Кузбассе. Основная деятельность компании – поставка металлолома на предприятия Сибири и Урала, производство щебня, добыча доломита [1].

Отдел информационных технологий считается одним из важных отделов компании. Его задачей является сопровождение пользователей. В состав отдела входят 72 сотрудника, которые оснащены всей нужной вычислительной техникой.

Начальник отдела информационных технологий заинтересован в автоматизированном учете вычислительной техники в своем отделе, так как на каждого сотрудника приходится порядка 9 единиц техники. В данный момент времени такой учет ведется в программе Microsoft Excel, где хранится информация об инвентарном номере и ФИО сотрудника, отвечающего за технику. Есть потребность в расширении

информации о вычислительной технике, сокращении времени на учет и минимизации вероятности ошибок.

Есть необходимость хранить не только инвентарный номер сотрудника, но и ряд других важный сведений, таких как состояние техники на текущий момент времени, местоположение техники, даты принятия на учет.

Для выполнения структурного анализа была использована методология SADT (Structured Analysis and Design Technique). Она отражает описание бизнес-процессов с помощью функциональных диаграмм [2].

Отразим результат анализа полученных сведений в модели SADT «As-Is» учета вычислительной техники в детализации уровня A0 (рис. 1).

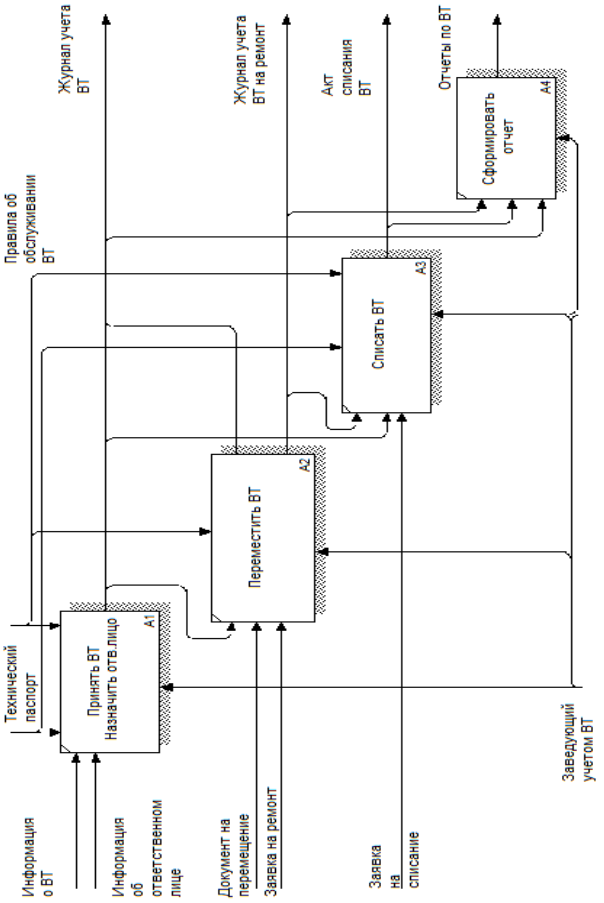


Рис. 1. SADT-модель

Для создания модели была использована компьютерная программа AllFusion Process Modeler r7, предназначенная для моделирования, анализа, документирования и оптимизации бизнес-процессов.

Входная информация: информация о вычислительной технике, информация об ответственном лице, документы на перемещение, заявки на ремонт, заявки на списание.

Выходная информация: журнал учета вычислительной техники, журнал учета вычислительной техники на ремонт, акты списания вычислительной техники, отчеты по вычислительной технике.

Учет вычислительной техники в отделе будет выполнять заведующий учетом.

Для данной предметной области были рассмотрены программы-аналоги:

1) IT Invent;
2) Hardware Inspector;
3) PrintStore.

В результате были изучены функциональные возможности данных программ, их стоимость, достоинства и недостатки.

Вывод: отталкиваясь от изученной информации об аналогах и поставленных требований к информационной системе, есть потребность в создании собственной информационной системы по учету. Главным недостатком программ-аналогов является их стоимость, а также не подробная информация о перемещениях вычислительной техники и текущем местоположении.

Автоматизации подлежит принятие вычислительной техники и назначение ответственного лица, перемещение вычислительной техники, списание вычислительной техники, формирование отчетов.

В качестве средств разработки были выбраны программа Microsoft Visual Studio, язык программирования C#, СУБД Microsoft SQL Server.

Заключение. Автоматизированные бизнес-процессы в информационной системе позволят отслеживать интересующую вычислительную технику и ответственных лиц в минимальные сроки, а также хранить структурированные упорядоченные данные.

ЛИТЕРАТУРА

1. Официальный сайт АО «СГМК» [Электронный ресурс]. – Режим доступа: https://www.sgmkgroup.ru/, свободный (дата обращения: 05.03.2023).

2. Золотов С.Ю. Проектирование информационных систем: учеб. пособие. – Томск: ТУСУР, 2016. – 117 с. [Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/publications/6478, свободный (дата обращения: 07.03.2023).

УДК 378.4; 004.912

ЭКОНОМИЧЕСКАЯ ВЫГОДА ИСПОЛЬЗОВАНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПРОВЕРКИ СТУДЕНЧЕСКИХ РАБОТ В ВУЗЕ

А.М. Аверьянова, К.Д. Глухих, студенты

Научный руководитель А.А. Захарова, проф. каф. АСУ, д.т.н.

г. Томск, ТУСУР, каф. АСУ, averjyanova-anna@mail.ru, ksenia2801@mail.ru

На сегодняшний день очень актуальным является процесс проверки различной документации на соответствие стандартам и установленным нормам, в связи с этим возникает проблема оптимизации данного процесса. Данная статья содержит информацию о потенциальных экономических выгодах, которые можно получить, используя автоматизированную информационную систему при проверке студенческих работ в университете.

Ключевые слова: нормоконтроль, автоматизированная информационная система, экономическая выгода.

Проверка документации на соответствие стандартам является обычной практикой практически во всех сферах деятельности. На официальном веб-сайте статистики доступен широкий спектр стандартов, включая 29 620 межгосударственных стандартов, 18 940 национальных стандартов и более 50 000 международных стандартов [1, 2].

Процесс нормоконтроля включает в себя оценку стиля и формата работы, чтобы убедиться, что она соответствует определённым стандартам, правилам или нормам, которые устанавливаются нормативными документами. Этот процесс направлен на повышение качества документации путем выявления и исправления любых несоответствий или ошибок.

Ответственность за проверку нормоконтроля лежит на нормоконтролере или лице, ответственном за оформление документации (например, преподавателе). Однако процесс проверки документации очень сложен и требует много времени и усилий.

Автоматизированная информационная система для проверки студенческих работ в университете – это программный инструмент, который может анализировать и оценивать студенческие работы по различным критериям, таким как проверка:

- стиля текста: шрифт, размер шрифта, цвет текста, выравнивание текста, межстрочный интервал, отступы и др.;
- оформления рисунков;
- оформления таблиц: границы, отступы и т.д.;
- нумерации страниц;
- формата сносок и др.

Данная система предназначена для оптимизации процесса выставления оценок, экономии времени и ресурсов, а также обеспечения справедливой и объективной оценки работы студентов. Автоматизированная система может использоваться в сочетании с человеческой сортировкой для повышения точности и надежности процесса проведения нормоконтроля.

Главным преимуществом использования автоматизированной информационной системы для проверки студенческих работ в вузе является экономическая выгода, это проявляется в некоторых аспектах:

1. Снижение затрат на рабочую силу. Одним из основных преимуществ использования автоматизированной информационной системы является то, что она может значительно снизить затраты на рабочую силу. Вместо того, чтобы требовать от нормоконтролера или преподавателя оценивать каждую работу, автоматизированная система может быстро сканировать и анализировать каждую работу, обеспечивая немедленную обратную связь и оценку.

2. Повышенная эффективность. Автоматизированная информационная система может повысить эффективность, обрабатывая документы намного быстрее, чем люди. Это может быть особенно полезно для нормоконтролеров с большим объемом работ для оценки, поскольку автоматизированная система может помочь сократить время и усилия, необходимые для оценки каждой работы.

3. Улучшенная согласованность. Автоматизированная система может помочь улучшить согласованность оценок, применяя согласованные правила и критерии к каждой работе. Это может помочь гарантировать, что все учащиеся будут оценены справедливо и точно, без возможности предвзятости или субъективной интерпретации.

4. Уменьшение количества ошибок. Автоматизированная система также может помочь уменьшить количество ошибок при оценке, устраняя ошибки, которые могут возникнуть из-за усталости, рассеянности или других человеческих факторов. Это может помочь гарантировать, что каждый студент получит точную и справедливую оценку своей работы.

В целом экономическая выгода от использования автоматизированной информационной системы для проверки студенческих работ заключается в том, что она может помочь снизить трудозатраты, повысить эффективность, обеспечить согласованность и уменьшить количество ошибок. Это может помочь сэкономить время и ресурсы, а также обеспечить более точную и справедливую оценку студенческой работы.

Подводя итог, стоит отметить, что проведение нормоконтроля имеет большое значение при проверке студенческих работ, а также

при проверке документов в различных сферах деятельности, и чтобы сократить время проверки и финансовые средства, необходимо создание автоматизированной информационной системы. Как только этап разработки автоматизированной информационной системы будет завершен, планируется протестировать систему и внедрить её на кафедру АСУ, а в дальнейшем на другие кафедры ТУСУРа. В долгосрочной перспективе планируется создать программный продукт, подходящий для различных сфер деятельности.

ЛИТЕРАТУРА

1. Стандарты и регламенты [Электронный ресурс]. – Режим доступа: https://www.rst.gov.ru/portal/gost/home/standarts, свободный (дата обращения: 02.03.2023).

2. Перечень стандартов ИСО [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Перечень_стандартов_ИСО#ISO_50001, свободный (дата обращения: 02.03.2023).

УДК 004.42: 374

АВТОМАТИЗАЦИЯ УЧЕТА СТАТИСТИКИ И ДОСТИЖЕНИЙ СПОРТСМЕНОВ МАУ ДО «ДЕТСКО-ЮНОШЕСКАЯ СПОРТИВНАЯ ШКОЛА № 17 Г. ТОМСКА»

В.П. Ловчановский, студент

Научный руководитель А.А. Захарова, проф. каф. АСУ, д.т.н.

г. Томск, ТУСУР, каф. АСУ, lovcha@vk.com

Описан бизнес-процесс деятельности МАУ ДО «Детско-юношеская спортивная школа № 17 г. Томска» по учету спортсменов и этапы его автоматизации.

Ключевые слова: спортсмены, статистика, информационная система, методология IDEF0, методология IDEF1x, SADT-модель, концептуальная модель.

Объектом исследования в данной работе является МАУ ДО «Детско-юношеская спортивная школа № 17 г. Томска», занимающаяся образовательной деятельностью по дополнительным общеразвивающим и предпрофессиональным программам в области физической культуры и спорта, а точнее в футболе. Основной задачей организации является подготовка спортсменов к переходу в профессиональные школы и команды.

Процесс подготовки спортсменов реализуется через тренировки, результатом которых является участие в соревнованиях различного уровня, а также возможный интерес профессиональных школ и ко-

манд к определенным спортсменам. При оценивании спортсмена учитываются его профессиональные навыки, командные и индивидуальные достижения, а также статистические показатели.

Руководство МАУ ДО «Детско-юношеская спортивная школа № 17 г. Томска» заинтересовано в автоматизации учета статистики и достижений спортсменов. Автоматизация данного процесса позволит увеличить скорость и улучшить качество оценивания навыков и результатов спортсменов, что позволит преподавательскому составу более своевременно принимать ключевые решения, а родителям отслеживать успехи своих детей. Также автоматизация данного процесса упростит процесс взаимосвязи с профессиональными футбольными школами и командами страны, которые нуждаются в качественных спортсменах.

В связи с закрытием центра подготовки футболистов «ЦПФ Томь», который являлся основным местом для развития футболистов в г. Томске, число спортсменов в МАУ ДО «Детско-юношеская спортивная школа № 17 г. Томска» сильно увеличилось.

На момент марта 2023 г. в спортивной школе занимается 17 групп разных возрастов, численность которых составляет от 10 до 23 спортсменов. Так как закрытие основного конкурента произошло относительно недавно, в ближайшее время ожидается приток спортсменов, оставшихся без школы для подготовки.

Для анализа процесса, требующего автоматизации, применялась методология IDEF0, в которой используется технология SADT (structured analysis and design technique), представляющая собой совокупность методов, правил и процедур, предназначенных для построения функциональной модели объекта какой-либо предметной области [1]. А также методология IDEF1x, которая используется для формирования графических представлений информационных моделей, которые отражают структуру и семантику информации внутри среды или системы [2].

После того как был проведен анализ автоматизируемого бизнес-процесса, были построены SADT-модель «As-Is» уровня A-0 и детализация A0 (рис. 1), а также концептуальные модели ER-, KB-, FA-уровней процесса учета статистики и достижений спортсменов.

Для визуализации моделей использовались такие программные продукты, как AllFusion Process Modeler r7 – инструмент для моделирования, анализа, документирования и оптимизации бизнес-процессов и CA ERWin Data Modeler – средство для проектирования баз данных.

Входная информация: данные спортсмена и тренера; данные о соревнованиях; результаты соревнований; факты посещения занятий; протоколы матчей.

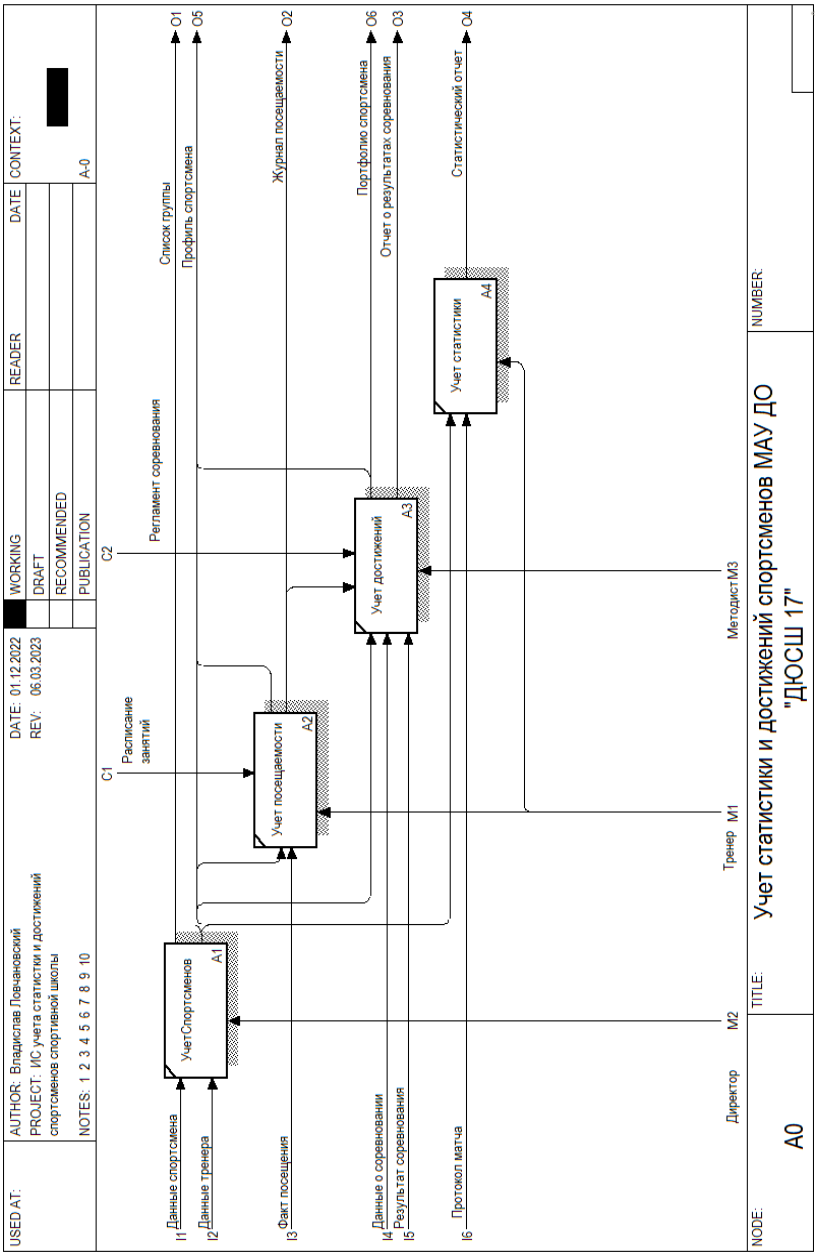


Рис. 1. SADT-модель «As-Is»

Выходная информация: списки групп; профили спортсменов; журналы посещаемости; портфолио спортсменов; статистические отчеты; отчеты о результатах соревнований.

Основными пользователями системы являются директор школы, тренеры и методист.

В ходе изучения предметной области были рассмотрены следующие программные продукты-аналоги: 1) «StatCrew» от CBS Sports Dgital [3]; 2) CRM-система «Отмечалка» от сервиса «Отмечалка»; 3) Сервис спортивной статистики «Flashscore» от компании Livesport Media Ltd и др. В результате анализа были выявлены их достоинства, выполняемые функции, платформы, стоимость и недостатки.

Автоматизации подлежат следующие действия: учёт статистики и достижений спортсменов, учет посещаемости занятий, формирование отчетов.

Для разработки ИС была выбрана СУБД PostgreSQL 15 и программная среда Microsoft Visual C# for Windows.

Заключение. Разработанная информационная система позволит ускорить и улучшить качество процесса анализа ключевых показателей спортсменов, а также упростит процесс связи между профессиональными спортивными школами и командами, нуждающимися в качественных спортсменах.

ЛИТЕРАТУРА

1. Золотов С.Ю. Проектирование информационных систем: учеб. пособие. – Томск: 2016. – 117 с. [Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/publications/6478 (дата обращения: 01.03.2022).

2. IDEF1X [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/IDEF1X (дата обращения: 06.03.2023).

3. Лучшее программное обеспечение для футбольной статистики – обзор [Электронный ресурс]. – Режим доступа: https://gadgetshelp.com//samosovershenstvovanie/luchshee-programmnoe-obespechenie-dlia-futbolnoi-statistiki-rukovodstvo-po-2020-godu/ (дата обращения: 06.03.2023).

УДК 681.518(075.8)

АВТОМАТИЗАЦИЯ УЧЕТА И КОНТРОЛЯ ПРОЕКТОВ IT-КОМПАНИИ В ИП «РЫЖКОВ Д.В.» Г. ТОМСКА

А.С. Мидуница, студент

Научный руководитель С.Ю. Золотов, доцент каф. АСУ, к.т.н.

г. Томск, ТУСУР, каф. АСУ, midanichka37@gmail.com

Описаны бизнес-процесс деятельности ИП «Рыжков Д.В.» г. Томска по учету заказов клиентов и этапы его автоматизации.

Ключевые слова: заказ, IT, IT-компания, автоматизация, медицинская информационная система, SADT-модель.

В роли объекта исследования в настоящей работе является IT-компания ИП «Рыжков Д.В.», сосредоточенная в области здравоохранения. Её основной деятельностью является внедрение и сопровождение медицинской информационной системы (МИС) «Медиалог», а также её настройка и доработка по запросу клиента.

Медицинская информационная система обеспечивает эффективную работу всех подразделений медицинской организации. Функционал МИС «Медиалог» позволяет настраивать отчёты, экранные формы, записывать пациентов, вести расписание врачей, вести электронную медицинскую карту и многое другое. В МИС отражается вся деятельность медицинской организации (МО) с её филиалами.

Среди инструментов компании также предлагаются клиентам:

– Ivoice: проектирование голосовых коммуникаций – платформа с голосовыми помощниками;

– Wazzup – сервис для интеграции мессенджеров (WhatsApp, Telegram, VK).

Для удовлетворения запроса клиента формулируется проект (глобальная задача) и назначается ответственное за его выполнение лицо. Проект подлежит декомпозиции на задачи, которые распределяются между сотрудниками в соответствии с их специализацией, чтобы оперативно удовлетворить потребности клиента. Для наглядности отображения задач по проектам используется канбан-доска.

Руководство и сотрудники IT-компании ИП «Рыжков Д.В.» проявили интерес к автоматизации учёта и контроля проектов. Данная автоматизация привлекательна не только для специалистов по работе с МИС и разработчиков, но и остальных сотрудников (менеджеров проектов, руководителей) компании, упрощает учёт и контроль своевременного выполнения не только проектов, но и других важных задач, а также позволяет осуществлять контроль деятельности сотрудников в рабочее время и отслеживать их продуктивность. Таким образом, решение обнаруженной проблемы является достаточно актуальным.

Вместе с ростом медицинских организаций, использующих МИС компании и желающих внедрить её в свою медицинскую организацию, увеличивается загруженность сотрудников, а именно количество проектов и задач, находящихся на различном этапе выполнения и подлежащих контролю со стороны сотрудников компании.

На февраль 2023 г. число внедрений МИС «Медиалог» свыше 1000 в крупных и средних медицинских организациях различных специализаций и профилей в России, а также 6 региональных внедрений МИС «Медиалог».

Для анализа процесса, требующего автоматизации, была использована методология SADT (Structured Analysis and Design Technique) –

набор методов, правил и процедур, определённых для построения функциональной модели объекта некоторой предметной области [1], формализующей и описывающей бизнес-процессы.

По итогам анализа полученных данных о совершенствуемом бизнес-процессе построена SADT-модель «As-Is» учёта и контроля проектов уровня A-0 и детализация A0 (рис. 1) в нотации графического моделирования IDEF0.

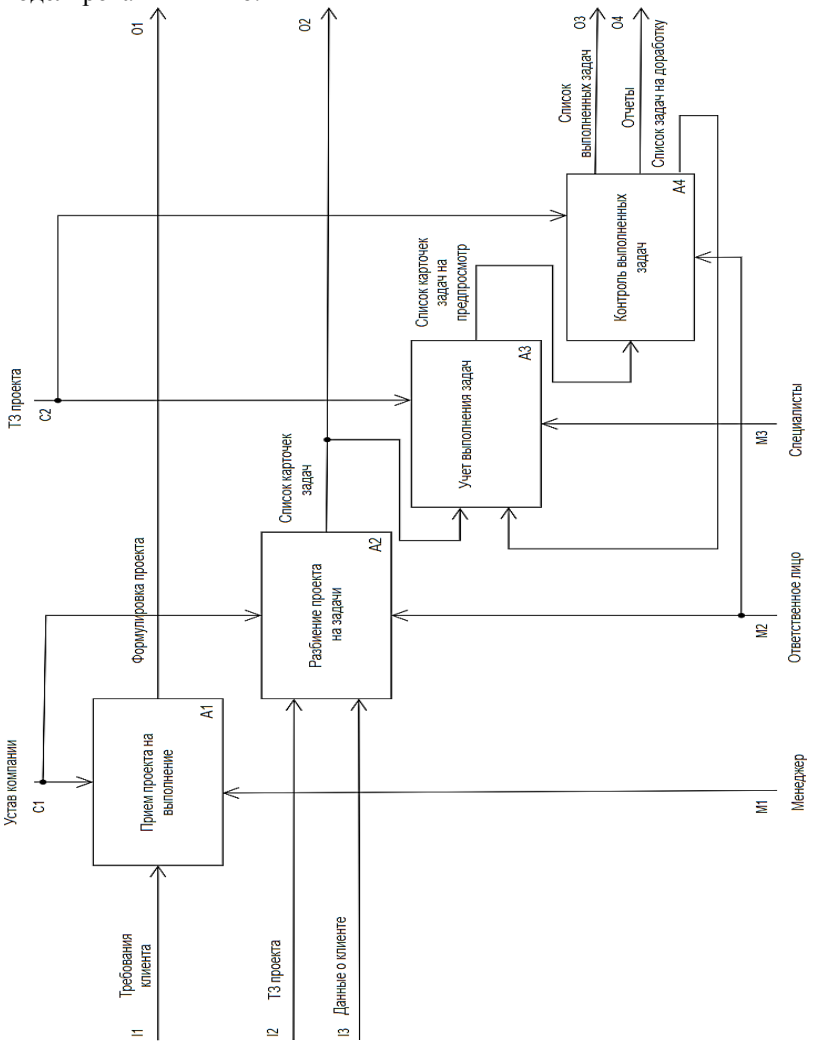


Рис. 1. SADT-модель «As-Is»

Для наглядного представления модели использовалось кросс-браузерное онлайн-приложение Diagrams.net, ориентированное на создание различных диаграмм (в том числе блок-схем).

В качестве входной информации использовались: требования клиента; техническое задание (ТЗ) проекта; данные о клиенте.

В качестве выходной информации использовались: формулировка проекта; список карточек задач; список выполненных задач; отчёты.

Работу по учёту и контролю проектов выполняют менеджер, ответственное (за проект) лицо и соответствующие специалисты.

Изучая способы решения вопроса в текущей предметной области, были рассмотрены и проанализированы информационные системы, созданные для автоматизации учёта и контроля выполнения проектов. Были изучены программные продукты, такие как: 1) таск-менеджер «WEEK»; 2) «Todoist»; 3) таск-менеджер «Asana» и др. [2]. Результатом анализа было выявление их достоинств и недостатков, выполняемых функций, платформ и стоимости.

Должны быть автоматизированы следующие действия: прием проекта на выполнение; разбиение проекта на задачи; учёт выполнения задач; контроль выполненных задач и проектов; формирование отчётов.

Осуществляя выбор средств разработки своей ИС, были рассмотрены следующие СУБД и программные редакторы кода: Microsoft SQL Server; HeidiSQL, MySQL, Visual Studio Code для Windows; Sublime Text 3. Для разработки информационной системы предпочтительными стали СУБД HeidiSQL и программа Visual Studio Code (язык программирования php).

Заключение. Информационная система сделает возможным использование структурированного подхода к выполнению проектов без потери важных аспектов, а также обеспечит учёт и контроль своевременного выполнения проектов и задач. Информационная система обеспечит обработку и хранение данных о проектах, их статусе и выполнении, суммах и сроках.

При защите будет представлено описание информационной системы учета и контроля проектов, ее функционала, а также интерфейс.

ЛИТЕРАТУРА

1. Золотов С.Ю. Проектирование информационных систем: учеб. пособие. – Томск, 2016. – 117 с. [Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/publications/6478 (дата обращения: 8.03.2023).

2. ТОП 20 таск-менеджеров для вашей команды [Электронный ресурс]. – Режим доступа: https://worksection.com/blog/task-managers-for-every-team.html (дата обращения: 08.03.2023).

УДК 681.518(075.8)

АВТОМАТИЗАЦИЯ УЧЁТА КЛИЕНТОВ ПРЕДПРИЯТИЯ ООО «ЭВЕРЕСТ КОНСАЛТИНГ ГРУПП» Г. САНКТ-ПЕТЕРБУРГА

А.И. Никифорова, студентка

Научный руководитель А.И. Исакова, доцент каф. АСУ, к.т.н.

г. Томск, ТУСУР, каф. АСУ, anyakef@yandex.ru

Описаны бизнес-процесс деятельности ООО «Эверест Консалтинг групп», г. Санкт-Петербурга по учёту клиентов предприятия и этапы его автоматизации.

Ключевые слова: клиент, информационная система, SADT-модель.

Объектом исследования в данной работе являются бизнес-процессы по учёту клиентов на предприятии ООО «Эверест Консалтинг групп». Предметом исследования выступает автоматизация учёта клиентов. Основным видом деятельности предприятия является оказание бухгалтерских и консалтинговых услуг, а именно: бухгалтерский консалтинг, ведение бухгалтерского и налогового учета, консультация по налоговым вопросам любой сложности.

Сегодня даже в случае наличия в штате бухгалтера услуга бухгалтерского консалтинга бывает нелишней. Во-первых, человек со стороны может проконтролировать работу штатного бухгалтера: заметит ошибки, подскажет, как оптимизировать процессы внутри бухгалтерии и повысить эффективность. Во-вторых, консультанты имеют опыт работы с разными сферами бизнеса. Организации, занимающиеся бухгалтерским консалтингом, обычно имеют существенный опыт и возможности для снижения налоговой нагрузки. Большой опыт достигается в силу постоянного контакта с фискальными органами, изучения судебных и налоговых споров и прецедентов, отслеживания постоянно меняющегося законодательства.

Руководство ООО «Эверест Консалтинг групп» заинтересовано в автоматизации учёта клиентов своего предприятия в формате программного продукта, который позволит облегчить работу сотрудникам компании и автоматизировать процесс ведения учёта информации о клиентах, договорах, оказанных услугах, а также платёжных поручениях.

Учитывая возраст предприятия, в последние годы количество новых клиентов увеличивается, а также растет количество информации, которая подлежит хранению и анализу.

По состоянию на январь 2022 г. число клиентов составило 8 предприятий (рис. 1).

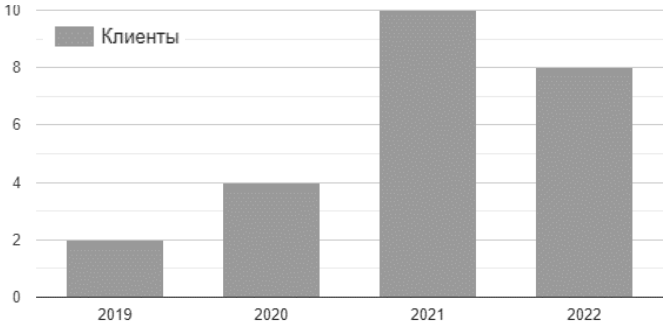


Рис. 1. Динамика количества клиентов в 2019–2022 гг.

Автоматизируемые процессы анализировались с помощью метода SADT (Structured Analysis and Design Technique) – набора методов, правил и процедур [1], предназначенных для построения функциональных моделей объектов любой предметной области, описывающих бизнес-процессы.

В результате анализа полученной информации об автоматизируемых бизнес-процессах была создана SADT-модель учёта клиентов компании «как есть» на уровне A-0, детализация A0 (рис. 2), в графической нотации IDEF0.

Используемое средство визуализации модели представляет собой программный продукт под названием BPWin, который относится к категории CASE-средств и ориентирован на ранние этапы построения, анализа и планирования информационных систем.

Входная информация: данные о клиенте, данные об ответственном лице клиента, заявка на услугу, доступ к 1С клиента.

Выходная информация: журнал клиентов, договор, отчёт о выполненных услугах, акт выполненных работ, журнал выполненных услуг, платёжное поручение, отчёт о платёжных поручениях.

Информационная система позволит хранить, изменять, просматривать и обрабатывать информацию о клиентах, контрактах и договорных услугах, отслеживать платежи и образование задолженностей.

Основным пользователем системы является менеджер, который будет отвечать за бухгалтерский учет и управление клиентами. Другие сотрудники компании, задействованные в бухгалтерии, также будут иметь доступ к системе.

Для ознакомления с темой были изучены информационные системы, направленные на автоматизацию учета клиентов. Исследовались следующие программные продукты: 1) Fillin, 2) 1С:Предприятие и 3) Контур. В результате были выявлены их основные особенности и преимущества, платформы, стоимость и недостатки.

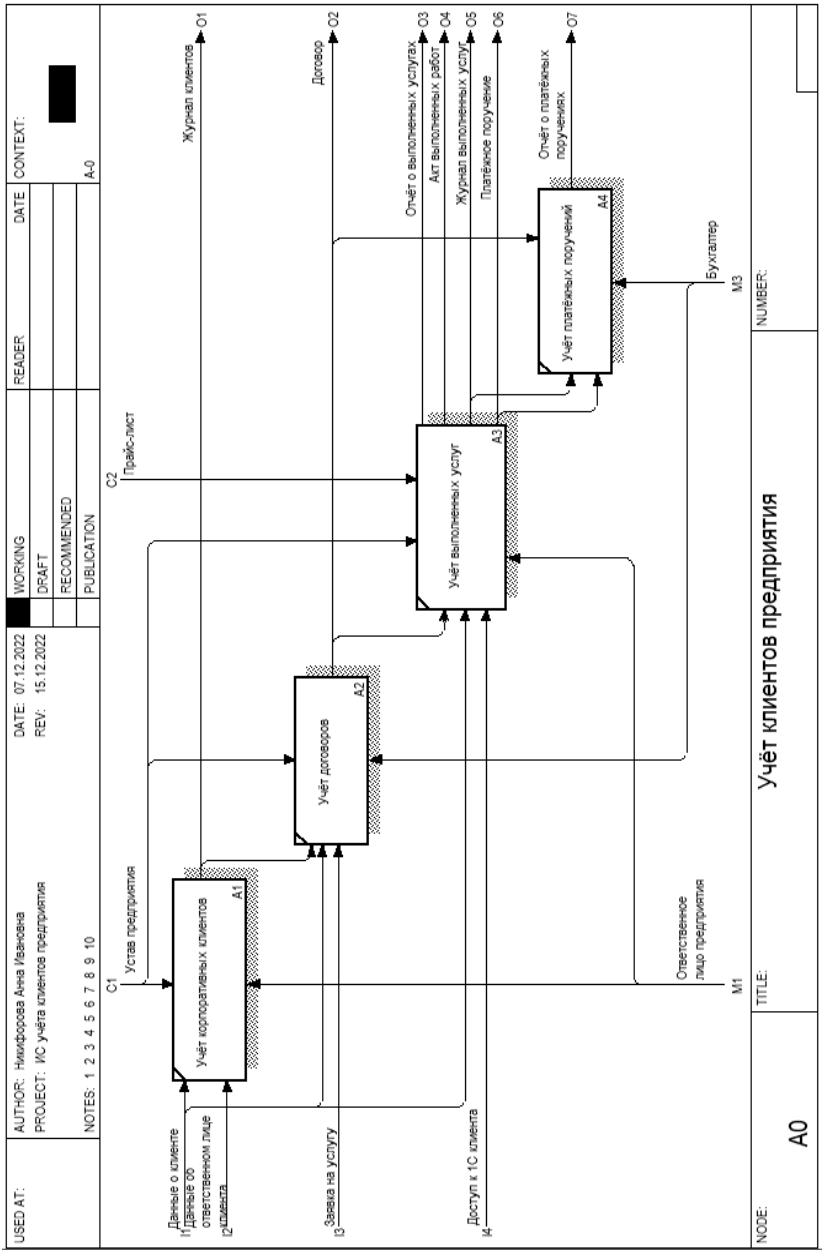


Рис 2. SADT-модель «As-Is»

Автоматизации подлежат следующие действия: учёт клиентов предприятия; учёт договоров и платежей по ним; контроль оплаты платежных поручений; учёт оказанных услуг по договору.

При выборе средств разработки для внутренней ИС рассматривались следующие СУБД: Microsoft SQL Server, Microsoft Access, Django, среда создания программного интерфейса: Microsoft Visual C# for Windows, React (JS); приоритетными были Django и React.

Заключение. Информационная система позволит оптимизировать процессы учёта клиентов в единой базе данных. Она разрешает отслеживать платежи и просроченную задолженность. Информационная система обеспечивает обработку и хранение данных о договорах, их статусе, выполнении ключевых обязательств, суммах и сроках.

ЛИТЕРАТУРА

1. Золотов С.Ю. Проектирование информационных систем: учеб. пособие. – Томск, 2016. – 117 с. [Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/publications/6478 (дата обращения: 12.03.2023).

УДК 004.42

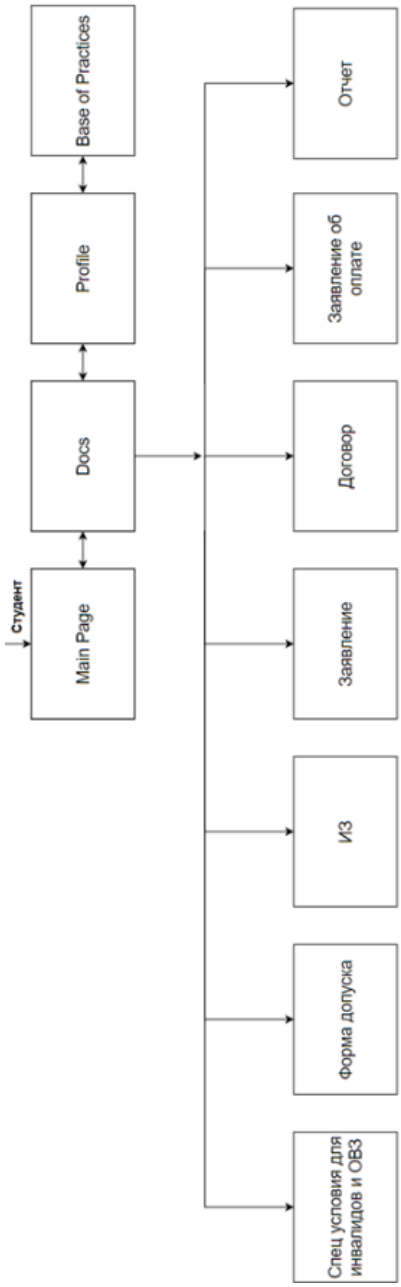
МАКЕТИРОВАНИЕ ИНТЕРФЕЙСА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДОКУМЕНТООБОРОТА ПО ПРАКТИКАМ ТУСУР

Д.С. Лисица, В.С. Завзятов, В.В. Прокудин, студенты
Научные руководители: М.В. Григорьева, доцент каф. АСУ.; А.А. Захарова, проф. каф. АСУ
г. Томск, ТУСУР, каф. АСУ, errlidie@gmail.com
Проект ГПО АСУ-2101. АИС стейкхолдеров кафедры

Рассматривается разработка макетов структуры веб-приложения «Информационная система организации документооборота по практике вуза».
Ключевые слова: стейкхолдеры, документооборот, практика, высшее учебное заведение, макет, интерфейс.

Информационная система документооборота по практикам представляет собой веб-приложение, автоматизирующее работу с соответствующими электронными документами на всех этапах прохождения студентом производственной практики.

Для того чтобы приступить к разработке клиентской части информационной системы взаимодействия вуза со стейкхолдерами, необходимо, во-первых, определиться со структурой веб-приложения, а во-вторых, построить макеты его отдельных страниц.



В системе находятся пользователи, у которых может быть одна из четырех ролей, а именно: студент, руководитель от вуза, секретарь, учебное управление – они обладают разными потребностями, поэтому необходимо отображать только соответствующую им информацию, которая в то же время должна иметь органичную структуру для создания унифицированного роутера страниц. Определим ряд основных страниц, которые будут отображаться у любой роли.

Стартовой частью структуры является страница авторизации и регистрации. Доступом к этой странице обладает только базовая роль – пользователь. После выполнения авторизации в системе пользователь получает доступ ко всем страницам и их содержимому.

Рассмотрим структуру страниц для роли «Студент». Она представлена на рис. 1.

Как видно из рис. 1, после аутентификации в системе пользователь будет автоматически перенаправлен на страницу Main Page, что показано с помощью стрелки над соответствующим блоком. На ней находится новостной блок, а также даты начала и окончания практики.

Рис. 1. Структура страниц, соответствующая роли «Студент»

Помимо Main Page, на том же уровне вложенности существуют еще три страницы: Docs (шаблоны и примеры заполнения документов, формы внесения данных), Profile (редактируемая информация о пользователе) и Base of Practices (список компаний с возможностью сортировки и фильтрации).

На основе вышеописанной структуры проведем макетирование, или прототипирование, веб-приложения. Прототипирование представляет собой создание макета или пробного варианта программы [1], в контексте данной работы остановимся на разработке макетов.

Макеты страниц представлены на рис. 2–4.

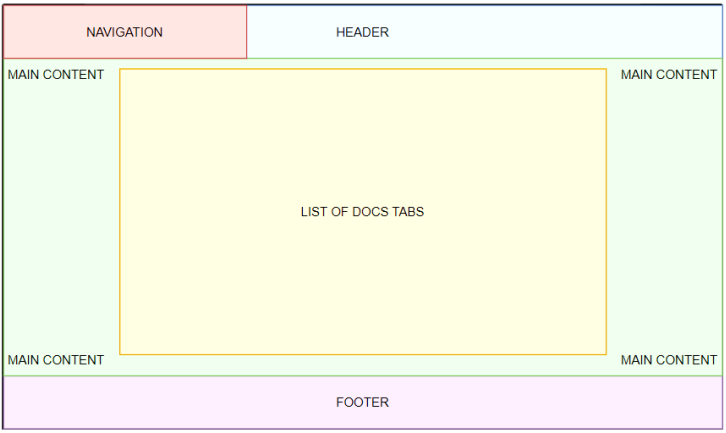


Рис. 2. Макет страницы Docs

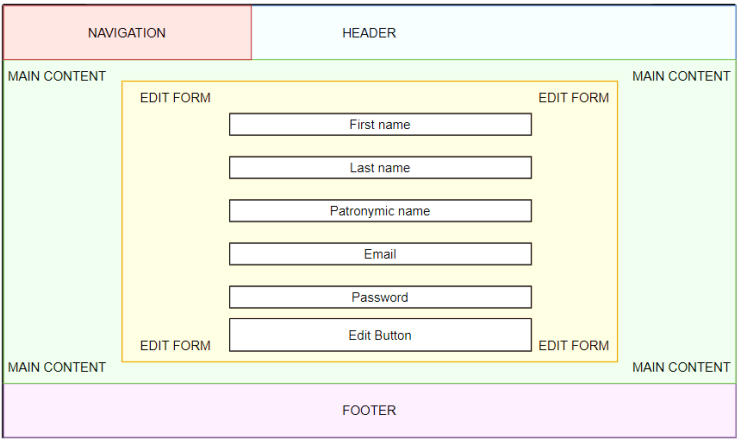


Рис. 3. Макет страницы Profile

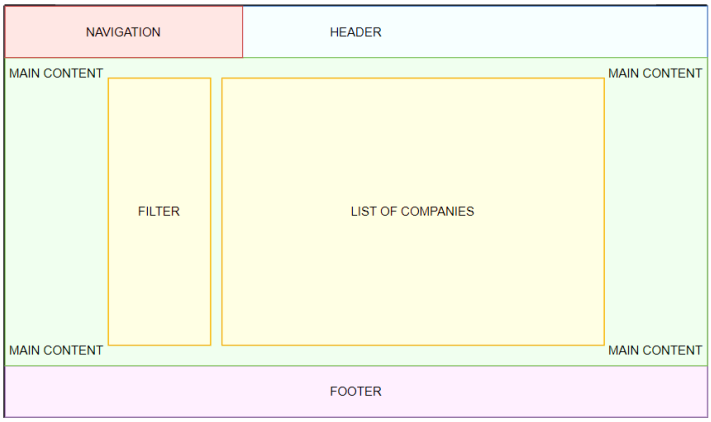


Рис. 4. Макет страницы Base of Practices

Разработанные прототипы в дальнейшем будут основой HTML-страниц и облегчат их разработку.

ЛИТЕРАТУРА

1. Шкляр Т. Разработка прототипа программного обеспечения [Электронный ресурс]: Образовательный портал «Справочник». – URL: https://spravochnick.ru/informatika/razrabotka_ prototipa_programmnogo_obespecheniya/ (дата обращения: 09.03.2023).

УДК 681.518**(075.8)**

АВТОМАТИЗАЦИЯ УЧЕТА, ОТСЛЕЖИВАНИЯ И КОНТРОЛЯ ПЕРСОНАЛА НА РАБОЧЕМ МЕСТЕ НА ОБЪЕКТАХ ФИЛИАЛА ООО «ГАЗПРОМ ИНВЕСТ «ТОМСК»

В.А. Викулин, студент каф. АСУ

Научный руководитель А.И. Исакова, доцент каф. АСУ, к.т.н.

г. Томск, ТУСУР, mrvlozar@mail.ru

Описан бизнес-процесс деятельности ООО «Газпром Инвест «Томск» по учету, отслеживанию и контролю персонала на рабочем месте и этапы его автоматизации.

Ключевые слова: информационная система, SADT-модель, контроль персонала, отслеживание персонала.

Объектом исследования в представленной работе является филиал компании «Газпром Инвест» – «Газпром Инвест «Томск». Данная организация является техническим заказчиком ПАО «Газпром» по

реализации инвестиционных проектов по геологоразведочным работам, строительству, реконструкции, капитальному ремонту объектов добычи, подземного хранения, переработки газа и объектов газификации.

Принимая во внимание статус ООО «Газпром Инвест» как заказчика при реализации объекта капитального строительства, необходимо строгое соблюдение от подрядных организаций требований промышленной безопасности и охраны труда.

На сегодняшний день отслеживание и контроль персонала происходит в режиме непосредственного визуального контроля специалистами охраны труда и промышленной безопасности (далее – ОТиПБ) на месте осуществления работ. Соотношение специалистов ОТиПБ и подконтрольных работников рассчитывается для каждого предприятия индивидуально и зависит от многих параметров, регламентируемых специальным приказом. Приведенный пример расчета в приказе показал, что на 8 специалистов ОТиПБ приходится 1100 работников [1].

Данное соотношение ввиду размеров и удаленности площадок не позволяет охватить и контролировать передвижение всех работников, что увеличивает риск несчастных случаев, технологических аварий и инцидентов. Таким образом необходимо свести к минимуму возникновение несчастных случаев на объектах строительства.

Программно-аппаратный комплекс отслеживания и контроля персонала (далее – ПАК ОиКП) позволит в режиме квазиреального времени отправлять сигнал на пульт специалиста ОТиПБ о возможных нарушениях режима работы сотрудников и нахождении их в опасных зонах без наличия соответствующего наряда-допуска.

Во время строительства необходимо учитывать указываемые в организационно-технической документации на строительное производство опасные зоны, в которых возможно воздействие опасных производственных факторов, связанных или не связанных с характером, особенностями выполняемых работ и их технологиями.

Зоны с постоянным присутствием опасных производственных факторов должны иметь защитные ограждения, а зоны, на которых возможны опасные производственные факторы, должны иметь сигнальные ограждения и знаки опасности. При реализации ПАК ОиКП опасные зоны будут отражены на пульте специалиста ОТиПБ и при пересечении охранной зоны система будет сигнализировать о нарушении, ПАК ОиКП служит в качестве дополнительной контрольной составляющей помимо стандартов по производственной безопасности.

Для анализа процесса создания информационной системы учета, отслеживания и контроля персонала на рабочем месте использовалась методология SADT (Structured Analysis and Design Technique) – набор

методов, правил и процедур, упрощающих создание функциональной модели объекта в любой предметной области. Этот процесс стандартизирует и объясняет бизнес-процессы [2].

Анализ модернизированного бизнес-процесса завершился построением SADT-моделей «As-Is» учета, отслеживания и контроля персонала на рабочем месте уровня А-0 и детализации А0 (рис. 1) с использованием графической нотации IDEF0.

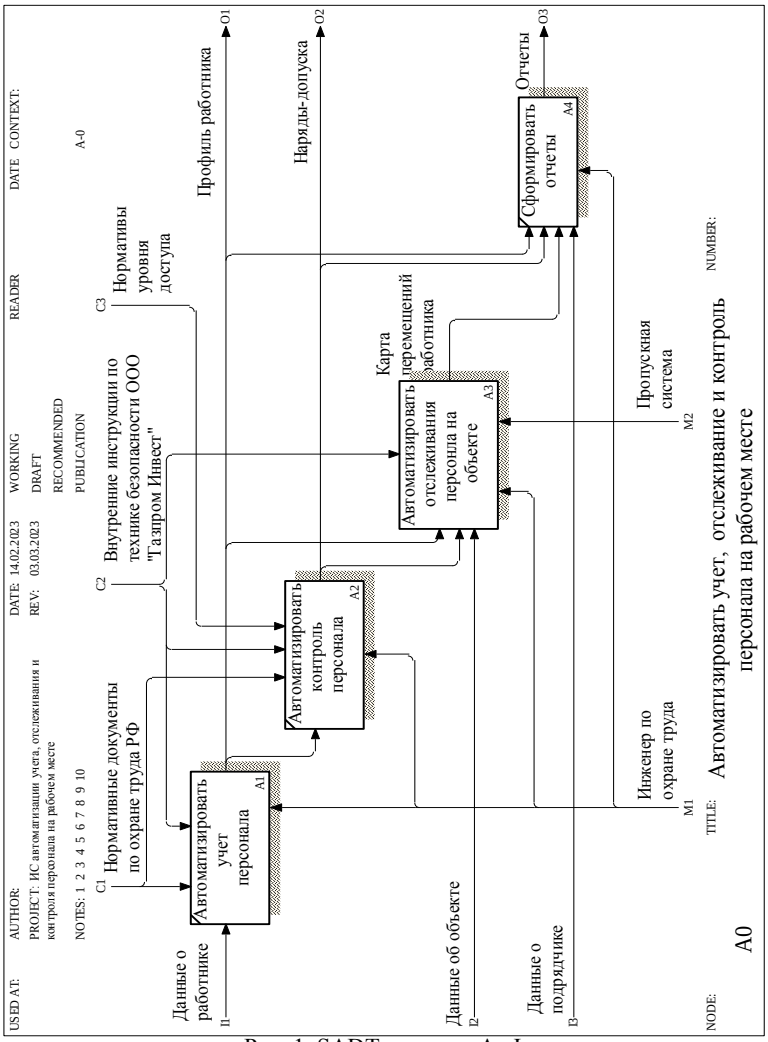


Рис. 1. SADT-модель «As-Is»

Для визуализации модели было выбрано CASE-средство – программный продукт BPWin, предназначенный для начальных этапов проектирования построения информационных систем, связанных с анализом и планированием.

Входная информация: данные о работнике; данные об объекте; данные о подрядчике.

Выходная информация: профиль работника; наряды-допуска; отчеты.

Пользователем системы является инженер по охране труда, также доступ к системе будет иметь вышестоящее руководство, а вспомогательным механизмом является пропускная система.

Для изучения предметной области были рассмотрены, проанализированы и изучены присутствующие на рынке аналоги информационных систем учета, отслеживания и контроля сотрудников на рабочем месте: 1) Navigine; 2) RealTrac; 3) My-Beacon.

Автоматизация бизнес-процесса предполагает учет персонала, контроль персонала, отслеживание персонала на объекте и формирование отчетов.

При выборе средств разработки информационной системы были рассмотрены следующие системы управления базами данных и среды разработки программного обеспечения: 1) Microsoft SQL Server; 2) Microsoft Access; 3) Delphi; 4) Microsoft Visual C#. Предпочтение было отдано СУБД Microsoft Access и Microsoft Visual C#.

В заключение следует отметить, что предлагаемая информационная система обеспечит учет, отслеживание и контроль персонала на рабочем месте, тем самым сведя к минимуму возможные нарушения техники безопасности.

ЛИТЕРАТУРА

1. Министерство труда и Российской Федерации. Приказ от 31 января 2022 года № 37 «Об утверждений Рекомендаций по структуре службы охраны труда в организации и по численности работников службы охраны труда» [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/728094912 (дата обращения: 27.02.2023).

2. Золотов С.Ю. Проектирование информационных систем: учеб. пособие. – Томск: ТУСУР, 2016. – 117 с. [Электронный ресурс]. – Режим доступа: https://edu.tusur.ru/publications/6478 (дата обращения: 24.02.2023).

УДК 681.518

АВТОМАТИЗАЦИЯ ЗАПОЛНЕНИЯ ШАБЛОНОВ ДЛЯ СТРЕСС-ТЕСТИРОВАНИЯ БАНКОВ

С.В. Яранцев, студент каф. АСУ
Научный руководитель С.Ю. Золотов, доцент каф. АСУ, к.т.н.
г. Томск, ТУСУР, seryaga228@gmail.com

Рассматриваются важность составления суперсета данных, необходимых для проведения стресс-тестирования, и проблемы, возникающие при его составлении.
Ключевые слова: стресс-тестирование, суперсет, Python.

Стресс-тестирование – это оценка потенциального воздействия на финансовое состояние кредитной организации ряда заданных изменений, которые соответствуют потенциально возможным событиям. Как правило, стресс-тесты измеряют устойчивость банков к гипотетическим неблагоприятным сценариям, таким как серьезные рецессии, а результаты используются центральными банками и регулирующими органами для измерения рисков и управления ими посредством пруденциальной политики. Также стресс-тестирование позволяет определить слабые стороны политики банка, установить процентные ставки на свои продукты и в целом корректировать политику банка для поддержания стабильной работы [1].

Использование и известность банковских стресс-тестов значительно возросли в годы, последовавшие за мировым финансовым кризисом. В настоящее время они являются ключевой частью инструментария банковского регулирования. Многие банки в разных странах проводят свое стресс-тестирование, из-за чего возникает большое разнообразие наборов переменных, которые необходимо вычислять во время стресс-тестирования. И, с одной стороны, это разнообразие тестов обосновано «национальными особенностями» различных стран (например, в Европейском союзе большую ликвидность показывают автокредиты, что позволяет отнести их к высококачественным ликвидным активам, в США же автокредиты не обладают для этого должным уровнем ликвидности), с другой стороны, некоторые банки в принципе используют различные переменные, исходя из собственных стандартов [2]. Это разнообразие вызывает множество проблем, связанных с обладанием различными активами и объективной оценкой устойчивости банков к различного рода кризисам.

Все эти проблемы возможно решить с помощью глобального проекта составления суперсета, содержащего все возможные наборы переменных. Стоит учитывать многообразие источников фреймвор-

ков, проводить анализ каждого из них и выделять различия и соответствия, чтобы в суперсете не возникало повторений. Но основной сложностью, с которой мы вынуждены столкнуться при создании суперсета, конечно, является большой объем обрабатываемых данных. Все данные, находящиеся в различных отчетных документах (таких как ипотечная или корпоративная книга), необходимо обработать и записать в нужные шаблоны для дальнейшей работы с ними. Этот процесс зачастую проводится вручную либо с минимальной автоматизацией, из-за чего он требует больших временных затрат. Именно эту проблему обработки данных необходимо решить в первую очередь при составлении суперсета.

Для ее решения необходимо создать систему автоматической обработки данных и заполнения нужных шаблонов. Система разрабатывается на языке программирования Python 3.9 с использованием библиотеки pandas, с помощью которой удобно работать с фреймворками. Для программной реализации решения выявленной проблемы используется интерактивная вычислительная платформа Jupyter Notebook. Для хранения всех данных используется Microsoft Excel.

Заключение. С помощью разрабатываемого программного продукта значительно уменьшатся временные затраты на обработку необходимой информации и ее расчеты; появится централизованная система для проведения стресс-тестирования банков; повысится надежность многих кредитных учреждений. Также дальнейшее развитие стресс-тестов позволит лучше изучить то, как различные кризисные ситуации влияют на финансовую систему и передаются по ней между элементами.

ЛИТЕРАТУРА

1. Stress testing [Электронный ресурс]. – Режим доступа: https://www.bankofengland.co.uk/stress-testing (дата обращения: 2.03.2023).

2. Liquidity Coverage Requirement Delegated Act: Frequently Asked Questions [Электронный ресурс]. – Режим доступа: https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_14_579 (дата обращения: 15.02.2023).

УДК 004.42:374

СРЕДСТВА РАЗРАБОТКИ САЙТА ОНЛАЙН-МАГАЗИНА «ЧАЙКА»

С.С. Тырышкин, А.А. Сеньков, студенты каф. АСУ
Научный руководитель А.А. Захарова, проф. каф. АСУ
г. Томск, ТУСУР, email: robert.lewan@yandex.ru

Разработка онлайн-магазина является актуальной задачей, так как позволяет любому человеку заказать необходимые товары, не выходя из дома. В статье проведено обоснование выбора средств для разработки программного обеспечения онлайн-магазина «Чайка».
Ключевые слова: сайт, онлайн-магазин, личный кабинет, веб-клиент, стек технологий

Задача состоит в том, чтобы разработать сайт (онлайн-магазин) с целью расширить функционал магазина «Чайка» и предоставить покупателям возможность заказа товаров через онлайн-магазин, не выходя из дома. На данный момент, по статистике, треть населения РФ предпочитает онлайн-доставку самостоятельному походу в магазин.

Разработка собственного сайта с доставкой является более удобным решением, так как в этом случае все заказы поступают непосредственно в сам магазин, а не идут через сайт или приложение посредника.

Пользователями программного продукта являются покупатели и администраторы магазина «Чайка». Основными функциями программного продукта со стороны покупателя являются: добавление товаров в корзину, оформление заказа, выбор способа доставки (доставка курьером, самовывоз), выбор способа оплаты (на сайте через банковскую карту, наличными курьеру). Со стороны администратора: получение заказов для их выполнения, добавление нового товара и редактирование уже имеющихся.

Для начала рассмотрим личный кабинет покупателя на сайте онлайн-магазина.

Чтобы обеспечить комфорт покупателя при использовании онлайн-магазина, необходимо разработать современный и удобный интерфейс, который должен отвечать всем запросам покупателя.

Для того чтобы пользователь смог воспользоваться личным кабинетом, ему необходимо для начала зарегистрироваться, а затем авторизироваться на сайте. Личный кабинет позволит запомнить адрес доставки, телефон и другие данные пользователя, чтобы при следующем заказе ему не нужно было вводить все данные заново. Также в личном кабинете покупателя будет находиться корзина, куда будут

складываться все товары, которые необходимо приобрести покупателю. В самой же корзине покупатель сможет оформить заказ.

Теперь рассмотрим личный кабинет администратора магазина на сайте.

Чтобы обеспечить простоту работы администратору магазина при использовании онлайн-магазина, также необходимо разработать современный и удобный интерфейс, который должен отвечать всем нуждам администратора.

Для того чтобы пользователь смог воспользоваться личным кабинетом администратора, ему необходимо авторизироваться на сайте при помощи логина и пароля, которые были сгенерированы заранее администратором сайта. После авторизации в личном кабинете отобразится адрес магазина, список актуальных заказов и панель управления ассортиментом товаров и совершенных заказов, откуда и ведется управление онлайн-магазином.

Рассмотрим средства разработки сайта онлайн-магазина с точки зрения внешнего представления.

Для разработки сайта необходимо выбрать наиболее подходящий стек технологий и провести анализ имеющихся решений.

Для реализации был выбран язык Python, чтобы пользователю было удобно ориентироваться на сайте. Также были выбраны язык JavaScript как язык сценариев для придания интерактивности, язык гипертекстовой разметки HTML и язык описания таблиц стилей CSS. Помимо языков, также были использованы фреймворк Flask и СУБД PostgreSQL. Фреймворк – программная платформа, облегчающая разработку и объединяющая разные компоненты программного проекта.

Python – язык программирования, который на данный момент является одним из лучших языков для разработки веб-клиента. Python позволяет повысить производительность сайта, поскольку код выполняется на сервере, а не в браузере. Поскольку Python подразумевает общую внутреннюю логику, следовательно, код выполняется на сервере, а не в браузере, что довольно значительно повышает производительность сайта [1].

Flask – это библиотека языка Python, с помощью которой разработчик может создать прочную основу веб-приложения, позволяющую использовать любое расширение [2].

Главными особенностями Flask являются: обработка HTTP-запросов, встроенный быстрый отладчик, встроенный сервер разработки.

JavaScript – язык программирования, который используется как встраиваемый язык для программного доступа к объектам приложе-

ний, а также для придания интерактивности веб-страницам. По сути, весь динамически обновляемый контент в веб-среде доступен именно благодаря JavaScript [3].

HTML (HyperText Markup Language) – это стандартизированный язык разметки документов в интернет-пространстве. Он определяет содержание и структуру веб-контента. HTML использует разметку для отображения различных заголовков, текстовых абзацев, изображений и прочего контента в веб-браузере.

CSS (Cascading Style Sheets) – это язык, который позволяет изменить оформление внешнего вида документа отдельно от его содержания.

PostgreSQL – российская СУБД, представляющая собой глубоко переработанную редакцию СУБД PostgreSQL. Около 20% кода и документации этой СУБД написано или модифицировано компанией Postgres Pro [4].

В качестве основного языка разработки был выбран Python, так как на данный момент он является одним из самых простых и эффективных в разработке веб-приложений. Также была выбрана библиотека Flask, которая является легко адаптируемым фреймворком, что позволит ускорить процесс разработки.

Также для реализации был выбран язык HTML – для разметки страниц веб-приложения, и CSS – для изменения внешнего вида страниц.

ЛИТЕРАТУРА

1. Python [Электронный ресурс]. – URL: https://digitrain.ru/articles/30903/, свободный (дата обращения: 01.03.2023).

2. Flask [Электронный ресурс]. – URL: https://medium.com/featurepreneur/introduction-to-micro-web-framework-flask-78de9289270b, свободный (дата обращения: 01.03.2023).

3. JavaScript [Электронный ресурс]. – URL: https://developer.mozilla.org/en-US/docs/Web/JavaScript, свободный (дата обращения: 01.03.2023).

4. PostgreSQL [Электронный ресурс]. – URL: https://postgrespro.ru/, свободный (дата обращения: 04.03.2023).

ПОДСЕКЦИЯ 5.3

РЕАЛИЗАЦИЯ СОВРЕМЕННЫХ ЭКОНОМИЧЕСКИХ ПОДХОДОВ В ФИНАНСОВОЙ И ИНВЕСТИЦИОННОЙ СФЕРАХ

*Председатель секции – **Васильковская Н.Б.**, доцент каф. экономики, к.э.н.;*
*зам. председателя – **Цибульникова В.Ю.**, зав. каф. экономики, к.э.н.*

УДК 336.63

ОСОБЕННОСТИ УПРАВЛЕНИЯ ПРЕДПРИНИМАТЕЛЬСКИМ РИСКОМ В XXI ВЕКЕ

П.А. Адаменко, аспирант каф. экономики
Научный руководитель В.Ю. Цибульникова, зав. каф. экономики, к.э.н., доцент
г. Томск, ТУСУР, adamenko.car@gmail.com

Цель исследования – выделение и описание характерных особенностей предпринимательского риска в XXI в. Рассмотрены группы и виды рисков. Научная новизна работы заключается в определении-группировок управления рисками, а также системы анализа, которая включает в себя оценку и анализ рисков в период COVID-19. Предложены этапы работы с предпринимательскими рисками.
Ключевые слова: предпринимательский риск, виды предпринимательского риска, индивидуальный предприниматель, управление риском.

Предпринимательский риск – это вероятность неполучения запланированного или ожидаемого положительного результата, равно как и возможность получения отрицательных последствий тех или иных действий, в чем бы они ни состояли [1]. Предпринимательский риск может быть рассмотрен с положительной и отрицательной стороны. На практике под «риском» предприниматели чаще понимают убытки и непредвиденные ситуации, которые неблагоприятно отражаются на деятельности компании и порой бывают губительны в определенных условиях.

Целью управления предпринимательским риском является снижение негативного влияния риска на деятельность компании.

Процесс управления рисками в малом бизнесе в основном включает анализ всех факторов, создающих внешнюю и внутреннюю среду бизнеса, определение приемлемых зон риска для предприятия и выбор методов минимизации последствий рисков [2].

Исследовав виды предпринимательского риска, их можно разделить на две группы: внешние и внутренние. На внешние риски предприниматель повлиять не может, в отличие от внутренних, так как последствия будут напрямую связаны от принятия тех или иных решений предпринимателем.

К внешним видам предпринимательского риска относятся политические, законодательные, природные, макроэкономические. К внутренним видам предпринимательского риска относятся производственные, коммерческие, финансовые, кадровые.

Один из внешних рисков, который появился неожиданно, был связан с массовым заражением заболеванием COVID-19. Всего за несколько месяцев он распространился до мирового уровня [3]. Более крупные компании смогли пережить этот период за счет достаточного финансирования, запаса прочности, а также лучшей системы управления рисками. Малые компании намного болезненней перенесли период с 2019 по 2021 г. [4]. Наиболее трудный период для малого бизнеса пришелся на активную фазу кризиса в 2020 г. В этот период новые компании стали регистрироваться на 25,1% реже, в то время как количество закрытий увеличилось на 29,5%. В 2021 г. после окончания активной фазы ситуация стабилизировалась, риски стали ниже, и компании начали чаще открываться и реже закрываться. На рис. 1 рассмотрим диаграмму открытия и закрытия индивидуальных предпринимателей в данный период.

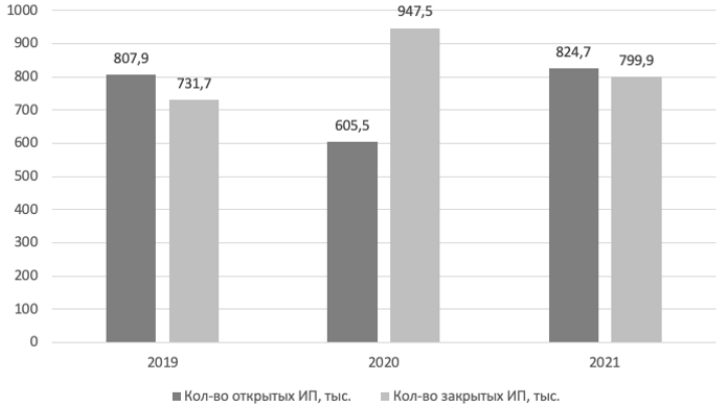


Рис. 1. Количество открытых и закрытых ИП по годам, тыс.

Таким образом, наблюдается, что индивидуальные предприниматели хотели зарабатывать и открывали бизнес, но, к сожалению, из-за недостатка ресурсов для изучения вопросов оценки риска и подготовки к нему, как только наступил риск, многие закрылись. Они оказались не в состоянии оптимизировать бизнес-процессы под новые реалии. После стабилизации риска открытие ИП снова возросло и в данный момент находится в состоянии роста. Данные факты свидетельствуют о том, что малый бизнес сейчас может развиваться только на рынке с минимальным риском в связи с малой подготовленностью к рисковым ситуациям.

При своевременном реагировании и анализе риска предприниматель может снизить вероятность его наступления. Важной задачей предпринимателя является не уклонение от риска, а объективное, обоснованное решение принятия мер по его снижению. В зависимости от той или иной стратегии принятия или уклонения от риска на рис. 2 предлагаются этапы в работе системы анализа и управления рисками.

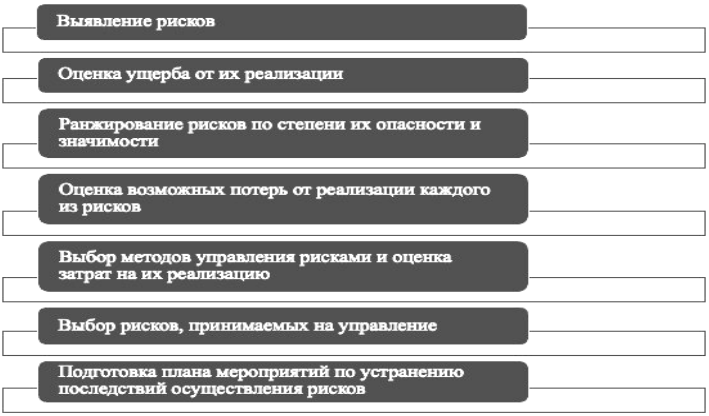


Рис. 2. Этапы работы системы анализа и управления рисками

Для стабильного и нормального развития малых и средних бизнесов, несомненно, следует рассматривать и готовиться к рискам. Вовремя принятый и оцененный риск может сохранить жизнеспособность компании. В период болезни COVID-19 риск стал мировым, и практически ни у кого не было возможности уклонения от риска, тем, кто не смог его принять и провести мероприятия по устранению риска, пришлось закрыться.

ЛИТЕРАТУРА

1. Олейник О.М. Предпринимательское (хозяйственное) право. – М.: Юрист, 1999. – 25 с.

2. Особенности управления рисками в малом бизнесе [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/osobennosti-upravleniya-riskami-v-malom-biznese, свободный (дата обращения: 26.02.2023).

3. История вируса: когда люди начали болеть COVID-19 [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/opinions/society/30/03/2020/5e7dbfa79a7947b91d218143,свободный (дата обращения: 9.03.2023).

4. Статистика по государственной регистрации [Электронный ресурс]. – Режим доступа: https://www.nalog.gov.ru/rn77/related_activities/statistics_and_analytics/regstats/, свободный (дата обращения: 9.03.2023).

УДК 336.77

АНАЛИЗ БАНКОВСКИХ ПРОДУКТОВ ДЛЯ ПРЕДПРИЯТИЙ МАЛОГО И СРЕДНЕГО БИЗНЕСА В СИБИРСКОМ ФЕДЕРАЛЬНОМ ОКРУГЕ И ТОМСКОЙ ОБЛАСТИ

В.В. Баладурина, студентка каф. экономики

Научный руководитель А.Д. Извекова, доцент каф. экономики, к.э.н.

г. Томск, ТУСУР, vika.baladurina@mail.ru, anna.d.izvekova@tusur.ru

Приведен сравнительный анализ условий кредитования банками субъектов малого и среднего бизнеса (МСБ) в г. Томске. Рассмотрены объемы кредитования и факторинга для предприятий МСБ за период 2021–2022 гг. в Сибирском федеральном округе.

Ключевые слова: кредитные продукты, малый и средний бизнес, кредит, факторинг.

Малый и средний бизнес (МСБ) в настоящее время является одним из важнейших способов ведения предпринимательской деятельности. Так, например, на 2022 г. количество занятых в данном секторе составляло 22 млн чел., а на долю субъектов МСБ приходилось около 39% общего оборота бизнеса по России [1]. Однако на определенных этапах своей деятельности (создание бизнеса, развитие, сохранение) предприятия МСБ могут испытывать недостаток собственных средств, и тогда у них возникает потребность в привлечении средств извне. Как правило, это банковские кредитные продукты, предоставляющиеся на самые разные цели.

Рассмотрим численность субъектов малого и среднего бизнеса в Томске и Томской области за 2020–2023 гг. Данные представлены на рис. 1 [2].

Согласно данным рис. 1, можно сделать следующий вывод: за рассматриваемый период (2020–2023 гг.) численность субъектов малых и средних предприятий Томской области ежегодно снижалась. Изменения в численности предприятий не критичные, однако если

сравнивать количество предприятий (малых+средних+микро) на начало
2020 г. (42 128) и на начало 2023 г. (39 111), то можно заметить, что оно изменилось, а именно уменьшилось на 3 017. Несомненно, на сокращение численности субъектов малого и среднего бизнеса влияет множество факторов, эпидемии (в частности, коронавирусная инфекция), политическая обстановка (санкции, ограничения, закрытие границ), платежеспособность населения, конкуренция и т.п. Однако, как уже говорилось ранее, одна из достаточно серьезных причин сокращения численности малых и средних предприятий – отсутствие финансирования. Данная проблема решается с помощью банков.

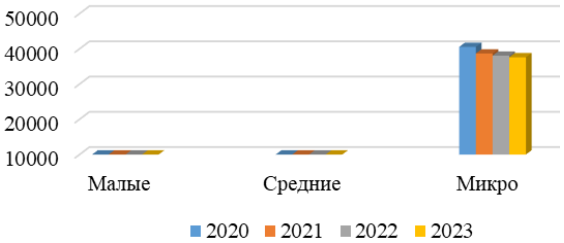


Рис. 1. Численность субъектов МСБ в Томской области за 2020–2023 гг., ед.

Существует разнообразное множество способов и форм финансирования субъектов МСБ, например, непосредственно кредит, факторинг, лизинг и т.п.

Рассмотрим более подробно такие кредитные продукты, как кредит и факторинг в банках г. Томска, а именно в Сбербанке, ВТБ-банке и Альфа-банке. Для рассмотрения были выбраны именно эти три банка, так как, согласно информации с сайта BankTOP.ru (рейтинг банков Томска), они находятся в топ-4 по размеру активов, исходя из чего можно судить о надежности данных банков.

Дадим определения понятиям «кредит» и «факторинг». Кредит – это предоставление банком клиенту денежных средств в долг на условиях возвратности [3]. Факторинг – финансовый инструмент, позволяющий клиенту покупать товар (услугу) с отсрочкой платежа [4].

После рассмотрения и сравнения условий предоставления кредита и оформления факторинга для предприятий малого и среднего бизнеса в разных банках г. Томска были сделаны следующие выводы [5–7].

Одним из наиболее выгодных банков (согласно анализу общедоступной информации, размещенной на официальном сайте) для предприятий малого и среднего бизнеса при оформлении кредита можно назвать ВТБ-банк. Требования к заемщику у данного банка (в сравне-

нии со Сбербанком и Альфа-банком) достаточно просты. Кроме того, наиболее выгодная процентная ставка (по состоянию на февраль 2023 г.) предлагается именно банком ВТБ (от 13,5 до 14% годовых).

Стоит отметить, что у каждого банка есть свои преимущества и недостатки, нельзя с точностью сказать, в каком банке предприятию будет выгодно кредитоваться, это могут решить лишь непосредственно представители малого и среднего бизнеса.

Сравнивая условия финансового инструмента – факторинг для малого и среднего бизнеса в банках Томска, а именно в Сбербанке, ВТБ-банке и Альфа-банке, стоит отметить следующее: в каждом из трех банков услуги факторинга предоставляются как поставщикам, так и покупателям. Конечно для каждой категории банк предлагает свои условия.

После изучения информации, размещенной на официальных сайтах банков (Сбербанк, ВТБ-банк и Альфа-банк), можно сказать, что одним из наиболее выгодных банков при оформлении факторинга как для поставщиков, так и для покупателей является ВТБ-банк, в сравнении с другими банками он предлагает наиболее выгодные условия, например, лимит без ограничений и отсрочка 365 дней, а также 100%-е финансирование. В других банках есть ограничения по сумме лимита, а также по отсрочке (у других банков по дням отсрочка меньше).

Таким образом, факторинг каждого банка отличается своими условиями, поэтому предприятиям МСБ нужно подробно их изучить и выбрать для себя тот банк и тот вид финансирования, который им наиболее подходит.

Рассмотрев условия двух кредитных продуктов – кредит и факторинг в трех разных банках г. Томска и Томской области, рассмотрим, чем предприятия малого и среднего бизнеса Сибирского федерального округа пользуются чаще. Данные представлены на рис. 2 [8–10].

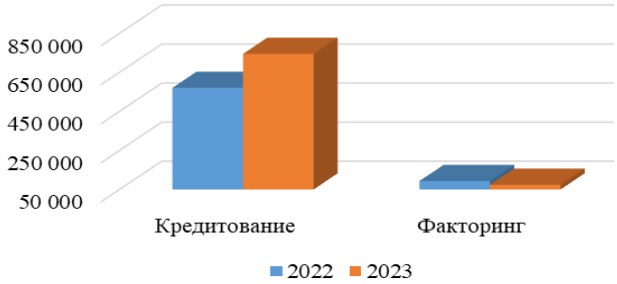


Рис. 2. Размер задолженности по кредиту и факторингу предприятий МСБ в Сибирском федеральном округе на 01.01.2022–01.01.2023, млн руб.

Согласно рис. 2, можно сделать следующий вывод, за рассматриваемый период размер задолженности по кредитованию увеличился на 173 791 млн. руб., величина задолженности по факторингу наоборот, уменьшилась на 19 202,3 млн. руб. Отсюда можно сделать вывод, что несмотря на рост популярности такого финансового инструмента, как факторинг, предприятия малого и среднего бизнеса пока отдают предпочтение такому кредитному продукту, как кредит. Однако это может быть связано также с тем, что не всем предприятиям малого и среднего бизнеса банки одобряют факторинг. Например, факторинг не могут оформить компании, имеющие большую дебиторскую задолженность, компании, поставляющие товары, требующие дальнейшего обслуживания, компании, продающие товары физическим лицам, а также бюджетные организации не могут оформить факторинг в банках.

Подводя итог всему вышесказанному, стоит отметить то, что количество предприятий малого и среднего бизнеса Томской области, ежегодно меняется (уменьшается). Однако нельзя не сказать, что малый и средний бизнес продолжает активно развиваться и пользоваться услугами банков. Кредитование и факторинг являются одними из наиболее популярных инструментов финансирования для предприятий малого и среднего бизнеса Сибирского федерального округа, в частности Томской области.

ЛИТЕРАТУРА

1. Кизимов В. Малый бизнес и его роль в экономике России [Электронный ресурс]. – Режим доступа: https://journal.open-broker.ru/economy/malyj-biznes-i-ego-rol-v-ekonomike-rossii/ (дата обращения: 17.02.23).

2. Единый реестр субъектов малого и среднего предпринимательства [Электронный ресурс]. – Режим доступа: https://rmsp.nalog.ru/statistics.html?statDate=10.01.2022&level=0&fo=7&ssrf=70&t=1675692758611&t=1675692758611 (дата обращения: 17.02.2023).

3. Кривельская-Ершова А. Какой вид кредитования выбрать? [Электронный ресурс]. – Режим доступа: https://unicom24.ru/articles/vidy-kreditov-kakie-byvayut-i-kakoj-luchshe-vybrat (дата обращения: 17.02.2023).

4. Факторинг для малого бизнеса [Электронный ресурс]. – Режим доступа: https://bankiros.ru/wiki/term/faktoring-dla-malogo-biznesa (дата обращения: 17.02.2023).

5. Официальный сайт Сбербанк [Электронный ресурс]. – Режим доступа: https://www.sberbank.ru/ru/s_m_business/onlinecredit (дата обращения: 18.02.23).

6 Официальный сайт ВТБ-банк [Электронный ресурс]. – Режим доступа: https://www.vtb.ru/malyj-biznes/kredity-i-garantii/ (дата обращения: 18.02.2023).

7. Официальный сайт Альфа-банк [Электронный ресурс]. – Режим доступа: https://alfabank.ru/sme/profits/businesscredit/ (дата обращения: 18.02.2023).

8. Статистический бюллетень. Кредитование субъектов малого и среднего предпринимательства. Декабрь 2021 [Электронный ресурс]. – Режим доступа: https://cbr.ru/Collection/Collection/File/39843/stat_bulletin_lending_2202-12.pdf (дата обращения: 19.02.2023).

9. Статистический бюллетень. Кредитование субъектов малого и среднего предпринимательства. Декабрь 2022 [Электронный ресурс]. – Режим доступа: https://cbr.ru/Collection/Collection/File/43791/stat_bulletin_lending_22-12_31.pdf (дата обращения: 19.0220.23).

10. Информационный обзор рынка факторинга. По итогам 2022 года [Электронный ресурс]. – Режим доступа: https://asfact.ru/wp-content/uploads/2023/02/AFC-Y2022_open.pdf (дата обращения: 19.02.2023).

УДК 338.242

АНАЛИЗ УПРАВЛЕНИЯ УСТОЙЧИВЫМ РАЗВИТИЕМ В СФЕРЕ ФИНАНСОВ И ИНВЕСТИЦИЙ В КОТ-Д'ИВУАРЕ

Д.Д. Бомиссо, магистрант каф. экономики

Научный руководитель В.Ю. Цибульникова, зав. каф. экономики

г. Томск, ТУСУР, bomiss92@gmail.com

Исследуются понятие устойчивого развития и модель управления устойчивым развитием в Кот-д'Ивуаре в финансовой, инвестиционной и экологической областях.

Ключевые слова: устойчивое развитие, менеджмент, финансово-инвестиционная сфера, экологические аспекты, Кот-д'Ивуар.

Проблема устойчивого развития крайне актуальна для Кот-д'Ивуар в современных условиях. Целью настоящей работы является исследование модели управления устойчивым развитием в Кот-д'Ивуаре в финансовой, инвестиционной и экологической областях.

Устойчивое развитие – понятие, допускающее несколько определений. Однако учет долгосрочной перспективы является основным стремлением к устойчивому развитию. Таким образом, она состоит из трех измерений: экономического, социального и экологического. Устойчивое развитие следует понимать как способ развития, который должен обеспечивать «баланс» между экономическим, экологическим и социальным измерениями. Однако речь идет не о противопоставлении трех столпов, а о реализации взаимосвязанных действий. Она становится системой, в рамках которой взаимодействуют экономические, экологические и социальные аспекты с целью удовлетворения потребностей нынешних поколений без ущерба для способности будущих поколений удовлетворять свои потребности. В отчете Брундт-

ланд содержится определение устойчивого развития, которое сегодня кажется единодушным [1].

Однако несмотря на единодушие с точки зрения семантики и его охвата для человечества, преимущества этого способа развития для стран, применяющих этот современный экономический подход, кажутся отсроченными, тем более для развивающихся стран. МВФ считает в одном из своих недавних отчетов, что краткосрочные экономические перспективы для стран Африки к югу от Сахары крайне неопределенны, зная, что они связаны с развитием мировой экономики и что на национальном уровне управление по-прежнему нестабильно. К этому следует добавить, что МГЭИК в одном из своих последних отчетов оценивает, что для ограничения глобального потепления примерно 1,5 °C (2,7 °F) глобальные выбросы газа должны достичь пика парникового эффекта не позднее 2025 г., и сократить на 43% к 2030 г. [2]. Кот-д'Ивуар, развивающаяся страна к югу от Сахары, не является исключением из этой реальности, поскольку помимо стабильного экономического положения в течение нескольких лет она, как и большинство стран к югу от Сахары, пострадала от климатических нарушений, многочисленных стихийных бедствий, которые нарушили производительность страны в различных сферах деятельности, что также может нарушить работу финансового сектора и отпугнуть инвесторов. Поэтому было бы полезно провести анализ управления устойчивым развитием в Кот-д'Ивуаре, особенно в финансовой, инвестиционной и экологической областях.

Финансовый сектор Кот-д'Ивуара на основании Декрета № 92-311 от 15 мая 1992 г. классифицирует финансовые учреждения на три группы в зависимости от характера их операций, которые они уполномочены осуществлять: кредитные организации, финансово-инвестиционные учреждения, другие финансовые учреждения.

Организация финансового ландшафта Кот-д'Ивуара позволила добиться значительного прогресса в улучшении делового климата по данным отчета Всемирного банка «Ведение бизнеса 2020» и занимает 112-е место из 190, в то время как в 2014 г. она была 145-й [3].

Рост финансовой системы и стремление правительства поощрять инвестиции сделали возможным в течение 2022 финансового года (с января по октябрь 2022 г.) «Единому окну для деловых формальностей» (GUFE) зарегистрировать создание 20 183 компаний по сравнению с 9 825 за тот же период с 5 342 прогнозируемыми рабочими местами против 3 954 в 2021 г. Инвестиции утверждены против 575 в 2021 г. Среднее время создания бизнеса сократилось с пятнадцати дней в 2021 г. до менее трех дней в конце октября 2022 г., 47% инве-

сторов – резиденты и 53% – иностранцы. Агропромышленность с 63% инвестиций остается преобладающим сектором, за которым следуют пластмассы (10%) и деревообработка (6%). Планируемое количество рабочих мест – 7 103.

Наиболее целевыми секторами создания бизнеса в 2022 г. являются услуги (44%, в том числе архитектура, проектирование, технический контроль, прокат автомобилей и т.д.), торговля (23%) и строительство (13%) [4].

Что касается экологического аспекта, то в Кот-д'Ивуаре один из самых высоких показателей сокращения лесов в мире: в период с 2001 по 2019 г. страна потеряла более 3 млн гектаров леса, т.е. 20%.

Правительство Кот-д'Ивуара все чаще принимает во внимание окружающую среду в своих проектах развития и сотрудничает с местными и международными партнерами в целях защиты и восстановления природной среды. Например, проекты REDD+ в Кот-д'Ивуаре представляют собой действия, направленные на сокращение выбросов парниковых газов, вызванных обезлесением и деградацией лесов. Они также играют роль в сохранении запасов, устойчивом управлении и увеличении запасов углерода. Согласно национальным данным, представленным Всемирным банком, в 2018 г. 14,892% национальной территории Кот-д'Ивуара составляли охраняемые участки суши и моря [5].

Общий анализ управления устойчивым развитием в Кот-д'Ивуаре показывает, что правительство прилагает усилия с целью улучшения финансового сектора, поощрения инвестиций для обеспечения хорошего экономического роста, хороших социальных условий и здоровой окружающей среды. Однако наблюдение состоит в том, что в Кот-д'Ивуаре акцент не делается на экологических ограничениях по отношению к компаниям, а также мало поощряется направление инвестиций в экологические вопросы. Однако устойчивое развитие определяется не как экономический подход, сопоставляющий три столпа, а как осуществление сквозных действий. Она становится системой, в рамках которой взаимодействуют экономические, экологические и социальные аспекты с целью удовлетворения потребностей нынешних поколений без ущерба для способности будущих поколений удовлетворять свои потребности. Таким образом, можно сказать, что в действиях правительства отсутствуют согласованные действия в части устойчивого развития, что сказывается на эффективности его управления.

ЛИТЕРАТУРА

1. Développement durable et gestion d'une entreprise : croisements fertiles / Eric Allix-Desfautaux, Luyindula G. Davy Makany // Management & Avenir. – 2015. – Vol. 7, No. 81. – C. 15–36 [Электронный ресурс]. – Режим доступа:

https://www.cairn.info/revue-management-et-avenir-2015-7-page-15.htm (дата обращения^ 07.03.2023).

2. 6e rapport d'évaluation du Groupe d'experts intergouvernemental sur l'évolution du climat (GIEC), 3e vol.: Atténuation, CITEPA, p. 40 [Электронный ресурс]. – Режим доступа: https://www.citepa.org/wp-content/uploads/Citepa_2022_05_d01_INT_GIEC_Attenuation_AR6_Vol3_VF.pdf (дата обращения: 06.03.2023).

3. Classement «DOING BUSINESS» des économies mondiales. Banque Mondiale [Электронный ресурс]. – Режим доступа: https://archive.doingbusiness.org/fr/rankings (дата обращения: 07.03.2023).

4. Bilan de l'exercice 2022 du Centre de Promotion des Investissements en Côte d'Ivoire (CEPICI) // Gouvernement de Côte d'Ivoire. https://www.gouv.ci/_actualite-article.php?recordID=14343 [Электронный ресурс]. – Режим доступа:https://apif.finances.gouv.ci/images/app/publications/219/cote-divoire-rapport-annuel-2021-sur-linclusion-financiere.pdf (дата обращения: 08.03.2023).

5. Rapport sur le développement durable en Côte d'Ivoire: Etat des lieux et tendances, 2021. Groupe de recherche «Gouvernance Société Développement Economique – GSDE» du Centre Suisse de Recherches Scientiques en Côte d'Ivoire [Электронный ресурс]. – Режим доступа: https://csrs.ch/storage/app/media/rapport-dd-1.pdf, стр. 33 (дата обращения: 08.03.2022).

УДК 334

АНАЛИЗ И ОСОБЕННОСТИ ИСТОЧНИКОВ ДОХОДА КИБЕРСПОРТИВНЫХ КОМАНД И ОРГАНИЗАЦИЙ

И.П. Чернышов, студент магистратуры каф. менеджмента

Научный руководитель М.А. Афанасова, проф. каф. менеджмента

г. Томск, ТУСУР

Раскрыты особенности киберспорта, рассмотрены причины роста данной индустрии. Определены самые распространенные источники дохода киберспортивных организаций, описаны потенциальные возможности использования новых моделей получения дохода в будущем.

Ключевые слова: киберспорт, организации, команды, источники дохода.

Киберспорт – это новая сфера экономических отношений [1] на стыке спорта, медиабизнеса и интернета, и в ближайшие десятилетия он будет на равных конкурировать с традиционными видами спорта и другими развлечениями [2, 3]. Растущая динамика киберспортивной индустрии приводит к широкомасштабным изменениям в размере и видах инвестиций в данную отрасль, что дает киберспортивным командам и организациям новые возможности для развития.

Индустрия киберспорта. В 2022 г. мировой рынок киберспорта оценивался чуть более чем в 1,38 млрд долларов США. Прогнозируется, что выручка мирового рынка киберспорта вырастет до 1,87 млрд долларов США к 2025 г. [4].

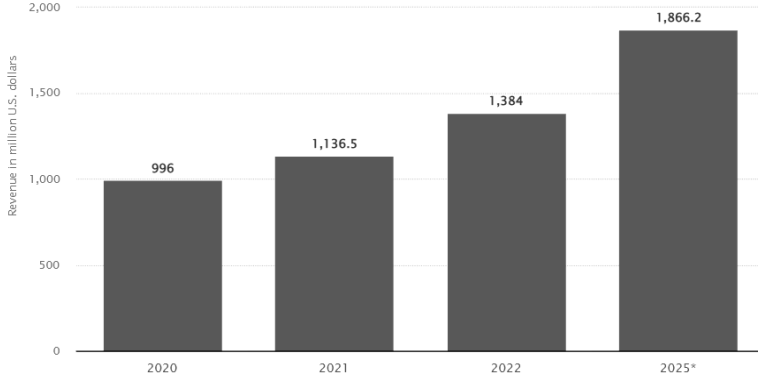


Рис. 1. Выручка рынка киберспорта по всему миру с 2020 по 2025 г. (в миллионах долларов США)

Этот рост обусловлен рядом факторов. Рассмотрим некоторые из них:

1. Рост инфраструктуры киберспорта. Развитие технического оснащения, специализированных объектов (киберарены и др.), обслуживающих предприятий, а также виртуальных сервисов.

2. Рост инвестиций от разнообразных брендов: бренды из смежных индустрий (Razer [5], Red Bull [6]), медиакомпании (Netflix [7], Amazon [8]), а также интерес со стороны брендов, далёких от индустрии (BMW [9], Gucci [10]).

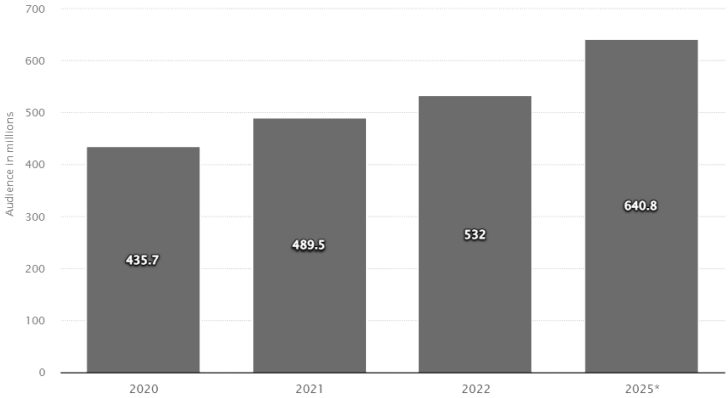


Рис. 2. Размер аудитории киберспорта во всем мире с 2020 по 2025 г. (в миллионах человек) [11]

3. Общий рост количества геймеров приводит к увеличению количества профессиональных игроков, а также зрителей.

4. Появление киберспортивных ассоциаций (Федерация компьютерного спорта России и др.), представляющих интересы киберспортсменов и способствующих развитию индустрии в целом.

Виды источников дохода киберспортивных организаций. Основные источники дохода в киберспорте – это спонсорство и реклама, медиаправа на трансляции турниров, продажи игровой атрибутики и билетов [12].

Турниры. Турнирные доходы зачастую ничтожная сумма по сравнению с тем, что необходимо для ведения деятельности. Многие киберспортивные организации оставляют турнирные доходы игрокам, не забирая долю себе. Вместо этого они предпочитают косвенно извлекать выгоду из успехов команды – это может быть полезно при переговорах о новых спонсорских сделках (которые могут стать более крупными, если у команды есть успехи в игре). Такой подход делает этот источник дохода менее значимым, ведь эта форма дохода не является гарантированной и крайне непостоянна.

Спонсорство. Спонсорство представляет собой ключевой канал дохода в отрасли. В 2019 г. спонсорство принесло 456,7 млн долларов [13]. Брендам из смежных областей это помогает повысить узнаваемость и показать свои продукты миллионам фанатов киберспорта по всему миру. Эта концепция не нова и пришла из практики профессиональных футбольных команд.

Сложно назвать этот источник дохода постоянным, так как спонсорство часто может быть отозвано в случае серьезных проблем с командой и при несоблюдении пунктов контракта.

Инвестиции. Прямые инвестиции отличаются от спонсорства постоянным характером. Часто они исходят от обычных спортивных команд. Например, AS Monaco сотрудничает с Gambit Esports. Многие спортивные команды в настоящее время хотят стать чем-то большим, чем организацией, которая преуспевает только в одном виде спорта. Это своеобразный «экосистемный» подход, который пришел из IT-среды. Наглядный пример – киберспортивная команда BetBoom, в которую инвестирует одноименная букмекерская организация.

В других случаях крупные инвестиционные фирмы вкладываются в киберспорт, видя его быстрый рост и желая заработать на расширяющейся отрасли.

Стриминг. Появление стриминговых платформ позволило многим командам заработать огромные деньги. Например, команда Counter Logic Gaming заключала эксклюзивные контракты с Twitch, Own3d и Azubu [14]. Однако текущие ставки на рекламу на YouTube и

Twitch намного ниже, поэтому это скорее дополнительный источник личного дохода для игроков.

Продукция с символикой бренда (мерч). Более низкодоходная, но более безопасная форма получения дохода от киберспорта: производство и продажа продукции с символикой команды, которую принято называть «мерч». Хорошим примером будет команда Team Liquid, которая заключила партнерское соглашение с Marvel в 2019 г. [15].

Виртуальный характер киберспорта во многих случаях дает дополнительные возможности. Внутриигровые покупки, связанные с киберспортивными организациями, – это уникальный канал, который может значительно увеличить доходы в будущем.

Разработчики и лиги. Еще один способ зарабатывать деньги для команд – напрямую получать выплаты от разработчиков и лиг. Лиги и турниры часто готовы платить командам, чтобы они присоединились к новым турнирам. Выгода организаторов чемпионатов (турниров и лиг) в том, что они будут владеть исключительными правами на трансляцию и рекламу. Это включает в себя продажу билетов, стриминг, продажу товаров на месте проведения.

Заключение. В целом киберспорт – сложная отрасль для получения дохода. Даже самые крупные организации сталкиваются со сложностями по получению доходов и тем более прибыли. Многие ведущие киберспортивные организации отдают предпочтение трем основным источникам дохода: киберспорт, спонсорство и мерч. Влияние и зависимость от этих источников дохода варьируются от команды к команде.

Большой проблемой является то, что инвесторам, которые хотели бы вложить деньги в команды, не гарантирован постоянный рост и рекордная прибыль, т.к. организации в отрасли работают с чрезвычайно переменными затратами и огромными расходами. Таким образом, для многих инвесторов и спонсоров киберспортивные команды рассматриваются как маркетинговое мероприятие.

Рассмотрение того, как киберспортивные команды зарабатывают в 2022–2023 гг., является важным для оценки будущего отрасли, ведь такого притока капитала, который мы наблюдаем сегодня, отрасль не видела никогда.

ЛИТЕРАТУРА

1. Хасанова А.Ш. Формирование устойчивой конкурентоспособности в условиях информатизации экономического пространства // Вестник экономики, права и социологии . – 2014. – Вып. № 4. – С. 101–105.

2. Hope A. The Evolution of The Electronic Sports Enter-tainment Industry and its Popularity. Computers For Everyone // 1st edn. ed. by J. Sharp, R. Self. – 2014 . – PP. 87–89.

3. Степанов С.Д. Киберспорт: тенденции развития отрасли // Научные труды Республиканского института высшей школы. – 2020. – Вып. 19. – С. 431–438.

4. Global eSports market revenue 2020–2025 [Элек-тронный ресурс]. – Режим доступа: https://www.statista.com/statistics/490522/global-esports-market-revenue/ (дата обращения: 10.01.2023).

5. Razer and Esports | What is Esports? [Электронный ресурс]. – Режим доступа: https://www.razer.com/esports (дата обращения: 10.01.2023).

6. Esports will compete at the Red Bull Home Ground Valorant event in Manchester [Электронный ресурс]. – Режим доступа: https://esports.gg/news/valorant/kru-esports-red-bull-home-ground-valorant/ (дата обращения: 10.01.2023).

7. Netflix и Riot Games перенесут League of Legends на экраны в анимационном сериале «Аркейн», премьера кото-рого состоится на Netflix по всему миру этой осенью [Электронный ресурс]. – Режим доступа: https://about.netflix.com/ru/news/netflix-and-riot-games-bring-league-of-legends-to-television-with-animated (дата обращения: 10.01.2023).

8. Activision announces Warzone Rebirth Island tourna-ment in Australia and New Zealand – Esports Insider [Электронный ресурс]. – Режим доступа: https://esportsinsider.com/2022/06/warzone-australia-new-zealand (дата обращения: 10.01.2023).

9. Berlin Brawl 20: BMW celebrates Esports show event as highlight for fans. Official press-release [Электронный ресурс]. – Режим доступа: https://www.press.bmwgroup.com/global/article/detail/T0313830EN/%E2%80%9Cberlin-brawl-20%E2%80%9D:-bmw-celebrates-esports-show-event-as-highlight-for-fans?language=en (дата обращения: 10.01.2023).

10. Gucci Stories – The House unveils its latest foray into the world of esports through a collaboration with 100 Thieves [Электронный ресурс]. – Режим доступа: https://www.gucci.com/us/en/st/stories/inspirations-and-codes/article/100-thieves-shoppable (дата обращения: 10.01.2023).

11. Global eSports audience 2020 [Электронный ресурс]. – Режим доступа: https://www.statista.com/statistics/1109956/global-esports-audience/ (дата обращения: 13.01.2023).

12. Киберспорт: обзор индустрии [Электронный ресурс]. – Режим доступа: https://esforce.com/about/esports-industry (дата обращения: 13.01.2023).

13. Newzoo's Global Esports & Live Streaming Market Report 2021 [Электронный ресурс]. – Режим доступа: https://newzoo.com/insights/trend-reports/newzoos-global-esports-live-streaming-market-report-2021-free-version (дата обращения: 13.01.2023).

14. Counter Logic Gaming announces new streaming partnership with Twitch – GameSpot [Электронный ресурс]. – Режим доступа: https://www.gamespot.com/articles/counter-logic-gaming-announces-new-streaming-partn/1100-6437849/ (дата обращения: 13.01.2023).

15. Team Liquid продлила партнерство с Marvel [Электронный ресурс]. – Режим доступа: https://www.cybersport.ru/tags/other/team-liquid-prodlila-partnerstvo-s-marvel (дата обращения: 10.01.2023).

УДК 338.984

ПРИМЕНЕНИЕ МЕТОДА МОНТЕ–КАРЛО В ИНВЕСТИЦИОННОМ АНАЛИЗЕ

Е.В. Викторенко, ст. преп. каф. экономики;
А.В. Гладышева, А.С. Лавренова, студентки
Проект ГПО Экономики-2203. Применение современных программных продуктов в деятельности экономистов
г. Томск, ТУСУР, каф. экономики, gladysevaana60@gmail.com, alylavren@mail.ru, elena.v.viktorenko@tususr.ru

Рассмотрена возможность использования математического метода Монте–Карло в инвестиционном анализе. Также приведена реализация решения задачи создания модели анализа инвестиционного проекта методом Монте–Карло в среде MS Excel и дальнейшего подключения полученного диапазона данных к проекту, реализованному в среде «Альт-Инвест».

Ключевые слова: риски, инвестиционный проект, метод Монте–Карло, NPV, Альт-Инвест, случайные параметры.

Целью данной статьи является исследование одного из методов количественного анализа рисков инвестиционного проекта метода Монте–Карло и его применения в анализе инвестиционного проекта.

Инвестиционный анализ и теория рисков неразрывно связаны друг с другом. Первое в экономической науке определение риска было дано Ф. Найтом [1], который считал, что риск является измеримой неопределенностью. Мы будем использовать следующее определение «Риск – это событие, связанное с опасным явлением или процессом, которое может произойти или не произойти» [2].

Отметим, что среди авторов, занимающихся вопросами оценки рисков инвестиционных проектов, нет однозначного мнения определения методики данной оценки. Наиболее популярными подходами, встречающимися в литературе, являются качественный и количественный подходы. Качественный подход к анализу не предполагает сложных финансовых расчетов, он основывается на общенаучных методах исследования. Для более точной оценки рисков применяются методы количественного анализа. При реализации некрупных инвестиционных проектов можно ограничиться применением методов анализа чувствительности и сценарного анализа [3].

Среди методов количественной оценки выделяется своим частым и удобным применением метод Монте–Карло. Он получил широкое распространение благодаря своей эффективности, так как позволяет учесть влияние на результат случайных величин и процессов [4]. «При использовании этого метода реальная модель заменяется имитационной, и далее работа с данными производится в имитационной

модели. Модель строится для сотен или тысяч вариантов возможных комбинаций параметров – чем больше вариантов комбинаций, тем качественней построенная имитационная модель» [5]. В результате анализа рисков данным методом вычисляется значение чистой приведенной стоимости (NPV) исследуемого проекта.

Для того чтобы получить значения распределения чистой приведенной стоимости инвестиционного проекта методом Монте–Карло, используем инвестиционный проект, реализованный в программе «Альт-Инвест», моделирование проведем при помощи редактора MS Excel, затем подключим модель к инвестиционному проекту.

При построении модели в MS Excel выставляем параметры для анализа Монте–Карло, будем считать, что они нормально распределены, т.е. их характеристики задаются двумя величинами – среднее значение и стандартное отклонение. При моделировании случайных чисел используется стандартная функция MS Excel СЛЧИС(), которая возвращает равномерно распределенное случайное число. Затем выполним моделирование сценариев.

В редакторе MS Excel запускаем цикл из тысячи повторений, на каждом шаге получаем случайные значения параметров в соответствии с их законом распределения.

Для подключения полученного диапазона данных к инвестиционному проекту в среде «Альт-Инвест» скопируем лист с моделью и внедрим в файл анализируемого инвестиционного проекта.

Результат моделирования представим в виде гистограммы, на которой видна частота попадания результата в интервалы значений. Пример графика распределения значений чистой приведенной стоимости инвестиционного проекта методом Монте–Карло изображен на рис. 1.

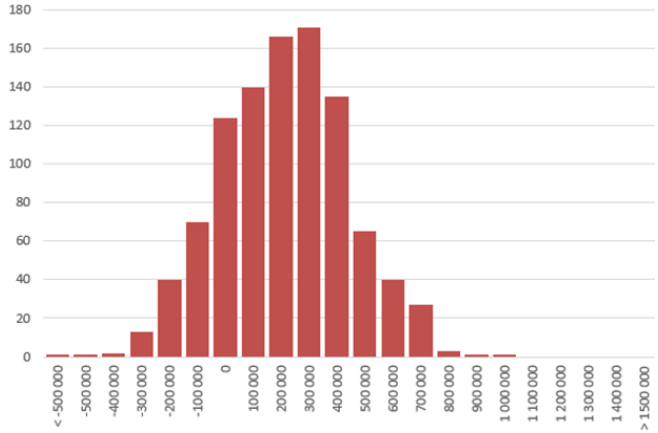


Рис. 1. График распределения значений чистой приведенной стоимости (NPV) методом Монте–Карло

На этом графике по оси *X* расположены значения чистой приведенной стоимости, полученные в расчетах, по оси *Y* – случаи попадания чистой приведенной стоимости в этот интервал.

В данной статье описана модель анализа инвестиционного проекта методом количественной оценки, реализованная в среде MS Excel, а также представлен результат распределения значений чистой приведенной прибыли, полученный вследствие внедрения модели в инвестиционный проект, реализованный средствами программы «Альт-Инвест».

ЛИТЕРАТУРА

1. Найт Ф.Х. Риск, неопределенность и прибыль / пер. с англ. М.Я. Каждана. – М.: Дело, 2003. – 359 с.

2. Анфилатов В.С. Системный анализ в управлении / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; под ред. А.А. Емельянова. – М.: Финансы и статистика, 2009. – 284 с.

3. Гареев А.З. Риски при реализации инвестиционных проектов // Инновационная наука. – 2016. – № 10-1. – С. 30–33.

4. Степаненко Н.В. Применение возможностей Microsoft Excel в моделировании рисков инвестиционных проектов / Н.В. Степаненко, С.В. Харитонов // Прикладная информатика. – 2017. – Т. 12, № 1 (67). – С. 137–142.

5. Ефремова Е.А. Применение метода Монте–Карло для оценки инвестиционных проектов / Е.А. Ефремова, В.А. Прядкина // Научное сообщество студентов XXI столетия. Экономические науки: сб. ст. по матер. XXVII студ. Междунар. науч.-практ. конф. – 2014. – № 12 (27). – С. 237–244.

УДК 336.763

О ВЛИЯНИИ ЭКОНОМИЧЕСКИХ КРИЗИСОВ НА ПОВЕДЕНИЕ ИНВЕСТОРОВ НА ФОНДОВОМ РЫНКЕ

А.В. Гордиенко, аспирант каф. экономики

Научный руководитель В.Ю. Цибульникова, зав. каф. экономики, к.э.н., доцент

г. Томск, ТУСУР, an.gordienko@inbox.ru

Проводится оценка поведения инвесторов под влиянием крупных экономических кризисов, вызванных различными факторами. Для оценки используются четыре наиболее популярных индекса, оцениваемых разными странами. Для анализа отобраны два наиболее крупных кризиса, которые повлияли не только на инвестиционные рынки, но и на мировую экономику в целом. В результате оценки выяснилось, что инвесторы склонны продавать активы под влиянием нестабильной экономической ситуации.

Ключевые слова: частный инвестор, инвестиции, экономический кризис.

Финансовые рынки являются сферой деятельности, в рамках которой инвесторы подвержены различным видам риска, вызванным как своими решениями, так и внешними факторами. Наиболее серьёзное влияние на поведение инвесторов могут оказывать экономические кризисы, затрагивающие всех участников рынка. Некоторые кризисы могут быть ми т.к. они вызваны цепочкой определённых событий на протяжении длительного времени и у инвесторов есть время к ним подготовиться и принять решение. Другие же могут наступить внезапно и быстро. Тогда инвесторы могут принять нерациональное решение, которое основывается на ограниченности информации, времени и ресурсов, что приводит к появлению убытков или упущению потенциальной прибыли.

Один из кризисов, который наступил быстро и непредсказуемо, был вызван массовым заражением вирусным заболеванием COVID-19. Изначально болезнь носила локальный характер. В течение нескольких месяцев он распространился воздушно-капельным путем до мирового уровня [1]. Вся мировая экономическая система начала реструктуризацию процессов, а многие компании не могли корректно функционировать. На эти изменения отреагировали и частные инвесторы, которые начали выводить деньги из финансовых рынков, опасаясь резкого падения стоимости активов, а также их фиксации в неликвидном состоянии. Эмоциональное давление, страх потери средств, стабильности и ликвидности вложений, реорганизация приоритетов распределения ресурсов и удовлетворения потребностей привели к массовому выводу активов инвесторами и падению рынка.

С другой стороны, можно выделить мировой экономический кризис (МЭК), который обозначился в 2008 г. и был вызван рядом событий, повлиявших на всю мировую экономику. Перегрев фондового, кредитного, в том числе и ипотечного рынков, установление высокого ценового уровня на сырьевые товары, сокращение ликвидности крупнейших мировых банков, автомобильных компаний, рецессия и спад производства, банкротство крупных финансовых институтов и т.д. привели к крупным убыткам многих участников экономической мировой системы разных стран [2, 3]. Это также отобразилось и на инвесторах, которые начали продавать активы из-за страха потерять деньги. Даже наличие предшествующих показателей, которые могли дать возможность спрогнозировать подобный исход событий, не смогли защитить инвестиционный рынок от падения. Стоит отметить, что начальные кризисы, которые эскалировали МЭК, были вызваны экономическим, зачастую нерациональным поведением физических лиц, многие из которых перенесли это поведение и на инвестиционные рынки.

Для оценки действий инвесторов в условиях кризисного состояния экономической среды использовались одни из наиболее популярных индексов четырёх региональных экономик, которые оценивают состояние собранных в них ценных бумаг [4, 5]:

1) индекс МосБиржи (IMOEX) – включает 50 наиболее ликвидных акций крупнейших российских компаний;

2) индекс S&P 500 (SPX) – включает примерно 500 акций наиболее крупных компаний на торгуемых фондовых биржах США;

3) индекс Shanghai Composite (SSEC) – включает более 1600 компаний из котировальных листов A и B Шанхайской фондовой биржи;

4) индекс DJ Euro Stoxx 50 (STOXX50E) – включает 50 крупнейших и наиболее ликвидных компаний европейского сектора.

На рис. 1 отражена динамика изменения стоимости этих индексов до начала кризиса, в период пика его активности и после окончания. Показатели:

1) «До» указывает на экономическое состояние до начала кризиса;

2) «В течение» помогает оценить влияние кризиса в его наиболее активной фазе, сравнивая стоимость индекса на момент закрытия цены «До» и закрытия цены «В течение»;

3) «После» оценивает состояние рынка после завершения активной фазы кризиса, показывая изменение стоимости фонда на момент закрытия цены «После» относительно закрытия цены «До».

Для кризиса, вызванного вирусным заболеванием COVID-19, можно выделить следующие периоды:

1) «До» – 01.01.2019–01.01.2020;

2) «В течение» – 01.01.2020 – 01.04.2020;

3) «После» – 01.04.2020 – 01.01.2021.

Для МЭК можно выделить следующие периоды:

1) «До» – 01.01.2007 – 01.01.2008;

2) «В течение» – 01.01.2008 – 01.01.2009;

3) «После» – 01.01.2009 – 01.01.2010.

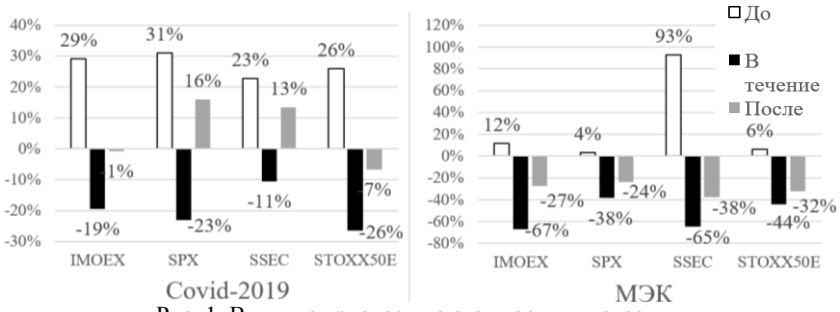


Рис. 1. Влияние кризисов на стоимость индексов

До начала кризисных ситуаций индексные показатели отображали экономический рост. Можно отметить, что с 2008 по 2019 г. у инвесторов вырос уровень диверсификации. Уровень падения рынка при внезапном кризисе в разы меньше, чем падение при МЭК. Также инвесторы восстановили активность, и рост рынка оказался быстрее после непредсказуемого кризиса. Такое состояние может быть вызвано повышением уровня готовности и адаптации инвесторов к кризисам после МЭК. Однако даже при готовности к кризисной ситуации инвесторы склонны к продаже бумаг в целях сохранения ликвидности. Такие действия могут быть вызваны страхом и другим эмоциональным состоянием.

ЛИТЕРАТУРА

1. История вируса: когда люди начали болеть COVID-19 [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/opinions/society/30/03/2020/5e7dbfa79a7947b91d218143, свободный (дата обращения: 25.02.2023).
2. Современный мировой экономический кризис [Электронный ресурс]. – Режим доступа: https://mirec.mgimo.ru/2008/2008-4/sovremennyj-mirovoj-ekonomicheskij-krizis, свободный (дата обращения: 27.02.2023).
3. Мировой финансовый кризис 2008 года и его последствия для России [Электронный ресурс]. – Режим доступа: https://ria.ru/20130816/956672411.html, свободный (дата обращения: 28.02.2022).
4. Мировые фондовые индексы [Электронный ресурс]. – Режим доступа: https://ru.investing.com/indices/major-indices, свободный (дата обращения: 01.03.2023).
5. Биржевой (фондовый) индекс [Электронный ресурс]. – Режим доступа: https://www.banki.ru/wikibank/birjevoy_indeks, свободный (дата обращения: 02.03.2023).

УДК 336. 763

ОСОБЕННОСТИ ОЦЕНКИ СТОИМОСТИ ПРЕДПРИЯТИЙ АГРОБИЗНЕСА

А.А. Гребенникова, магистрант каф. экономики

Научный руководитель Н.Б. Васильковская, доцент каф. экономики

г. Томск, ТУСУР, arina.grebennikova.2013@mail.ru

Интеграционные процессы в агропромышленной сфере делают актуальным вопрос о стоимости присоединяемого бизнеса. На стоимость агробизнеса оказывает большое влияние набор экономических, социальных и природно-климатических факторов, поэтому возникает проблема выбора подхода к оценке стоимости и методов в его составе.

Ключевые слова: оценка стоимости бизнеса, агробизнес, методы оценки.

Оценка стоимости предприятий агробизнеса играет ключевую роль в принятии решения о целесообразности инвестирования в него. Особенно это касается тех предприятий, которые сейчас нуждаются в больших инвестициях. Поскольку все предприятия имеют ограниченное количество ресурсов, вопрос оценки стоимости их имущества, определения стоимости предприятия, максимально приближенной к реальной, приобретает особое значение. Предприятия АПК имеют ряд особенностей, которые не позволяют применить весь спектр методологических подходов и методов, используемых для оценки других видов бизнеса.

Цель статьи – обоснование выбора подходов и методов к оценке стоимости предприятий агробизнеса.

В процессе исследования применялись способы группировки и сравнения, аналитический метод.

Для определения стоимости бизнеса существует три различных подхода: затратный, доходный и сравнительный [1]. При определении стоимости может использоваться либо один подход, либо комбинация трех подходов (рис. 1).

Несмотря на отличия методов затратного подхода (метод чистых активов фокусируется на коррекции активов и обязательств на дату оценки, а ликвидационной стоимости – на стоимости, которую бизнес получит после продажи актива на открытом рынке), их особенностью является их ориентация на стоимость активов.

Рис. 1. Основные подходы к оценке стоимости бизнеса

Но одна из особенностей предприятий агробизнеса – моральный и физический износ основных фондов, короткий срок эксплуатации технологического оборудования в животноводстве [2] – ограничивает возможности использования этих методов. В АПК затратный подход могут применять только те предприятия, которые используют в процессе производства большое количество основных средств и оборудо-

вания (например, агрохолдинг или современная высокотехнологичная агрофирма).

К наиболее распространенным методам доходного подхода относят методы капитализации доходов и дисконтирования денежных потоков (ДДП) [3]. В первом случае речь идет о будущих доходах в текущей стоимости, полученных с помощью коэффициента капитализации. Известно, что этот метод неприменим для предприятий с убытками либо с нестабильными темпами роста доходов, а для агробизнеса с его сезонностью производства, зависимостью доходов от природно-климатических условий, большим влиянием на доходы финансово-экономических условий нестабильность доходов является ключевой характеристикой.

Главным достоинством метода ДДП является то, что им можно оценить бизнес с непостоянными, а иногда и отрицательными финансовыми результатами, в условиях непостоянности доходов и рынка в целом.

Доходный подход в оценке стоимости агробизнеса является наиболее актуальным и достоверным, так как позволяет учесть все изменения внешней среды и ситуации, которые могут сложиться на предприятии в определенный период времени.

Сравнительный подход – это метод относительной оценки, при котором сравнивается текущая стоимость бизнеса с другими аналогичными предприятиями [3].

Все три метода сравнительного подхода, с одной стороны, отражают близкие к реальным значения спроса и предложения на объект в текущий момент времени, с другой стороны, они предполагают наличие достоверной, сопоставимой и своевременной информации, и это является главным ограничением возможности их применения. Например, предприятия должны соответствовать таким критериям, как:

– тождество объёма и качества произведённой продукции;

– идентичность размеров, финансовых характеристик и стратегий развития рассматриваемых компаний.

При этом метод компании-аналога основан на рыночной цене обыкновенных акций, т.е. неприменим для ООО.

Метод сделки также предполагает наличие информации о ранее совершенных сделках, однако существенные условия сделок, влияющие на стоимость, обычно являются коммерческой тайной.

Третий метод требует от оценщика наличия опыта оценки объектов данного типа.

Результаты. Можно сделать вывод о том, что специфика агробизнеса делает ряд подходов нецелесообразными к применению, и

более подходящим для АПК подходом является доходный подход, однако данный подход не всегда дает объективные результаты, поэтому существует необходимость в корректировке подхода, использование которого позволит снизить финансовые риски.

ЛИТЕРАТУРА

1. Антилл Н. Оценка компаний. Анализ и прогнозирование с использованием отчетности по МСФО / Н. Антилл, Л. Кеннет. – М.: Альпина Паблишер, 2019. – 442 с.

2. Стратегия развития агропромышленного и рыбохозяйственного комплексов Российской Федерации на период до 2030 года [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/G3hzRyrGPbmFAfBFgmEhxTrec694MaHp.pdf

3. Спиридонова Е.А. Оценка стоимости бизнеса: учебник и практикум для вузов. – 2-е изд., перераб. и доп. – М.: Юрайт, 2022. – 317 с. [Электронный ресурс]. – Режим доступа: https://urait.ru/bcode/489925 (дата обращения: 12.02.2023).

УДК 336.71

ПРОБЛЕМЫ БАНКОВСКОГО ИПОТЕЧНОГО КРЕДИТОВАНИЯ ФИЗИЧЕСКИХ ЛИЦ В УСЛОВИЯХ ВНЕШНЕЭКОНОМИЧЕСКИХ САНКЦИЙ

К.В. Макарчикова, студентка

Научный руководитель Л.С. Хромцова, к.э.н., доцент каф. бизнеса и экономики

г. Ханты-Мансийск, ФГБОУ ВО Югорский государственный университет, kmakarchikova@gmail.com

Оценивается влияние внешнеэкономических санкций 2022 г. на коммерческие банки в части ипотечного кредитования физических лиц Российской Федерации. Проводится анализ уровня кредитования, выявляются проблемы процесса кредитования для обеих сторон: банков и физических лиц.

Ключевые слова: внешнеэкономические санкции, ипотечное кредитование физических лиц, российские коммерческие банки, банковские системы, актуальные проблемы ипотечного кредита.

На современном этапе развития банковские отечественные системы переживают экономическое потрясение в связи с изменениями политической ситуации в мире, общественной изменчивостью и девальвацией российского рубля, которые приводят к негативным последствиям. Стабильность денежного эквивалента является первостепенной задачей банков в экономике, сопоставимости массового по-

требления национальной валюты и сбалансированности денежной политики банковского сектора. Специфика деятельности банков подвержена многочисленным рискам, которые зависят от разного периода изменений в финансово-экономическом положении страны. Например, зависимость от депозитных счетов, чем от основного капитала; низкая ликвидность имущественных активов по сравнению с собственным капиталом и заемными средствами банка. Тем самым недооценка возможности убыточности кредитной организации может повлиять на основную массу клиентов и собственников банков. Вследствие чего главной стратегической целью банковской системы является создание макроэкономических условий и финансовой стабильности для экономического роста денежно-кредитной политики государства.

Особенно кардинально кризис повлиял в коммерческих банках на ипотечное кредитование заемщиков. Двухлетний рост цен на недвижимость продолжил свою динамику и в 2022 г., при том, что порядка 70% жилой недвижимости на рынке приобретается с привлечением ипотечных средств. По прогнозам на 2023 г. в среднем жилье подешевеет незначительно всего на 15–20%. Прежде всего потому, что рынок 2023 г. будет под давлением кризиса, который увеличивает стоимость всех аспектов жизнедеятельности, включая недвижимость. Так, в 2023 г. будет увеличена конкуренция между застройщиками и владельцами вторичного жилья по причине падения возможности погашения ипотеки.

Покупка квартиры для российских граждан является одной из наиболее сложных социальных и экономических проблем, решение которой требует значительных изменений в сфере ипотечного кредитования. Экономические санкции затрагивают всех субъектов и объектов рыночных отношений, включая другие государства. Для населения страны возникли трудности с получением ипотечного жилья. К таким проблемам относятся внешние факторы влияния:

1. Девальвация российского рубля. За последние три года уровень инфляции существенно изменялся, так на апрель 2022 г. показатель достиг 17,83%. При этом ключевая ставка Центрального банка России колебалась по нескольку раз за год от 20 до 7,5%. Тенденция снижения платежеспособности и потребности в приобретении недвижимости прямо связана с процентными ставками банка.

2. Уменьшение реальных денежных доходов населения. Ипотечные кредиты обычно выдаются на срок до 10–30 лет, а реальные доходы граждан зависят от инфляции и развития экономики.

3. Процесс региональной монополизации строительства жилищного сектора. Поскольку в регионе нет крупных строительных компа-

ний, то отсутствует конкуренция на рынке, и руководители частных строительных организаций взимают большую плату за жилье с целью получения большего дохода.

4. Повышение процентных ставок по кредиту. На фоне финансовых трудностей в России темпы развития рынка ипотечного кредитования приостанавливаются, что привело к замедлению совершенствования ипотек для граждан из категории социально нуждающихся. На примере филиала ПАО Банка «ФК Открытие», функционирующего в городе Ханты-Мансийске, в модуле ипотечного кредитования есть ряд внутренних факторов, которые влияют на решение по ипотечному кредитованию населения в нынешнее время:

1. Отсутствие выбора застройщиков и жилья для покупки. Заемщикам приходится осуществлять самостоятельный поиск квартир либо обращаться к риэлтерским услугам, так как у большинства нет необходимых знаний и времени в данном вопросе. Также они пытаются избежать мошенничества и потери денег. А это носит дополнительные расходы для клиента.

2. Сложность процедуры оформления и неопределенный срок одобрения ипотеки. Данная проблема автоматизирована через официальный сайт банка, где можно подать заявку на кредитование. Но дальнейшая процедура проходит в очном формате, где нужны полные сведения о человеке и его собственности. Многие люди считают, что процесс оформления долгий и загруженный, и от качества необходимых сведений банк принимает окончательное решение. После первого отказа банка клиент ожидает три месяца для повторной заявки.

3. Высокие цены на квартиры и процент первоначального взноса. Рынок Ханты-Мансийска не является перенасыщенным, но с увеличением спроса и завышением цен на квартиры, которые отличаются от её реальной стоимости, покупка квартиры в данном городе является недоступной для молодежи по сравнению с Тюменью. При том, что здесь развивается студенчество и приток молодого поколения возрастает, но возможности остаться на постоянное проживание минимальные.

Таким образом, результаты показали возможные пути развития ипотечных программ на данном этапе, которые требуют принятия решений для совершенствования процесса кредитования. Такими решениями могут являться создание новейшей ипотеки для физических лиц с новыми условиями и выгодными ставками либо разработка иных мероприятий, но полное устранение данных потерь считается невозможным из-за отсутствия влияния банков на такие факторы.

ЛИТЕРАТУРА

1. Постановление Правительства РФ от 11.01.2000 № 28 (ред. от 08.05.2002) «О мерах по развитию системы ипотечного жилищного

кредитования в Российской Федерации» (вместе с «Концепцией развития системы ипотечного жилищного кредитования в Российской Федерации», «Планом подготовки проектов нормативных правовых актов, обеспечивающих развитие системы ипотечного жилищного кредитования в Российской Федерации») [Электронный ресурс] // Консультант Плюс. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_25763/

2. Показатели рынка жилищного (ипотечного жилищного) кредитования / Ключевые ставки Банка России и инфляция [Электронный ресурс]. – Банк России. – Режим доступа: https://cbr.ru/statistics/bank_sector/mortgage/ (дата обращения: 26.02.2023).

3. Риски ипотечного кредитования: анализ моделей мирового рынка [Электронный ресурс]. – Режим доступа: http://www.ahml.ru. (дата обращения: 27.02.2023).

4. Рынок строительства и недвижимости: стимулы отрасли на фоне кризиса – 2020 // Центр социально-экономических исследований [Электронный ресурс]. – Режим доступа: https://www.csr.ru/upload/iblock/4b5/4b5726e9ed7a3df78621cf6aab8e9630.pdf (дата обращения: 27.02.2023).

УДК 336.77

АНАЛИЗ ДИНАМИКИ ОБЪЕМОВ КРЕДИТОВАНИЯ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ И ЮРИДИЧЕСКИХ ЛИЦ В СОВРЕМЕННОЙ РОССИИ

Е.А. Мищенко, студентка каф. экономики

Научный руководитель А.Д. Извекова, доцент каф. экономики, к.э.н.

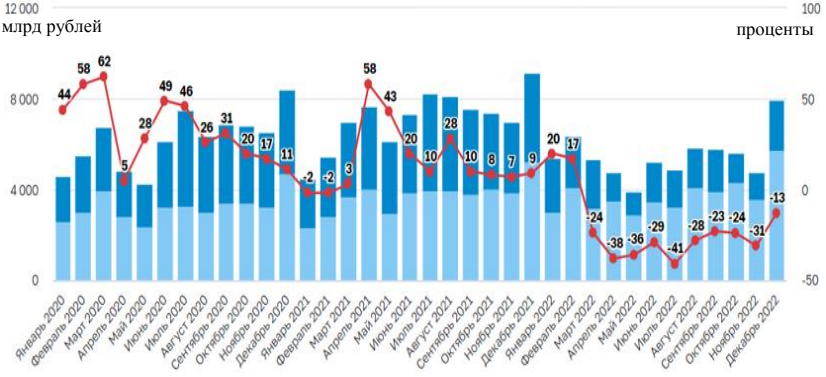
г. Томск, ТУСУР, Katyusha.m2001@bk.ru

Приведен анализ основных тенденций на рынке банковского кредитования индивидуальных предпринимателей и юридических лиц в 2022 г. Выявлены основные факторы, оказавшие влияние на динамику объемов кредитования и величину ссудной задолженности индивидуальных предпринимателей и юридических лиц.

Ключевые слова: банки, кредитование, просроченная задолженность, Центральный банк, ключевая ставка.

В экономике нет стандартных ситуаций, и в процессе своей деятельности банкам приходится корректировать свою политику. Во избежание банкротства, для достижения и долгосрочного сохранения устойчивого положения на рынке необходимо находить и активно применять эффективные методы и инструменты управления [1].

Для того чтобы разработать эффективную кредитную политику, необходимо детально анализировать складывающуюся на финансовом рынке ситуацию и адекватно реагировать на различные внутренние и внешние шоки. Рассмотрим, какие тенденции были характерны для рынка кредитования в России в 2022 г. (рис. 1).



Кредиты, предоставленные заемщикам, осуществляющим деятельность, относящуюся к разделу ОКВЭД 2 «К – деятельность финансовая и страховая».

Кредиты, предоставленные заемщикам, осуществляющим деятельность, относящуюся к иным разделам ОКВЭД 2.

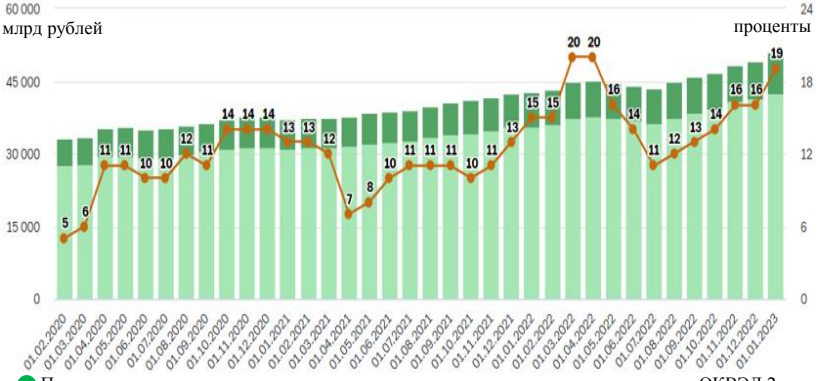
Годовой темп прироста объема предоставленных кредитов (правая шкала).

Рис. 1. Динамика объема кредитов, предоставленных ИП и ЮЛ, в рублях и иностранной валюте в период с 2020 по 2022 г. [2]

Из рис. 1 можно сделать вывод, что объем выдачи новых кредитов в 2022 г. снижается по сравнению с 2021 г. Так, в ноябре 2021 г. объем выданных кредитов составил 6,98 трлн рублей, а в аналогичном периоде в 2022 г. – 4,79 трлн рублей, что на 31% меньше, разница составила 2,19 трлн рублей [2]. Больше всего кредитов в декабре 2022 г. было выделено заемщикам, чья деятельность связана с финансовой и страховой сферами (2190 млрд руб.). За аналогичный период заемщикам, относящимся к сфере «Торговля оптовая и розничная; ремонт автотранспорта», было выдано кредитов на сумму 1600 млрд рублей, к сфере «Обрабатывающие производства» – 1584 млрд рублей, «Деятельность профессиональная, научная» – 628 млрд руб., «Добыча полезных ископаемых» – 351 млрд руб., на прочие сферы деятельности приходилось 1601 млрд рублей.

Если объемы выдачи кредитов индивидуальным предпринимателям и юридическим лицам в 2022 г. снижались (по объективным причинам) по сравнению с годом ранее, то динамика ссудной задолженности по этой категории заемщиков, напротив, имела тенденцию к росту (рис. 2).

Анализируя рис. 2, мы видим, что задолженность по кредитам, предоставленным юридическим лицам и ИП, за декабрь 2022 г. возросла на 3,4%, до 50,8 трлн рублей (на 01.01.2023 г.). Пик роста задолженности можно наблюдать в период с апреля по июнь 2022 г. Но начиная с 3 квартала 2022 г. ситуация нормализовалась – задолженность уменьшилась [2].



По кредитам заемщиков, осуществляющим деятельность, относящуюся к разделу ОКВЭД 2 «К – деятельность финансовая и страховая».

По кредитам заемщиков, осуществляющим деятельность, относящуюся к иным разделам ОКВЭД 2.

Годовой темп прироста задолженности (правая шкала).

Рис. 2. Динамика задолженности по кредитам, предоставленным ЮЛ и ИП, в рублях и иностранной валюте в период с 2020 по 2022 г. [1]

Существует множество факторов, которые повлияли на вышеуказанную ситуацию в сфере кредитования:

1. Изменение Центральным банком РФ ключевой ставки. 28 февраля 2022 г. Центральным банком было принято решение о повышении ключевой ставки до 20% годовых, с целью защиты рубля от обесценивания.

После повышения ключевой ставки ставки на кредиты в коммерческих банках пропорционально возросли, что сделало кредиты менее привлекательными для заемщиков, а вклады более актуальными.

2. Спецоперация. После начала спецоперации количество заявок на кредиты и количество их одобрений снизились практически в два раза. Банки с целью собственной защиты начали одобрять небольшие суммы для выдачи в кредит.

3. Заморозка активов Центрального банка РФ. Существенная доля активов Центрального банка, находившихся за границей, была заморожена, что негативно сказалось на экономике. Это повлекло за собой рост инфляции в России и повышение ключевой ставки, как сдерживающего регулятора. Вследствие чего выросли процентные ставки по кредитам.

Как банки отреагировали на происходящее в России:

Стали вести сдержанную политику, несмотря на высокий спрос в заемных средствах со стороны клиентов. Вводились разного рода ограничения, изменялись условия и тарифы на банковские продукты.

Это было сделано для того, чтобы не допустить массовых дефолтов и чтобы иметь возможность продолжать эффективную деятельность в сложившихся условиях [3].

Чтобы удержать средства на счетах, банки стали вводить комиссии за снятие средств со счетов, которые не пролежали там определенного периода. Также существенно выросли банковские ставки по кредитам. Была запрещена покупка наличной валюты. Был введен запрет на снятие наличных более 10 000 долларов. Отменили НДС на покупку банковского золота [4].

Таким образом, политика банков в этот период времени была направлена на удержание клиентов и денежной массы, стабилизацию ситуации в стране.

Вероятнее всего, банки продолжат ограничивать выдачу высокорискованных займов, что приведет к повышению стоимости кредитования и ужесточению требований к заемщикам [5]. Если уровень инфляции снизится до ожидаемых Центральным банком 5–7%, то ситуация с кредитованием стабилизируется, так как Центральный банк снизит ключевую ставку, что, в свою очередь, позволит банкам уменьшить ставки по кредитам [6].

Таким образом, можно заметить, что рынок кредитования, как и экономика нашей страны в целом, в настоящее время переживает не самые легкие времена. Но банковская система сделала все возможное, чтобы сдержать отток клиентов и стабилизировать ситуацию. В данный период еще рано судить об эффективности проводимой денежно-кредитной политики, можно только предполагать и надеяться, что объемы кредитования индивидуальных предпринимателей и юридических лиц постепенно восстановятся.

ЛИТЕРАТУРА

1. Управление кредитным риском в коммерческом банке [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/upravlenie-kreditnym-riskom-v-kommercheskom-banke (дата обращения: 01.02.2023).

2. Кредитование юридических лиц и индивидуальных предпринимателей в декабре 2022 г. [Электронный ресурс]. – Режим доступа: https://cbr.ru/statistics/bank_sector/sors/credit/ (дата обращения: 05.02.2023).

3. Портрет заемщика банка в 2022 г. [Электронный ресурс]. – Режим доступа: https://www.banki.ru/news/research/?id=10977910 (дата обращения: 10.02.2023).

4. НБКИ в I полугодии 2022 г. [Электронный ресурс]. – Режим доступа: https://nbki.ru/company/news/?id=1140323 (дата обращения: 13.02.2023).

5. Кредиты в 2023 г. [Электронный ресурс]. – Режим доступа: https://www.banki.ru/news/daytheme/?id=10977277 (дата обращения: 17.02.2023).

6. Основные направления единой государственной денежно-кредитной политики на 2023 г. [Электронный ресурс]. – Режим доступа: https://cbr.ru/about_br/publ/ondkp/on_2023_2025/ (дата обращения: 20.02.2023).

УДК 338.4.055.2:005.344(470+571)

БЫСТРЫЙ РОСТ БИЗНЕСА ПОСЛЕ СТАГНАЦИИ: ВЛИЯНИЕ ФАКТОРА ИНВЕСТИЦИЙ

В.А. Леонова, ассистент ШИП; В.В. Спицын, к.э.н., доцент ШИП
г. Томск, НИ ТПУ, vap60@tpu.ru

Исследуется влияние инвестиционного фактора на развитие фирм после периода стагнации. Установлено, что группы фирм, показавшие быстрый рост после периода стагнации, характеризовались более высокой инвестиционной активностью в последний год периода стагнации. Следовательно, более высокая инвестиционная активность фирмы является одним из факторов преодоления стагнации и выхода на магистраль роста.

Ключевые слова: быстрорастущие компании, стагнация, возобновляемый рост, постстагнационное развитие, экзогенные шоки, Россия.

Проблема развития предприятий после стагнации крайне актуальна для России в современных условиях. Практически с 2008 г. экономика страны периодически сталкивается с кризисными явлениями, вызываемыми внешними неблагоприятными факторами. Многие российские предприятия оказались в длительной стагнации. При этом финансовые ресурсы для создания и развития новых предприятий в настоящее время ограничены из-за введенных санкций западными странами. В этих условиях одним из вариантов преодоления кризиса является разработка механизмов по преодолению стагнации и выходу на магистраль роста для перспективных российских предприятий. Разработка таких механизмов предполагает выявление факторов, способствующих преодолению стагнации и росту предприятий.

Целью настоящей работы является исследование влияния фактора инвестиционной активности на переход к росту российских предприятий, находящихся в стагнации.

Гипотеза исследования. Предприятия, показавшие существенный рост выручки после периода стагнации, характеризовались более высокой инвестиционной активностью в последний год периода стагнации.

Методика исследования. Выборка предприятий и их финансовых показателей была сформирована на основе данных ИС СПАРК [1]. В выборку включались предприятия ведущих отраслей добывающей и обрабатывающей промышленности России, а также высокотехнологичных отраслей сферы услуг. Критерии включения в выборку:

– наличие ежегодных данных о выручке за 2012–2021 гг.;

– ежегодная выручка превышает пороговое значение (20–50 млн руб.).

Ежегодная выручка и другие показатели были скорректированы на накопленный индекс инфляции и приведены к 2012 г.

Далее была сформирована выборка предприятий, находящихся в длительной стагнации, т.е. показавших отрицательный прирост выручки ежегодно в течение трех лет подряд за 2013–2017 гг. (2 232 фирмы).

Эта выборка была разделена на 4 группы:

– группа 1 – предприятия, не показавшие существенный рост после стагнации (1 709 фирм);

– группа 2 – предприятия, показавшие умеренный долгосрочный рост (ежегодный темп прироста выручки более 10% в течение 3 из 4 лет после стагнации, общий прирост более 30%) (197 фирм);

– группа 3 – предприятия, показавшие быстрый долгосрочный рост (ежегодный темп прироста выручки более 20% в течение 3 из 4 лет после стагнации, общий прирост более 30%) (95 фирм);

– группа 4 – предприятия, показавшие быстрый краткосрочный рост (темп прироста выручки более 60% за 4 года, но более 10% – не более 2 лет) (231 фирма).

Исследуемый показатель: доля инвестиций в выручке в последний год периода стагнации. Визуализация этого показателя проводится с помощью диаграммы размаха, в которой линия – медиана, прямоугольник – 25–75%-й квартальный размах, усы – минимальное и максимальное значение или 1,5 интерквартильный размах. Для выявления значимых различий между группами предприятий по исследуемому показателю используется критерий Манна–Уитни [2].

Результаты. Исследуемый показатель представлен на рис. 1.

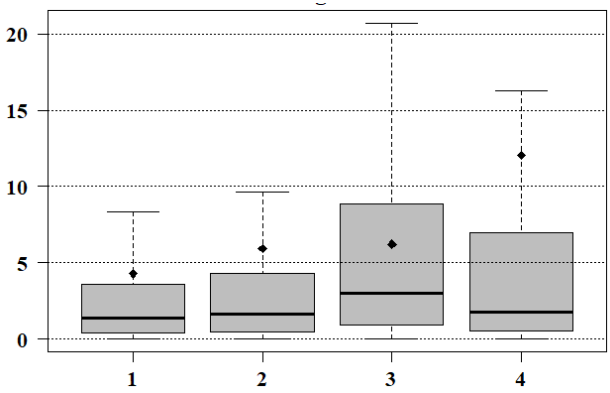


Рис. 1. Диаграмма размаха инвестиционной активности по группам предприятий, %

Визуально мы наблюдаем более высокую инвестиционную активность у третьей группы предприятий. Согласно критерию Манна–Уитни, обнаружено:

– незначимые различия между 1-й и 2-й и между 3-й и 4-й группами;

– инвестиционная активность 3-й и 4-й групп сильно значимо выше, чем у 1-й группы, и статистически значимо выше, чем у 2-й группы.

Таким образом, наша гипотеза подтверждается частично, только в отношении групп предприятий, показавших быстрый рост выручки после стагнации. Следовательно, более высокая инвестиционная активность фирмы является одним из факторов преодоления стагнации и перехода к быстрому долгосрочному росту или быстрому краткосрочному росту.

Исследование выполнено за счет гранта Российского научного фонда № 23-28-01404, https://rscf.ru/project/23-28-01404.

ЛИТЕРАТУРА

1. СПАРК. Система сервисов по оценке рисков и обеспечению экономической безопасности бизнеса [Электронный ресурс]. – Режим доступа: http://www.spark-interfax.ru/, свободный (дата обращения: 13.01.2023).

2. Халафян А.А. Теория вероятностей, математическая статистика и анализ данных: основы теории и практика на компьютере. Statistica. Excel / А.А. Халафян, В.П. Боровиков, Г.В. Калайдина. – М.: URSS, 2016. – 317 с.

УДК 336.71

НЕОБАНКИ В РОССИИ: ПРЕДПОСЫЛКИ ВОЗНИКНОВЕНИЯ И ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ

А.А. Захарова, студентка каф. экономики

Научный руководитель А.Д. Извекова, доцент каф. экономики

г. Томск, ТУСУР, dolly5764@rambler.ru, anna.d.izvekova@tusur.ru

Рассмотрены перспективы реформации кредитных учреждений, предпосылки возникновения необанков. Проанализированы его отличия от традиционного финансового института, а также выделены критерии отнесения банка к категории необанков. Рассмотрены особенности функционирования, достоинства и недостатки необанков.

Ключевые слова: необанк, традиционный банк, цифровой банкинг, дистанционный доступ, модель банка.

В настоящее время происходит существенный прогресс в сфере банковского дела. Применение новых технологий направлено на

удобство не только со стороны клиентов и простоту в обслуживании, но и оптимизацию деятельности и комфорта в работе самих банков.

За счет популяризации различного вида цифровых технологий в последние годы в России наблюдается стабильный рост использования физическими и юридическими лицами дистанционных каналов обслуживания. Так, по данным Центрального банка на начало 2022 г., на территории Российской Федерации были открыты уже 321 млн счетов в различных банках с дистанционным доступом (рис. 1).

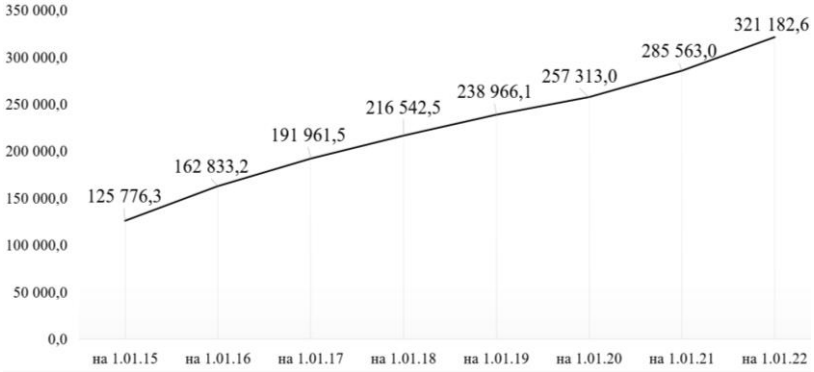


Рис. 1. Количество счетов с дистанционным доступом, открытых в кредитных организациях в РФ, тыс. ед. [1]

Исходя из представленного графика, можно сделать вывод, что в период с 2015 по 2022 г. число счетов с дистанционным доступом, открытых на начало года в кредитных организациях, неуклонно росло. Делая прогноз, можно также отметить, что данное количество с каждым годом будет только увеличиваться, так как такие счета имеют удобства в плане открытия, произведения операции и закрытия из любой точки мира в любом банке, в котором только есть такая возможность.

Для определения дальнейших тенденций в развитии банковской деятельности стоит отметить, какие типы и модели банков существуют на данный момент.

В настоящий момент существуют 2 модели банков: традиционные и необанки (онлайн-банки, цифровые банки). Необанк работает только в интернете и исключает необходимость предоставления финансовых услуг через физическое присутствие клиента в филиалах банка. Эту модель можно рассматривать как противоположность существующей традиционной модели, поскольку она полностью суще-

ствует в виртуальном пространстве, используя современные цифровые технологии.

На конец 2021 г. во всём мире существовало 319 действующих необанков, и по прогнозам экспертов их количество будет только возрастать [3].

Основные отличия традиционного банка и необанка представлены на рис. 2.

Традиционные банки	Необанки
Точкой начала взаимодействия с клиентом, как правило, является офис	Точкой начала взаимодействия с клиентом является сайт или приложение банка
Цифровые сервисы являются продолжением сервисов филиала, где обслуживается клиент	Цифровые сервисы находятся в центре модели обслуживания клиента независимо от филиала. Взаимодействие с клиентами осуществляется дистанционно
Более высокая стоимость обслуживания	Более низкая стоимость обслуживания
Продукты и сервисы стандартизированы	Продукты и сервисы более индивидуальны
Клиенты менее подвержены угрозам электронной безопасности в обычных банковских операциях	Клиенты могут существенно подвергаться угрозам электронной безопасности
Пример: Газпромбанк	Пример: Тинькофф

Рис. 2. Отличия традиционного банка и необанка [2]

Банки будущего, или необанки, должны соответствовать следующим основным критериям.

– Отсутствие офисов. Большинству клиентов уже сейчас не нужны офисы, так как они имеют доступ к различным услугам банков с любых устройств отовсюду и всегда.

– Самостоятельный онлайн-банк, осуществляющий деятельность на основе лицензии Банка России, либо посредническая организация, не имеющая лицензии Банка России, но помогающая онлайн-банку в финансовых операциях.

– Сокращение штата сотрудников. Машина с искусственным интеллектом способна сделать быстрее и качественнее работу с большим количеством данных, отсюда вытекает отсутствие потребности в некоторых сотрудниках и сокращение штатов сотрудников.

– Изменение клиентской базы. Банки будут обслуживать не только людей, но и интернет вещей.

– Использование квантовых вычислений. Квантовые алгоритмы способны обнаруживать мошенничества, кибератаки и различные технические сбои, выявлять манипуляции, эффективно составлять стратегии против них, также они способны вычислять риски при покупке актива.

Перечень предоставляемых услуг необанками и традиционными банками практически одинаковый. Основной особенностью и достоинством является снижение затрат на создание такого банка, но помимо достоинств есть и недостатки. Сравнительная характеристика представлена на рис. 3.

Достоинства	Недостатки
Минимум затрат на строительство, ремонт главного офиса и филиалов	Издержки на создание и внедрение приложений и специализированных программ, а также значительные затраты на разработку и внедрение надежной защиты от кибермошенников
Документооборот онлайн	При проблеме на сервере, работа со счетом и документами может остановиться на неопределенный период
Ведение и управление операциями по счету в удобное время, в удобном месте	Большие первоначальные вложения средств для развития необанка
Отсутствие очередей	Низкий уровень финансовой грамотности населения
Быстрота и легкость контроля за состоянием счета в режиме онлайн	
Конфиденциальность	
Доступность	

Рис. 3. Достоинства и недостатки необанков [4]

Какие же организации на территории Российской Федерации можно уже сейчас отнести к необанкам? К банкам данного сегмента можно отнести, например, Тинькофф Банк, Рокетбанк, Touch Bank, Точка банк и др.

Основные особенности российских необанков в сравнении с зарубежными заключаются в следующих аспектах:

– Зарубежные необанки работают на платной подписке с пробным бесплатным периодом длительностью один месяц, в то время как российские работают бесплатно, но с дополнительной подпиской, обеспечивающей определенные привилегии клиентам.

– Использование голосовых ассистентов для управления счетом без входа в само приложение. В российской практике такое отсутствует по причине слабого развития биометрии.

– Общие счета для накоплений, т.е. счета к которым клиенты могут подключиться и совместно копить деньги. Такие счета существуют в российской опыте, но в большинстве случаев только для юридических лиц [5].

Российский необанкинг с каждым годом набирает обороты и развивается, внося собственные клиенто-ориентированные технологии.

Заключение. Современный мир постоянно развивается, а вместе и с ним и банковская сфера. За последние годы в данную область бы-

ло внесено много различных технологических новшеств. В связи с прогрессивным развитием этих новшеств были созданы банки, не похожие на то, что было, – необанки. Использование технологических инноваций и отказ от традиционных отделений и филиалов предоставляет необанкам много преимуществ по сравнению с традиционными банками. Самые главные преимущества необанков заключаются в способности быстро реагировать на потребности рынка и предлагать финансовые услуги быстрее и удобнее для пользователя. Низкие эксплуатационные расходы дают им возможность предлагать клиентам выгодные условия обслуживания по сравнению с традиционными банками.

ЛИТЕРАТУРА

1. Статистика национальной платежной системы [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/statistics/nps/psrf/ (дата обращения: 11.04.2022).

2. Стратегия современного банка в эпоху цифровых сервисов [Электронный ресурс]. – Режим доступа: https://www.finversia.ru/publication/strategiya-sovremennogo-banka-v-epokhu-tsifrovykh-servisov-27091 (дата обращения: 15.04.2022).

3. Необанк – новый тренд на мировом финансовом рынке [Электронный ресурс]. – Режим доступа: https://internationalwealth.info/all-about-fintec/neobank-novyy-trend-na-mirovom-finansovom-rynke/ (дата обращения: 30.04.2022).

4. Необанк как новое направление финансовых инноваций в Российской Федерации [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/neobank-kak-novoe-napravlenie-finansovyh-innovatsiy-vrossiyskoy-federatsii (дата обращения: 13.05.2022).

5. 6 практик зарубежных необанков, которые улучшат опыт пользователей России [Электронный ресурс]. – Режим доступа: https://markswebb.ru/blog/foreign-neobanks-practices/ (дата обращения: 14.05.2022).

ПОДСЕКЦИЯ 5.4

ПРОЕКТНЫЙ МЕНЕДЖМЕНТ И ЕГО ИСПОЛЬЗОВАНИЕ В ЦИФРОВОЙ ЭКОНОМИКЕ

*Председатель – **Афонасова М.А.**, зав. каф. менеджмента, д.э.н., проф.;*
*зам. председателя – **Богомолова А.В.**, доцент каф. менеджмента, декан ЭФ, к.э.н.*

УДК 331.08

ОСОБЕННОСТИ ПРИМЕНЕНИЯ «МЕТОДА А» ПРИ ОРГАНИЗАЦИИ ПОИСКА, ПОДБОРА, ОТБОРА И НАЙМА ПЕРСОНАЛА В IT-КОМПАНИЮ

И.В. Бершанская, А.А. Мисяченко, студенты каф. менеджмента
Научный руководитель А.П. Молодых, ассистент каф. менеджмента
г. Томск, ТУСУР, anna.p.molodykh@tusur.ru

Рассмотрен метод системной организации процесса поиска, подбора, отбора, набора кандидатов на вакантные должности в IT-компанию для привлечения высокопрофессиональных специалистов с внешнего рынка труда.
Ключевые слова: набор персонала, методы отбора персонала, HR-служба.

Поиск релевантных кандидатов на современном рынке труда достаточно обширен, поскольку исключает локализацию специалистов в ограниченном радиусе проживания. На данный момент многие IT-компании сумели перестроить традиционные модели взаимодействия и коммуникации сотрудников на гибридный режим, когда часть команды сосредоточена в офисе, а часть работает онлайн. Поэтому при такой системе организации бизнеса наём персонала является важнейшим условием эффективной деятельности в высококонкурентной IT-сфере.

При организации полного цикла поиска, подбора, отбора и найма подходящего для должности кандидата IT-компании зачастую обращаются к «Методу А». Данный метод ориентирован на выявление и привлечение исключительно талантливых высококлассных специали-

стов своей профессиональной ниши – A-players, которые с вероятностью 90% имеют шанс добиться высоких результатов, доступных лишь для 10% подходящих кандидатов [1]. Использование «Метода А» подразумевает чётко структурированный системный подход и включает в себя пять этапов рекрутинга: открытие вакансии, sourcing, проведение собеседований, оффер, 90 day review.

На этапе открытия вакансии для должности заполняются 3–8 конкретных, измеримых и достижимых параметров, грейдированных в приоритетном порядке, при выполнении которых будет возможно оценить степень достижения индивидуальных целей сотрудника, учтённых в общей системе каскадирования целей OKR. Таким образом, вновь созданная вакансия будет внедрена в организационную структуру компании с позиции достижения требуемых от исполнителя результатов. Также для новой должности непосредственному руководителю необходимо определить полный функционал деятельности сотрудника, сформировать и утвердить профиль кандидата, базовый набор компетенций, после чего передать запрос тимлиду рекрутингового отдела. Рекрутер, в свою очередь, проведёт бенчмаркинг по аналогичным вакансиям на рынке, определит «вилку» заработной платы и условия для успешного найма и, наконец, зациклит процесс, согласовав параметры с заказчиком – руководителем отдела, куда требуется сотрудник.

На этапе Sourcing ответственный за набор по данной вакансии рекрутер размещает информацию на общедоступных популярных интернет-площадках, тем самым создаёт фокусированный поиск кандидатов. Площадками для поиска кандидатов в IT-компанию могут быть, к примеру, hh.ru, career.habr.com, vc.ru/job, ingamejob.com/ru/jobs, github.com, huntflow.ru и др. По мере откликов на вакансию рекрутер осуществляет выборку соответствующих требованиям компании резюме.

Собеседование с кандидатами осуществляется в несколько последовательных регламентированных этапов. Как правило, на первом этапе – Topgrading interview – рекрутер на онлайн-встрече сначала ориентирует претендента на должность по основным предложениям и требованиям компании, при этом считывая определённые в ответах специалиста характеристики. Один из комплексных методов собеседования на данном этапе – метод «Who?», на котором задаются наиболее весомые и конкретные вопросы, касающиеся прошлых опытов работы. Например, «Для чего вас наняли на предыдущее место работы и как оценивали успех?»; «Каким достижением вы больше всего гордитесь?»; «Какие были не самые лучшие моменты во время

вашей предыдущей работы?»; «Как бы вы оценили свою команду по шкале A-B-C?»; «Какие изменения вы произвели?»; «Почему вы ушли с прошлого места работы?» и т.п. Рекрутер в интервью с кандидатом проводит анализ соответствия ценностям компании, проверяет возможность достижения заявленным OKR, выясняет, был ли кандидат ТОП-перформером, выявляет ключевую мотивацию в деятельности. Также обязательно обращает внимание на «Push/Pull», «Boss rating», «Red flags» по соответствующим метрикам. По окончании встречи рекрутер вносит как положительные, так и отрицательные характеристики кандидата в карту оценки.

На втором этапе собеседований – Focused interview – помимо рекрутера с кандидатом встречаются непосредственный руководитель и члены команды для оценки компетенций (например, по методу STAR), а также технических и(или) аналитических навыков кандидата, лидерских качеств, умения работать в команде, добиваться поставленных результатов и др. В некоторых случаях, в зависимости от должности, кандидату будет необходимо предоставить рекомендации от коллег или подтвердить свои профессиональные умения в момент собеседования. К примеру, от претендента на должность бизнес-тренера требуется проведение демо-тренинга, а от IT-специалиста – выполнение тестовых заданий. Перед оценивающим рекрутером на данном этапе стоят следующие вопросы: «Имеет ли кандидат 90% и выше шансов достичь результата?»; «Соответствует ли кандидат миссии и компетенциям более чем на 90%?». Результаты собеседования также фиксируются в карте оценки кандидата со стороны рекрутера и присутствующих на интервью руководителя и членов команды.

На этапе выбора кандидата и формирования выгодного предложения (оффера) демонстрируется возможность для подходящего кандидата расти в уровне профессионализма, раскрыть свой потенциал, участвовать в реализации амбициозных целей.

Завершающим этапом набора является мониторинг кандидата по методу «90 day review», где в течение трёх месяцев обязательного испытательного срока руководителем определяется, верно ли был подобран сотрудник на должность. После анализа параметров деятельности и степени достижения OKR принимается окончательное решение касательно работы конкретного специалиста в компании.

Для найма и набора сотрудников в IT-сфере «Метод А» может являться наиболее эффективным, так как предоставляются полные сведения о возможностях, эффективности и приверженности к корпоративной культуре компании соискателя и их соответствие индивидуальным характеристикам конкретного специалиста.

ЛИТЕРАТУРА

1. «Метод А» для найма персонала: сайт «HR-академия» [Электронный ресурс]. – URL: https://hr-academy.ru/templates/who-smart-r.pdf (дата обращения: 01.03.2023).

УДК 04.9

ФОРМИРОВАНИЕ СТРАТЕГИИ РЕГИОНАЛЬНОЙ ЭКСПАНСИИ МАРКЕТПЛЕЙСОВ

И.В. Федорова, студентка каф. УИ

Научный руководитель О.В. Гальцева, доцент каф. УИ, к.т.н.

г. Томск, ТУСУР, ira.fedorova.0101@mail.ru

Изучено формирование стратегии региональной экспансии маркетплейсов. Представлены этапы развития и формирования, а также классификация российских и зарубежных маркетплейсов и их влияние на способы заключения сделок и тренды рынка. Показано, как влияет инновационный и трансформационный подход посредством искуственного интеллекта на электронную коммерцию России и других стран.

Ключевые слова: маркетплейсы, экспансия, рынок, конкуренция, организация.

Нынешний ритейл характеризуется возникновением электронных платформ, дозволяющих реализовывать куплю-продажу продуктов и услуг в сети вместе с поддержкой электронных платежей, а также компании доставки. Данная оценка более конкретно описывает интернет-магазины. Но на рынке электронной коммерции стремительно формируются подобные игроки типа маркетплейсов. За последние годы их часть на рынке составляет 62% сравнительно со стандартными интернет-магазинами. Потребители желают приобретать более комфортный сервис с приемлемыми условиями.

Актуальность состоит в том, что маркетплейсы считаются наиболее активными платформами со стороны развития. Реферальные проекты, а также рекламные инструменты станут ключевым конкурентоспособным преимуществом уже после скорости доставки, а также обширного перечня продукции. С целью изучения темы применяются соответствующее способы: исследование отечественных и иностранных источников, сопоставление бизнес-моделей, мониторинг динамики рынка, синтез академических концепций, способ экспертных оценок, моделирование.

Многознаменательное основание популярной и известной бизнес-модели сопряжено с возникновением классифайдов. В русском сегменте данная форма именовалась доской объявлений. Следующим шагом формирования модели стало возникновение предметных мар-

кетплейсов. Этому поспособствовала потребность распределения объявлений согласно категориям с целью упрощения поиска. Первым маркетплейсом в этом варианте, в котором в настоящее время общепринято рассматривать маркетплейсы, считался американский Amazon. В русской истории основным маркетплейсом является Ozon, который формировался согласно виду маркетплейса Безоса.

Вследствие большого количества условий западные рынки очень различаются от отечественного рынка электронной коммерции. В случае если в западных рынках имеется постоянный лидер, проявивший себя за десятки лет – Amazon, то в русском – за последние годы наблюдается большая конкурентная борьбы среди маркетплейсов.

Взгляды специалистов сходятся в том, что пандемия проявила значительное воздействие на рынок электронной коммерции Российской Федерации.

Уже после внезапного увеличения рынок не прекращает совершенствоваться, а также в настоящее время маркетплейсы обладают большим числом разных стратегий последующего роста. Основными двигающими мощностями всемирного рынка электронной коммерции являются интернет-магазины, а также маркетплейсы.

Важным является рассмотрение понятий маркетплейсов различными экспертами в области электронной торговли и как они менялись по ходу изменения этой модели. Таблица демонстрирует изменение понятия «маркетплейс».

Развитие понятия «маркетплейс»

Автор	Год	Определение
J.Y. Bakos	1991	Межорганизационная информационная система, позволяющая покупателям и продавцам обмениваться информацией о ценах и предложениях товаров
N.P. Archer	2000	Виртуальная рыночная площадка
E. Christiansee	2002	Посредник, который использует ИТ-возможности и правила ведения бизнеса для стимулирования межорганизационных взаимоотношений в определенной индустрии
M. Grieger	2003	Уникальная виртуальная площадка, которая собирает многочисленных продавцов и покупателей на одной виртуальной рыночной площадке
R. Stockdale	2004	Межорганизационная информационная система
W. Zheng	2006	Виртуальный информационный посредник, встроенный в промышленную сеть
V. Choudhury	2015	Инфраструктура, позволяющая участникам встречаться и осуществлять рыночные транзакции
О.М. Куликова	2020	Бизнес-модель, объединяющая продавцов и покупателей, совершающих сделки посредством онлайн-платформы

Тщательно проанализировав определения, выведено заключение, что маркетплейс в качестве бизнес-модели осуществил продолжительный, а также полномасштабный ход изменения от информационной концепции с целью обмена данными. Имеется ряд каналов дистрибуции в сети интернет. Немаловажно осознать, в каких существует маркетплейс, выявить его роль в любом из них. Кроме того, имеется систематизация маркетплейсов согласно видам участников. Модель B2C анализирует прямое вовлечение бизнеса и неравноправные взаимоотношения сторон. Яркими образцами такого рода модели считаются Aliexpress, Российская Федерация, Airbnb, Юлмарт и прочие компании.

Исторически доски объявлений миновали систематический ход собственных изменений, дойдя до той степени развития, что представлен в настоящем времени. В этот период можно отметить 2 категории маркетплейсов – многоцелевые и предметные. Главная значимость, которая наблюдается в абсолютно всех видах маркетплейсов, состоит в наличии значительного объема сведений – касательно товаров, продавцов, методов совершения сделок.

Розничный онлайн-экспорт в Российской Федерации считается стратегически значимой составляющей русской электронной коммерции. Data Insight вместе с eBay выполнили аналитику, и оказалось, то что размер рынка увеличился на 31%. Из числа крупных отечественных маркетплейсов прослеживается тенденция: Yandex.Магазин захватывает лидирующую позицию согласно темпам подъема, равно как Wildberries показывается первенство по увеличению размера продаж в абсолютных значениях.

Еще одно направление, прослеживаемое на рынке, – уменьшение ниши. Ритейлеры начали понимать достоинства специализации в определенной группе, а также в кратчайший период наибольшее число интернет-магазинов станут превращаться в нишевые. На рынке стремительно формируется явление социальной коммерции. Это сопряжено не только с тем, что пользователей перенаправляют в интернет-магазин с социальных сетей. Зерокодинг не считается явным трендом вместе с точки зрения покупателя, однако для промышленности этот подход считается иннновационным и трансформационным. Вместе с поддержкой зерокодинга возникает шанс привести в действие интернет-магазин без программирования, что гарантирует облегчение входа в e-commerce. Искусственный интеллект продолжительное время считается трендом в рамках многих индустрий, а также рынков. Его способности дают возможность автоматизировать почти все механические функции, а также персонализировать предложения.

Известные маркетплейсы работают на территории всей России, некоторые из них стабильно распространяют свои отделения в зарубежных странах. Большая их часть сфокусирована на увеличении количества продуктов, расширении списка категорий товаров. С появлением маркетплейса или его продукта в новом регионе возрастает сложность компании в её организации. Для большего удовлетворения спроса на рынке и активного освоения территории при учете особенностей региона появляется нужда в децентрализации.

Важной частью экспансии региона становится рост фармакологической категории на маркетплейсах.

Для последующего этапа экспансии необходим учет региональных и культурных особенностей. Например, погодные условия, особенности языка, отраслевые рынки. Непродуманная стратегия развития за счет особенностей региона может не дать развиться бизнесу.

Таким образом, маркетплейсы являются основной частью рынка электронной коммерции в Российской Федерации. Зарождение и развитие трендов помогают трансформации рассмотренной бизнес-модели. В рамках такого бизнеса могут быть осуществимы разные варианты региональной экспансии. Как научная новизна исследования экспансии интерес дает возможность развития системы для разработки стратегии выхода в новый регион для растущей бизнес-модели маркетплейс, где объектом исследования будет выступать бизнес-модель маркетплейс при экспресс-доставке товаров и услуг.

ЛИТЕРАТУРА

1. Бородин В.А. Перспективы формирования электронной торговли // Организация и управление: проблемы и решения. – 2017. – С. 126–128.

2. Бочкова Е.В. Анализ рынка интернет-торговли в РФ и за рубежом // Вестник ИрГТУ. – 2014. – № 10. – С. 225–229.

3. Ергунова О.Т. Маркетинг территории. – Екатеринбург: Изд-во Урал. ун-та, 2018. – 135 с.

4. Зайнетдинов Э. 30 бизнес-процессов, которые изменятся из-за искусственного интеллекта [Электронный ресурс]. – URL: https://hype.ru/deecrypto-store-club/30-biznes-processov-kotorye-izmenyatsya-iz-za-iskusstvennogo-intellekta-dkvza585 (дата обращения: 13.02.2023).

5. Иванова Е. Важнейшие тренды eCommerce в 2019 году [Электронный ресурс]. – Режим доступа: https://new-retail.ru/business/e_commerce/vazhneyshie_trendy_ecommerce_v_2019_godu4695/ (дата обращения: 09.03.2023).

6. Корешков В.А. Региональная экспансия ритейла в России // Интеллект. Инновации. Инвестиции. – 2011. – № 3. – URL: https://cyberleninka.ru/article/n/regionalnaya-ekspansiya-riteyla-v-rossii-kak-faktor-formirovaniya-v-nem-slozhnyh-organiaztsionnyh-struktur (дата обращения: 01.03.2023).

УДК 027.7:005.8-047.44

АНАЛИЗ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ВУЗОВСКИХ БИБЛИОТЕК НА ОСНОВЕ ДАННЫХ ФОРУМА «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА #СЛЕДУЙЗАНАМИ»

И.В. Котова, аспирант каф. менеджмента
Научный руководитель М.А. Афонасова, зав. каф. менеджмента, д.э.н., проф.
г. Томск, ТУСУР, kirina2302@mail.ru

Рассматриваются вопросы развития университетских библиотек, реализации новых направлений работы за счет участия в проектной деятельности. Приведены примеры проектной деятельности университетских библиотек, их цели и задачи.
Ключевые слова: персонал, проектная деятельность, библиотечные инновации, университетские библиотеки.

В последние годы университетские библиотеки стали принимать активное участие в различных конкурсах, проектах, консорциумах с целью получить грант и финансирование [1]. Основная задача библиотечных проектов – создание новых сервисов, услуг, форматов работы с пользователями, расширение ресурсной базы, реализация социокультурной деятельности [2].

Вопросы развития вузовской библиотеки, ее интеграции в вузовскую среду, создание новых форматов работы и т.д. обсуждались на форуме «Университетская библиотека #следуйзанами» [3]. Отдельная площадка форума была посвящена проектной деятельности, где было представлено 12 проектов университетских библиотек из г. Томска, Омска, Красноярска, Астрахани и других городов (таблица).

Описание проектов

№ п/п	Название	Университет	Цели
1	*2*	*3*	*4*
1	Дорога знаний	Томский государственный университет	Продвижение ресурсов и услуг библиотеки с помощью геймификации
2	Час куратора #времябиблиотеки	Томский политехнический университет	Поиск новых форматов работы со студентами, погружение первокурсников в физическое и информационное пространство библиотеки
3	The Library// Пространство, которое можно менять...	Сибирский государственный медицинский университет	Реорганизация пространства, оптимизация процесса обслуживания читателей

Продолжение таблицы

1	*2*	*3*	*4*
4	«Мюсли Канта»	Омский государственный университет путей и сообщения	Организация культурно-образовательного пространства: культурное развитие студентов, развитие творческого потенциала студентов
5	Клуб книго-путешествий	Сургутский государственный педагогический университет	Новые формы социально-культурных коммуникаций в информационно-образовательном пространстве
6	Редкий фонд #выходимзарамки	Томский политехнический университет	Совместная деятельность с библиотеками, музеями, архивами по продвижению культурного наследия. Привлечение широкого круга пользователей
7	Библиотека я тебя слышу. Школа	Омский государственный технический университет	Поддержка лиц с нарушениями слуха, социализация детей старшего школьного возраста, новые форматы обслуживания
8	Электронно-образовательный ресурс	Астраханский государственный университет	Объединение электронных ресурсов библиотеки на одной платформе, создание цифровой среды для интеграции ресурсов вузов Каспийского региона
9	Хранилище приоткрывает двери	Томский государственный университет	Новые способы взаимодействия с пользователями, повышение видимости фонда в информационном пространстве
10	Красная книга объектов культурного наследия Алтайского края	Алтайский государственный педагогический университет	Сохранение историко-культурного наследия Алтайского края. Привлечь внимание к состоянию объектов, мотивирование к деятельности по спасению памятников
11	Ректорский читальный зал	Байкальский государственный университет	Организация нового пространства и формирование уникальных коллекций редких изданий
12	«SpeakEnglish»	Сибирский федеральный университет	Создание языкового клуба для адаптации иностранных студентов и практики общения на иностранном языке учащихся общеобразовательных школ

Представленные проекты можно разделить на следующие группы, решающие общие задачи:

– организация новых форм работы с читателем – проекты 1, 2, 4, 5, 7, 9, 12;

– продвижение ресурсов – 1, 2, 6, 8, 9;

– изменение пространства – 3, 4, 11;

– культурно-просветительская деятельность – 4, 5, 6, 10.

О реализации проектов, их успешности и результатах можно узнать из материалов форума [3].

Таким образом, проектная деятельность направлена на решение основных задач университетских библиотек, управление проектами становится их необходимой деятельностью, в результате чего расширяются компетенции и профессиональные навыки сотрудников.

ЛИТЕРАТУРА

1. Григорьева Н.Е. Проектная деятельность в университетской библиотеке: достижения, поиски, перспективы // Динамика библиотечно-информационного обеспечения образования, науки и культуры: матер. Всерос. науч.-практ. конф., Омск, 10–11 ноября 2020 г. – Омск: Омский гос. техн. ун-т, 2020. – С. 61–66 [Электронный ресурс]. – URL: https://www.elibrary.ru/item.asp?id=44204937 (дата обращения: 18.02.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

2. Кирнос А.А. Проектная деятельность библиотек / А.А. Кирнос, Г.А. Кулюпина // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности: матер. VI Междунар. науч. конф., Донецк, 26–28 октября 2021 га. – Т. 11. – Донецк: Донец. Нац. ун-т, 2021. – С. 128–130 [Электронный ресурс]. – https://www.elibrary.ru/item.asp?id=47289177 (дата обращения: 18.02.2023) (дата обращения: 18.02.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

3. Университетская библиотека #следуй за нами : форум, 12–16 окт. 2020 г., Томск. – URL: https://lib.tpu.ru/ntb-120 (дата обращения: 19.02.2023).

УДК 330.101.542

ПРОБЛЕМЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОГРАММ ПОДДЕРЖКИ МАЛОГО БИЗНЕСА В ТОМСКОЙ ОБЛАСТИ

О.Р. Малашонок, студент магистратуры

Научный руководитель В. Н. Жигалова, доцент каф. менеджмента

г. Томск, ТУСУР, ef@tusur.ru

На сегодняшний день субъекты малого бизнеса заслуживают особой поддержки и тщательного внимания. В совокупности все эти небольшие организации обеспечивают огромную часть экономики всей страны. Во времена различных кризисных ситуаций государ-

ство опирается в большей степени на эту систему, так как она способствует сглаживанию колебаний. В исследовании в рамках статьи представлена модель механизма оценки эффективности программ поддержки малого бизнеса. Отражена необходимость создания методического подхода оценки эффективности программ поддержки малого бизнеса, так как существующее множество групп критериев не обладает стабильной системностью.
Ключевые слова: малый бизнес, поддержка малого бизнеса, эффективность программ, оценка эффективности программ.

В настоящее время современная рыночная экономика определяет направления к повышению интереса органов национальной власти к оценке эффективности их деятельности, а также к анализу социально-экономических характеристик. Особое внимание органов власти повышается к методам и средствам оценки эффективности поддержки малого бизнеса, поскольку малым предприятиям отводится центральная роль в реализации социально-экономических задач страны.

На пути формирования и развития малого бизнеса стоят многочисленные проблемы. Так, например, одной из актуальных проблем являются административные барьеры, которые в дальнейшем приводят к длительному принятию решений из-за сложной структуры и противоречивости нормативно-правовой базы. Специалисты назвали процедуры, вызывающие у малых предпринимателей некоторые трудности в Томской области, такие как:

– лицензирование;
– регистрация определенных изделий;
– прохождение конкурентных процедур (торгов, тендеров);
– субсидирование;
– аттестация рабочих мест;
– возмещение затрат на открытие бизнеса;
– налоговая отчетность [1].

Регулярные изменения в законодательстве Российской Федерации, в свою очередь, создают сложности в прохождении административных процедур. В связи с этим у субъектов малого бизнеса возрастают риски совершения ошибок, что впоследствии может повлечь за собой административную ответственность. Также в ряде проблем малого бизнеса необходимо выделить ограниченный доступ к получению государственных и муниципальных заказов, поскольку выстоять в конкурсной борьбе с крупными организациями значительно сложнее, чем с аналогичными.

Для полного раскрытия темы необходимо рассмотреть понятие механизма оценки эффективности программ поддержки малого биз-

неса, которое в свое время является организованной системой экономических процессов, состоящей из совокупности институциональных факторов, обеспечивающих органам власти достижение заданных результатов в поставленных временных рамках [2].

Комплексный методический подход оценки эффективности государственной поддержки малого бизнеса ориентирован на выполнение следующих задач:

– увеличение объёмов производства организаций;
– обеспечение занятости населения;
– создание новых и сохранение рабочих мест на предприятиях;
– увеличение налоговых поступлений в бюджет государства;
– развитие инновационной деятельности предприятий;
– поддержание конкурентной среды.

В рамках исследования предлагается использовать модель механизма оценки эффективности программ поддержки малого бизнеса, которая представлена на рис. 1.

Рис. 1. Модель механизма оценки эффективности программ поддержки малого бизнеса

В исследовательских работах предлагаются разнообразные наборы критериальных показателей для оценки результативности и эффективности программ поддержки малого бизнеса. Однако большая доля показателей отличается незначительными вариантами. Следовательно, невзирая на наличие огромного числа критериев в научных трактатах, комплексная система таких показателей, которая была бы пригодна для управления, до сих пор не была создана.

В заключение хотелось бы отметить о необходимости создания комплексного методического подхода оценки эффективности программ поддержки малого бизнеса, так как имеющееся множество групп показателей не обладает общей системностью, которая позволила бы использовать её в основе универсального инструмента для будущего анализа эффективности программ поддержки малого бизнеса.

ЛИТЕРАТУРА

1. Исследование состояния и тенденций развития малого и среднего предпринимательства Томской области [Электронный ресурс]. – Режим доступа: https://www.kolpadm.ru/upload/files/doc/2021/issledovanie_sostoyanij_i_tendentsij_razvitiya_msp.pdf (дата обращения: 20.02.2023).

2. Быкова Н.В. Оценка эффективности государственной поддержки малого предпринимательства, 2018 [Электронный ресурс]. – Режим доступа: https://disser.spbu.ru/files/2018/disser_bykova_n_v.pdf (дата обращения: 01.03.2023).

УДК 338

ПРАВОВОЕ РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТ В 2023 ГОДУ: ОСНОВНЫЕ ТЕНДЕНЦИИ

М.С. Лапин, В.С. Мордвинов, студенты

Научный руководитель М.А. Афонасова, зав. каф. менеджмента

г. Томск, ТУСУР

Рассматривается актуальная тема правового регулирования криптовалют в 2023 г. В работе представлен обзор правовых мер, которые уже приняты или находятся в процессе разработки в разных странах мира. Дана оценка существующих вызовов и проблем, которые возникают при регулировании криптовалют, а также представлены тенденции и направления развития правового регулирования в мире.

Ключевые слова: криптовалюты, правовое регулирование, законодательство, криптовалютная экономика, проблемы, тенденции, направления развития, регулирование ICO, криптовалютные биржи.

В последние годы криптовалюты и блокчейн-технологии стали все более популярными во всем мире. Однако в связи с новизной дан-

ной технологии возникла необходимость в правовом регулировании криптовалютных операций и сделок. В 2023 г. это остается одной из самых актуальных тем в мире экономики и права.

Цель данной статьи – проанализировать существующее правовое регулирование криптовалют в разных странах мира, определить тенденции и направления развития правового регулирования криптовалют в мире, оценить роль правительств и регуляторов в развитии правового регулирования криптовалют и выявить проблемы и риски данного регулирования.

Анализ данных вопросов позволяет подойти к решению вопроса прогнозирования развития правового регулирования криптовалют в 2023 г. и определить необходимость в дальнейшем развитии правового регулирования криптовалют в мире.

Обзор существующих правовых мер в разных странах. В настоящее время правовое регулирование криптовалютных операций и сделок различается в разных странах мира. Некоторые страны уже приняли законодательные акты и создали регуляторы, которые регулируют криптовалютные операции, в то время как в других странах этот вопрос до сих пор остается не решенным.

Практика регулирования криптовалют отличается в разных странах. Например, США имеют целый ряд законов в этой сфере, а в штате Нью-Йорк существуют лицензионные требования [1].

В Европейском союзе осуществляется регулирование на уровне стран-членов [2].

Китай запретил криптовалютные операции, а Япония стала одной из первых стран, которые приняли законодательные акты по этому вопросу [3, 4].

Швейцария уже создала правовую базу, а в России криптовалюты регулируются несколькими законами [5, 6].

Некоторые другие страны также работают над созданием правовых актов, регулирующих криптовалютные операции, например, Австралия, Канада и Индия [7–9].

Следует отметить, что в некоторых странах, таких как Бразилия и Южная Корея, криптовалютные операции по-прежнему находятся в серой зоне [10, 11].

Регулирование криптовалют и блокчейн-технологий остается сложной темой в правовом регулировании, однако с каждым годом все больше стран принимают законодательные акты.

Тенденции и направления развития правового регулирования криптовалют в мире. Развитие правового регулирования криптовалют в разных странах привело к появлению нескольких общих тенденций и направлений. Создание инфраструктуры для контроля и

надзора за криптовалютными операциями становится одной из главных тенденций. В различных странах это включает создание специальных регуляторов, лицензирование платформ для криптовалютных операций и разработку систем для отслеживания и регулирования криптовалютных операций. Разработка стандартов и правил для криптовалютных операций также становится важным направлением с установлением правил для идентификации пользователей, защиты данных и финансовой стабильности. Регулирование Initial Coin Offerings (ICO) также становится приоритетом для многих стран, чтобы предотвратить мошенничество и риски для инвесторов.

Мировое правовое регулирование криптовалют развивается в нескольких направлениях. В некоторых странах, таких как США и Канада, ICO регулируются как ценные бумаги, в других – существуют специальные правила для ICO. Введение налогов на криптовалютные операции также становится распространенной практикой. Стабильные монеты, связанные с реальными активами, получают все большую популярность, и многие страны уже начали их регулировать. Общая тенденция направлена на обеспечение безопасности и стабильности криптовалютных операций и установление четких правил и стандартов для криптовалютных проектов.

В заключение можно сказать, что правовое регулирование криптовалют в мире продолжает развиваться и совершенствоваться. Многие страны уже приняли или находятся в процессе разработки законодательства, регулирующего криптовалютные операции, ICO и другие аспекты криптовалютной экономики.

Однако на данный момент существует значительная разница между законодательствами разных стран, что может привести к неравномерному регулированию криптовалют в глобальном масштабе. Поэтому важно продолжать работу в этом направлении, чтобы обеспечить единообразное правовое регулирование криптовалют и сделать их более доступными и безопасными для использования.

Кроме того, необходимо учитывать, что правовое регулирование криптовалют является достаточно новым явлением и, возможно, будут появляться новые вызовы и проблемы, которые потребуют новых решений и правил. Однако благодаря работе законодательных органов и регуляторов, можно ожидать, что криптовалюты станут более стабильными и надежными в будущем, что создаст условия для их успешного развития и использования.

ЛИТЕРАТУРА

1. Global legal insights [Электронный ресурс]. – Режим доступа: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa#:~:text=Sales%20regulation,-Back%20to%20top&text=The%20sale%

20of%20cryptocurrency%20is,MSB%E2%80%9D)%20under%20Federal%20law. (дата обращения: 06.03.2023).

2. Regulation of the European parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [Электронный ресурс]. – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 (дата обращения: 06.03.2023).

3. Bloomberg [Электронный ресурс]. – Режим доступа: https://www.bloomberg.com/news/articles/2022-10-10/china-s-crypto-founders-test-government-limits-with-xi-s-industry-restrictions#:~:text=%E2%80%9CCrypto%20transactions%20and%20crypto%20services,kind%20are%20banned%20in%20China (дата обращения: 06.03.2023).

4. The Japan times [Электронный ресурс]. – Режим доступа: https://www.japantimes.co.jp/news/2023/01/04/business/tech/japan-crypto-2022-review-regulation-future/ (дата обращения: 06.03.2023).

5. Regulated United Europe [Электронный ресурс]. – Режим доступа: https://rue.ee/crypto-regulations/switzerland/ (дата обращения: 06.03.2023).

6. КонсультантПлюс [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 06.03.2023).

7. Cryptocurrency in Australia – Statistics & Facts [Электронный ресурс]. – Режим доступа: https://www.statista.com/topics/8519/cryptocurrency-in-australia/ (дата обращения: 10.01.2023).

8. Government of Canada [Электронный ресурс]. – Режим доступа: https://www.canada.ca/en/revenue-agency/news/newsroom/tax-tips/tax-tips-2023/cryptocurrency.html (дата обращения: 10.01.2023).

9. Forbes Advisor [Электронный ресурс]. – Режим доступа: https://www.forbes.com/advisor/in/investing/cryptocurrency/crypto-bill/ (дата обращения: 10.01.2023).

10. Brazilian President Signs Bill Creating Crypto Regulations [Электронный ресурс]. – Режим доступа: https://www.competitionpolicyinternational.com/brazilian-president-signs-bill-creating-crypto-regulations/#:~:text=The%20regulatory%20framework%20included%20in,%E2%80%9Cvirtual%20service%20provider%E2%80%9D%20license (дата обращения: 10.01.2023).

11. Crypto Travel Rule in South Korea by The Financial Services Commission (FSC) [Электронный ресурс]. – Режим доступа: https://notabene.id/world/south-korea#:~:text=1.,legal%20tender%20in%20South%20Korea. (дата обращения: 13.01.2023).

УДК 338.465.4

ПОВЫШЕНИЕ ПРИВЛЕКАТЕЛЬНОСТИ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ В СОЦИАЛЬНЫХ СЕТЯХ

Н.С. Берликова, Н.А. Черногодова, К.А. Щербинина,
студентки каф. менеджмента
Научный руководитель Н.П. Прудникова, ассистент каф. менеджмента
Проект ГПО менеджмента-2201. Использование инструментов коммуникаций для поддержания имиджа и конкурентоспособности учебного подразделения вуза
г. Томск, ТУСУР, nadya.berlikova@mail.ru, nadezhda.chernogodova@mail.ru, chsherbinina_k@mail.ru

Рассматривается применение социальных сетей для продвижения образовательных услуг. Рассмотрены социальные сети как инструмент повышения привлекательности образовательных услуг, характерные особенности составления стратегии продвижения сообществ вузов в «ВКонтакте», а также проведен анализ полученных результатов.

Ключевые слова: образовательные услуги, социальные сети, стратегия продвижения, сообщество, контент-план.

В настоящее время социальные сети являются неотъемлемой частью коммуникации между людьми и организациями, в связи с чем всё больше образовательных учреждений используют социальные сети для повышения привлекательности своих услуг и их продвижения. Они создают сообщества на различных интернет-сервисах, где формируют информационное поле для достижения маркетинговых целей.

Многие университеты создают группы «ВКонтакте», однако они оказываются невостребованными из-за неэффективной стратегии продвижения.

Цель статьи: рассмотреть социальные сети как инструмент повышения привлекательности образовательных услуг и дальнейшего их продвижения. Для реализации цели были поставлены следующие задачи:

– выявить проблемы сообществ университета и структурных подразделений в социальной сети «ВКонтакте»;

– разработать основные пункты стратегии продвижения;

– оценить стратегию продвижения на примере сообщества «Кафедра менеджмента ТУСУР»;

– провести анализ полученных результатов.

В первую очередь были выявлены проблемы ведения сообществ образовательных организаций.

1. Нерегулярность размещения контента. Большинство групп «ВКонтакте» и не только образовательных учреждений не соблюдают временные рамки размещения постов и не имеют четкого графика публикаций. Из-за чего теряется коммуникация между сообществом и подписчиками.

2. Отсутствие взаимодействия с аудиторией. При ведении социальных сетей многие публикуют информацию без инструментов вовлечения (опросы, комментарии, розыгрыши). В результате аудитория теряет интерес к контенту сообщества и покидает его.

3. Однообразие контента. Сообщества образовательных учреждений размещают информацию только об учебном процессе. Данный вид контента является полезным, но не удерживает интерес подписчиков.

Все эти проблемы приводят к невостребованности групп вузов и их структурных подразделений.

На основе этих проблем были разработаны основные пункты стратегии продвижения образовательных услуг в социальных сетях.

Учитывая целевую аудиторию образовательных сообществ, необходимо отобрать темы, которые в дальнейшем будут освещаться в сообществе. Исходя из выбранных тем, разрабатывается контент-план, включающий в себя различные виды контента. Важно использовать информацию не только об учебном процессе, но и освещать другие стороны деятельности студентов. Например, полезные советы об учебе, события и новости университета, интервью со студентами, выпускниками и сотрудниками вуза. Контент-план должен вовлекать аудиторию и повышать взаимодействие с ней. Также необходимо составить и соблюдать график выхода постов.

Немаловажным фактором является оформление сообщества и создание уникального дизайна. При оформлении сообщества необходимо расписать информацию о том, чем полезна группа и что в ней можно узнать. А благодаря современному дизайну складываются позитивные ассоциации с брендом и повышается лояльность аудитории. Он должен быть связан с корпоративным дизайном вуза или структурного подразделения.

Вышеперечисленные пункты специализируют стратегию для продвижения образовательных услуг в социальных сетях.

Большинство российских вузов находятся в сложной ситуации из-за новых форматов взаимодействия с абитуриентами и необходимости набора абитуриентов. Не все старые форматы коммуникации

эффективны в последние годы. Необходимо использовать современные коммуникационные технологии. Также со временем абитуриенты становятся все более требовательными к информации и мероприятиям, проводимым вузами.

Активное сообщество создаст основу для продвижения образовательных услуг кафедры. Информационные посты и статьи о направлении обучения не только помогут в профориентации студентам кафедры, но и помогут абитуриентам с выбором будущей профессии.

В представлении абитуриентов/студентов современное образование – это, в первую очередь, получение конкурентоспособных преимуществ, а уже во вторую очередь – знания.

Можно сделать вывод о том, что современный рынок образовательных услуг становится примером потребительского рынка. Данный факт необходимо использовать в маркетинговой коммуникации вуза со школами, абитуриентами и их родителями.

Маркетинговый подход анализа ассортимента вуза или кафедры позволяет выявить и удовлетворить запросы потребителей (абитуриентов), а также содействует улучшению имиджа и значимости высшего образования в обществе и умах потребителей.

Подобная специализированная стратегия продвижения была применена к сообществу «Кафедра менеджмента ТУСУР» (рис. 1).

Рис. 1. Сообщество «Кафедра менеджмента ТУСУР»

Таким образом, было создано наполненное информационное поле, в котором присутствуют все сведения о направлениях обучения, специальностях кафедры и их особенностях, а также развлекательный контент, связанный с ними. Благодаря активной группе, студенты-бакалавры, обучающиеся на кафедре менеджмента, могут узнать о магистерских программах и продолжить обучение на кафедре. Абитуриенты также могут посетить сообщество и, увидев полную информацию, сделать выбор в пользу образовательных услуг кафедры менеджмента ТУСУР.

В течение полугода количество подписчиков увеличилось на 47% с момента начала ведения группы. Охват в среднем составил 7627 человек, что на 7278 человек больше, чем до применения стратегии. Посещаемость сообщества увеличилась на 1033 человека.

Научная новизна работы заключается в создании специализированной стратегии продвижения для образовательных учреждений в социальных сетях.

Показатели эффективности характеризуют успешность разработанной стратегии продвижения. Ее применение способствует повышению привлекательности вуза и позволяет более эффективно продвигать его образовательные услуги.

ЛИТЕРАТУРА

1. Оценка эффективности вуза в социальных сетях [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/otsenka-effektivnosti-prodvizheniya-vuza-v-sotsialnyh-setyah (дата обращения: 4.03.2023).

2. Как проанализировать целевую аудиторию «ВКонтакте» за 5 шагов – стартапы, бизнес, технологии [Электронный ресурс]. – URL: https://vc.ru/marketing/171835-kak-proanalizirovat-celevuyu-auditoriyu-vkontakte-za-5-shagov (дата обращения: 10.11.2022).

3. Составляем матрицу контента, рубрикатор и контент-план для постов и статей: Site Elite Studio – digital [Электронный ресурс]. – URL: https://st-lt.ru/blog/useful/sostavlyaem-matriczu-kontenta.html (дата обращения: 10.11.2022).

4. Сообщество кафедры менеджмента, ТУСУР: Социальная сеть «ВКонтакте» [Электронный ресурс]. – URL: https://vk.com/kafmanager (дата обращения: 10.11.2022).

УДК 338

ПРОЕКТНЫЙ МЕНЕДЖМЕНТ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ УПРАВЛЕНИЯ БИЗНЕСОМ

У.В. Капранова, Е.А. Мальцева, А.А. Терентьева,
студентки каф. менеджмента
Научный руководитель М.А. Афонасова, д.э.н., проф.
г. Томск, ТУСУР, u_kapranova-17@mail.ru, ktrrrnmmlt@gmail.com, STerentieva03@yandex.ru

Рассмотрены сущность и роль проектного менеджмента. Показаны особенности и преимущества данного вида управления современными компаниями.

Ключевые слова: проектный менеджмент, управление, эффективность.

В настоящее время проектный менеджмент является хорошо зарекомендовавшим себя методом организации и управления производством, современными компаниями. Проектный менеджмент направлен на достижение определенных, четко поставленных целей, он универсален и применим практически во всех областях и сферах деятельности. Проектный менеджмент предполагает использование различных методов, средств, технологий для достижения требуемого результата. Он позволяет обеспечивать рациональное планирование, учитывающее множественные риски и неопределенности, реализовать в полной мере потенциал проектной команды.

Проектный менеджмент – это методология, применяющая современные научные методы для достижения оптимальных результатов с точки зрения стоимости, времени и качества, а также для достижения успеха при удовлетворении всех потребностей участников проекта.

Деятельность современных предприятий (организаций) представляет собой непрерывное выполнение определенных функций (операций) и проектов. Главное отличие между операционной и проектной деятельностью заключается в том, что стандартные операции выполняются постоянно и повторяются, в то время как каждый проект уникален и реализуется в течение ограниченного времени.

Целью проектного менеджмента является получение необходимого результата в заданные сроки и с заданным качеством. Каждый проект имеет конкретную цель, которую нужно достичь с соблюдением сроков и не выходя за рамки установленного бюджета.

Большинство работающих на рынке компаний используют технологии и методы традиционного менеджмента, при котором достаточно трудно собрать качественную проектную команду из действующих сотрудников, привыкших работать в традиционной обстановке и выполнять стандартные операции. В данном случае выходом из си-

туации будет являться привлечение участников проектной команды «со стороны».

Одним из инструментов обеспечения эффективности управления бизнесом как раз является использование принципов проектного управления. Именно проектный менеджмент позволяет обеспечить гибкость и адаптивность системы управления, ее быструю реакцию на изменения внешней среды, что является важным фактором успеха в бизнесе [1].

Управление проектом можно считать эффективным, если:

- достигнуты конечные результаты, соответствующие поставленной цели;
- конечные результаты удовлетворяют потребности заказчика.

Под эффективностью менеджмента следует понимать некую характеристику результативности деятельности команды управленцев, которая отражается и проявляется в конечных показателях деятельности управляемой системы.

Эффективность системы управления проектами – это степень достижения поставленных перед командой проекта целей при минимальных, но необходимых затратах. В данном случае результаты соотносятся с затратами системы в целом, включая производственные затраты, коммерческие и административно-управленческие расходы [2].

Анализ опыта успешных предприятий свидетельствует о переходе их к проектному управлению в условиях роста динамичности и неопределенности среды, что позволяет им быстрее адаптироваться к новым вызовам и изменениям, происходящим во внутренней и внешней среде.

Таким образом, проектное управление представляет собой эффективный инструмент управления современными бизнес-структурами, который обеспечивает не только высокую степень открытости и прозрачности планирования и достижения результатов, но и позволяет более рационально распределять ресурсы, оценивать поставленные задачи, стимулировать проектную команду, укладываться в намеченные сроки, выходить на планируемые показатели эффективности бизнеса.

ЛИТЕРАТУРА

1. Михайлов А.А. Проектный менеджмент как инструмент реализации программ импортозамещения в российской авиационной промышленности / А.А. Михайлов, А.А. Комова // Московский экономический журнал. – 2019. – № 1 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/proektnyy-menedzhment-kak-instrument-realizatsii-programm-importozamescheniya-v-rossiyskoy-aviatsionnoy-promyshlennosti, свободный (дата обращения: 15.03.2023).

2. Стешин А.И. Современные подходы в проектном управлении: учеб. пособие / А.И. Стешин, М.В. Мирославская, В.А. Стешин. – СПб.: Балт. гос. техн. ун-т, 2020. – 80 с.

ПОДСЕКЦИЯ 5.5

СОВРЕМЕННЫЕ СОЦИОКУЛЬТУРНЫЕ ТЕХНОЛОГИИ В ОРГАНИЗАЦИИ РАБОТЫ С МОЛОДЕЖЬЮ

*Председатель секции – **Орлова В.В.**, зав. каф. ФиС, директор НОЦ «СГТ», д.соц.н.;*
*зам. председателя – **Корнющенко-Ермолаева Н.С.**, ст. преп. каф. ФиС*

УДК 303.022

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОНЛАЙН-КУРСОВ ПО СИСТЕМНОМУ АНАЛИЗУ И ПРОГРАММ ВУЗОВ

П.Г. Букина, С.Г. Букина, студентки каф. БИС
Научный руководитель А.С. Колтайс, ст. преп. каф. ЭБ
Проект ГПО ЭБ-2301. Разработка электронного курса по профессии «Системный аналитик»
г. Томск, ТУСУР, bukina.polina2014@gmail.com

Рассматриваются популярные онлайн-курсы по системному анализу и направления томских университетов, проводится их сравнение с целью выявления пользы данных программ.
Ключевые слова: высшее образование, онлайн-обучение, системный анализ, онлайн-курсы.

Онлайн-образование набирает популярность, особенно после пандемии. Только за время пандемии оборот онлайн-школ увеличился почти в 2,5 раза, большинство школ – стартапы [1]. Среди молодежи идет тенденция к уменьшению значимости высшего образования, поскольку отсутствует желание учиться несколько лет, когда курсы предлагают освоить профессию за год или несколько месяцев. По данным Министерства науки и высшего образования РФ, общая численность поступивших студентов за 7 лет уменьшилась в 1,3 раза, а выпущенных – в 1,5 раза [2]. Целью данной статьи является выявление пользы программ курсов и вузов после сравнения с профессиональным стандартом.

Были рассмотрены курсы по системному анализу следующих платформ: GetAnalyst, Яндекс Практикум, ASAP Education,

GETIT.ACADEMY [3-6]. В табл. 1 представлены стоимость и длительность каждого курса.

Таблица 1

Сравнение программ онлайн-курсов по длительности и стоимости

	GetAnalyst	Яндекс Практикум	ASAP Education	GETIT.ACADEMY
Длительность, мес	3	8	4	4
Стоимость, руб.	70 000	102400	70 000	32 700

Был проведен анализ на соответствие программ курсов трудовым функциям, указанным в профессиональном стандарте [7], результат представлен в табл. 2. Знак «~» означает освоение одной или нескольких задач трудовой функции, «+» – функция осваивается, «–» – функция не осваивается.

Таблица 2

Сравнение программ онлайн-курсов с профессиональным стандартом системного аналитика

Код	GetAnalyst	Яндекс Практикум	ASAP Education	GETIT.ACADEMY
A/01.04	+	+	~	–
A/02.04	+	+	~	–
A/03.04	~	~	–	+
A/04.04	–	+	–	~
A/05.04	–	–	~	–
A/07.04	+	+	~	+
A/08.04	~	~	–	–
A/09.04	–	+	–	–
A/11.04	+	+	–	–
A/13.04	~	~	–	~
A/14.04	~	~	~	~
B/04.5	~	~	–	~
B/05.5	–	–	~	–
B/10.5	–	–	–	–
B/11.5	–	–	–	~
B/13.5	+	+	–	–
B/14.5	~	–	–	–

Результаты анализа таковы: курс от Яндекс Практикума позволяет освоить чуть меньше половины компетенций, курс от GetAnalyst – лишь треть основных функций, другие два курса компетенции практически не формируют.

Далее будут рассмотрены программы следующих вузов: ТГУ, ТПУ и ТУСУР [8–11]. В табл. 3 представлено сравнение учебных программ вузов по длительности и стоимости.

Таблица 3

Сравнение учебных программ вузов по длительности и стоимости

	ТГУ, 09.03.03	ТПУ, 09.03.02	ТУСУР, 27.03.03	ТУСУР, 10.05.04
Длительность	4 года	4 года	4 года	5,5 лет
Стоимость, руб.	675000	680000	600000	840000

В табл. 4 представлено аналогичное сравнение программ с профессиональным стандартом.

Таблица 4

Сравнение программ томских университетов с профессиональным стандартом системного аналитика

Код	ТГУ, 09.03.03	ТПУ, 09.03.02	ТУСУР, 27.03.03	ТУСУР, 10.05.04
A/01.04	–	–	+	+
A/02.04	–	–	+	+
A/03.04	+	+	+	+
A/04.04	+	+	+	+
A/05.04	+	+	+	+
A/07.04	+	+	+	+
A/08.04	~	~	~	~
A/09.04	~	~	~	~
A/11.04	~	~	+	+
A/13.04	+	+	~	+
A/14.04	+	+	~	+
B/04.5	+	+	+	+
B/05.5	+	+	+	+
B/10.5	–	–	–	–
B/11.5	–	~	–	+
B/13.5	+	+	+	+
B/14.5	–	–	–	+
C/03.6	+	+	+	+
C/07.6	+	+	+	+

Таким образом, учебные программы университетов города Томска, косвенно связанные с системным анализом, превосходят программы онлайн-курсов, обучающих профессии системного аналитика. Длительность обучения в вузе в 4 раза превышает длительность онлайн-курсов, но при этом студент осваивает компетенции в степени, позволяющей трудоустроиться еще при обучении.

ЛИТЕРАТУРА

1. Онлайн-образование и коронавирус: как развивается рынок? | EdMarket [Электронный ресурс]. – Режим доступа: https://edmarket.ru/blog/coronavirus/, свободный (дата обращения: 18.02.2023).

2. Сведения о приеме, численности студентов и выпуске специалистов образовательных организаций, осуществляющих образовательную деятельность по образовательным программам высшего образования [Электронный ресурс]. – Режим доступа: https://minobrnauki.gov.ru/opendata/9710062939-svedeniya-o-prieme-chislennosti-studentov-i-vypuske-spetsialistov-obrazovatelnykh-organizatsiyakh-os, свободный (дата обращения: 18.02.2023).

3. Курс «Системный аналитик» – обучение по системному анализу – Яндекс Практикум [Электронный ресурс]. – Режим доступа: https://practicum.yandex.ru/systems-analyst/, свободный (дата обращения: 20.02.2023).

4. Программа курса «Системный аналитик: с нуля до опыта работы на проекте» [Электронный ресурс]. – Режим доступа: https://getanalyst.ru/education/systems-analyst-start-program?ysclid=lezsr7v6qi802721702, свободный (дата обращения: 20.02.2023).

5. Курсы системного аналитика для начинающих, обучение системных аналитиков – ASAP Education – офлайн-обучение digital и it в Томске [Электронный ресурс]. – Режим доступа: https://asapeducation.ru/course/systems-analyst/?ysclid=lezsvb7v1q560419133, свободный (дата обращения: 20.02.2023).

6. Программа курса «Базовый курс по системному анализу» GETIT.ACADEMY [Электронный ресурс]. – Режим доступа: https://getit.academy/imodul?ysclid=lf2uqp3lck965966633, свободный (дата обращения: 22.02.2023).

7. Приказ Минтруда России «Об утверждении профессионального стандарта «Системный аналитик» [Электронный ресурс]. – Режим доступа: https://fgosvo.ru/uploadfiles/profstandart/06.022.pdf?ysclid=lf2tysef67609474520, свободный (дата обращения: 22.02.2023).

8. Учебный план по направлению «Прикладная информатика» профиля «Прикладная информатика» ТГУ [Электронный ресурс]. – Режим доступа: https://www.tsu.ru/upload/iblock/d19/gooqbuq1b8jtkyl0o7blp4lbo3enssb5/UP_09.03.03_Prikladnaya_informatika_PI_2020_na_zamenu.pdf, свободный (дата обращения: 22.02.2023).

9. Учебный план по направлению «Информационные системы и технологии» профиля «Информационно-аналитические системы и технологии в бизнесе» ТПУ [Электронный ресурс]. – Режим доступа: https://up.tpu.ru/view/all.html?id=26169, свободный (дата обращения: 22.02.2023).

10. Учебный план по направлению «Системный анализ и управление» ТУСУР [Электронный ресурс]. – Режим доступа: https://abiturient.tusur.ru/ru/napravleniya-podgotovki/ochnaya-forma-obucheniya/2023-27-03-03-sistemnyy-analiz-i-upravlenie-fulltime-5b4ddfe6-a1f8-4282-bcb1-135fc89c4626, свободный (дата обращения: 22.02.2023).

11. Учебный план по направлению «Информационно-аналитические системы безопасности» профиля «Информационная безопасность финансовых и экономических структур» ТУСУР [Электронный ресурс]. – Режим доступа:

https://abiturient.tusur.ru/ru/napravleniya-podgotovki/ochnaya-forma-obucheniya/2023-10-05-04-informatsionno-analiticheskie-sistemy-bezopasnosti-fulltime-57aa5509-5763-4413-9745-e47071c1c2d6, свободный (дата обращения: 22.02.2023).

УДК 101.1:316

РОЛЬ СОВРЕМЕННОГО МОЛОДЕЖНОГО ЛИДЕРА В МЕДИАСФЕРЕ

А.В. Булыгина, студентка каф. ФиС

Научный руководитель М.Ю. Раитина, доцент каф. ФиС, д.филос.н.

г. Томск, ТУСУР, neftieleon@yandex.ru

Рассматриваются подходы к пониманию молодежного лидера, типология и функции лидерства; медиасфера и способы реализации деятельности молодежного лидера, влияние, оказываемое лидером на молодежную аудиторию.

Ключевые слова: молодежный лидер, медиасфера, видеоблогер, блогер, молодежная аудитория.

Изучение молодежного лидера в медиасфере и его деятельности актуально, так как блогеры оказывают значительное влияние на формирование мнения, ценностей у молодежной аудитории. Изучение феномена блогинга и блогеров помогает предостеречь разрушение социальных институтов, насаждение деструктивных паттернов поведения, манипуляции общественным мнением, и также дает возможность применения методов, оказывающих позитивное влияние на молодежную аудиторию.

Целью данной работы является изучение роли и влияния молодежного лидера в медиасфере на молодежную аудиторию.

Исторически термин «лидер» появился в XIII в. в английском языке и использовался в значении «вожак», «глава». Тем самым обозначается главная особенность лидера – направление других людей. Г. Тард определил подражание лидеру как основной закон социальной жизни, М. Вебер создал идею харизматического лидера, основываясь на системе компенсации неполноценности за счет приобретаемой власти, З. Фрейд выделил влияния «вытесненного» на становление лидером [1]. Платон выделял 3 типа лидеров, основываясь на их положении в социальной иерархии и исполняемых функциях. М. Вебер разработал типологию авторитета, которая широко распространена в наше время [2]. На основе вышеперечисленных работ сформировались основные функции лидера: организационная, конструктивная, координационная и интегративная.

В литературе российских авторов феномен лидерства изучался преимущественно с точки зрения психологии и политики, где существует система доминирования и подчинения.

Отметим, что сегодня медиасфера является непосредственным полем деятельности современных молодежных лидеров, блогеров. Однако научное сообщество не дает четкого определения медиасферы. Опираясь на характерные особенности, можно сказать, что она является частью четырех сфер общественной жизни и непосредственно связана с ними [3]. Например, информация может выступать как вспомогательный элемент в духовном развитии личности – самореализации и самоактуализации. Существует философия медиа, занимающаяся рефлексией понятийных проблем в СМИ, медиаполитика, реализующая продвижение политических идей в массы. Главной спецификой является медиатекст, понимаемый как язык, на котором распространяется информация и происходит коммуникация в медиасфере [4]. Он обладает характерными особенностями: ориентация на массовую аудиторию, потоковое производство информации, ее одноразовость, открытость для комментирования и интерпретирования, мультимедийность и медийность. Таким образом, медиасфера – это совокупность идей, мнений, мыслей, которые представлены в виде медиатекста с присущими ему особенностями.

В медиасфере свою деятельность реализуют блогеры, проявляющие себя как лидеры и собирающие вокруг себя многотысячную аудиторию. Термин «блогер» в современном мире имеет аналогичное значение, что и лидер мнения, а именно, человек, который отличается в глазах своих последователей высоким социальным статусом и информированностью [5]. Блогеры занимаются производством контента в социальных сетях и виртуальных площадках, например Youtube.

Классификацию блогеров можно представить следующим образом: лайфстайл блогеры, летсплейщики, бьютиблогеры, техноблогеры, новостные блогеры, кинообзорщики, музыкальные блогеры [6]. Они выполняют следующие функции: коммуникативную, развлекательную, функцию самопрезентации и сплочения. На основе исследования «Hello bloggers» можно сделать вывод о среднем российском блогере – это девушка в возрасте от 25 до 34 лет, живущая в Москве, Санкт-Петербурге, ведущая канал на Youtube с 2014, 2015 или 2016 г., с доходом 95 тыс. руб. в месяц, с высшим образованием, состоящая в браке или отношениях, бездетная [7].

• Блогеры и видеоблогеры, имея огромную молодежную аудиторию и обладая авторитетом в молодежной среде, оказывают на фор-

мирование общественного мнения молодежи как негативное, так и позитивное влияние.

• Остановимся на иллюстрации позитивного влияния видеоканала для молодежи, – например, видеоблогинг «Слово пацана», который помогает людям, попавшим в трудную жизненную ситуацию, повысить их нынешний уровень жизни. Людям предоставляют возможности, которые можно как использовать, так и проигнорировать, тем самым видеоблогеры не навязывают свою волю, но и дают возможность проявить себя, изменить свою жизнь к лучшему. Кроме того, на канале поднимается тема низкого уровня жизни пенсионеров, погибающих деревень и отношений между малоимущими гражданами и государством. Таким образом, данные видеоблогеры затрагивают не только личные проблемы людей, но и масштабные, проявляющиеся на государственном уровне, являются способом реализации благотворительности в медиасфере посредством пожертвований от их аудитории.

• В рамках исследования была выдвинута гипотеза «молодые люди склонны доверять мнению видеоблогера, не учитывать личность видеоблогера, которая может влиять на субъективное и острое восприятие тех или иных явлений и событий» и проведен опрос с целью выяснения, доверяют ли молодые люди молодежным лидерам среди студентов томских университетов, молодых людей в возрасте от 18 до 25 лет и более. На основе ответов респондентов был сделан следующий вывод: гипотеза была подтверждена не полностью – респонденты интересуются личностью видеоблогера и блогера, но в большей мере склонны доверять видеоблогеру и блогеру, что является негативной тенденцией, так как в ответах часто появлялись имена медийных лиц, представляющих отрицательный пример влияния молодежного лидера в медиасфере на молодежную аудиторию.

Подводя итог, можно сказать, что молодежные лидеры реализуют свою деятельность в новой среде – медиасфере, обладая большим влиянием на молодежную аудиторию, формируя общественное мнение и модели поведения. Таким образом, изучение данной темы нацелено на формирование мнения молодежи и позитивных моделей ее поведения, а также предупреждение разрушения социальных институтов общества и предотвращение моральной деградации молодежи.

ЛИТЕРАТУРА

1. Абашкина Е.Б. О теориях лидерства в современной политической психологии / Е.Б. Абашкина, Ю.И. Косолапова // США: экономика, политика, идеология. –1993. – № 4. – С. 13–21.

2. Вебер М. Харизматическое господство // Социол. исслед. – 1998. – № 5. – С. 139–143.

3. Дебре Р. Введение в медиалогию. – М.: Праксис, 2010. – 368 с.
4. Кузьмина Н.А. Современный медиатекст: учеб. пособие. – Омск: Полиграф. центр «Татьяна», 2011. – 414 с.
5. Лидеры мнений [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Лидер_мнения, свободный (дата обращения: 12.02.2023).
6. Блог [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Блог, свободный (дата обращения: 12.02.2023).
7. Hello blogger [Электронный ресурс]. – Режим доступа: https://helloblogger.ru (дата обращения: 12.02.2023).

УДК 32.019.52

УЧАСТИЕ МОЛОДЕЖИ В ПОЛИТИЧЕСКОЙ ЖИЗНИ СОВРЕМЕННОЙ РОССИИ: ПРОБЛЕМЫ И ОСОБЕННОСТИ

Б.И. Черемисина, студентка каф. ФиС
Научные руководители: М.Ю. Раитина, доцент каф. ФиС, д.филос.н.; Н.С. Корнющенко-Ермолаева, ст. преп. каф. ФиС
г. Томск, ТУСУР, cheremisina.2003@mail.ru

Рассматриваются проблемы политического абсентеизма молодежи, а также причины и формы активного участия в политике молодого поколения.
Ключевые слова: политическое участие, митинг, молодёжь, абсентеизм.

Сегодня молодежь выступает не просто как демографическая категория, но и как ключевой стратегический ресурс страны, поскольку именно молодежь воплощает ведущие идеи и инициативы, определяет будущее социально-экономического и технического развития. В целом политическое участие граждан в современной России – достаточно противоречивое явление, которое зависит от множества факторов: осведомленности о политической жизни страны, доверия к государственному аппарату, интересу к политике и т.п. Стоит отметить, что большой вклад в расстановку политических сил вносит старшее поколение не только из-за своей численности, но также и из-за участия в выборах и референдумах. Но как на данный вопрос влияет молодежь? К сожалению, мы приходим к неутешительным выводам и можем наблюдать пассивность и незаинтересованность в политической жизни среди молодого поколения.

Для того чтобы разобраться в данном вопросе, необходимо изучить особенности положения молодёжи как социальной и демографической группы в политической жизни страны, а также определить

причины, по которым молодёжь поддерживает митинги и протестные акции.

Для рассмотрения данной проблемы необходимо выделить следующие термины. *Политическое участие* – действия, которые социальные субъекты совершают для того, чтобы повлиять на то, как будет функционировать политическая система [1]. *Политический абсентеизм* – уклонение или неучастие граждан страны в политической жизни. В вопросе, связанном с положением молодежи в политической жизни современной России, необходимо затронуть тему демографии, а именно рассмотреть демографическую пирамиду.

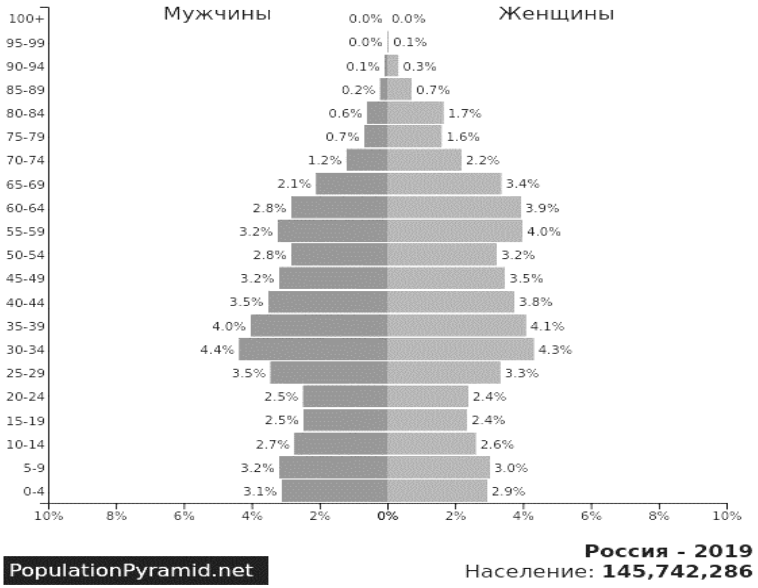


Рис. 1. Демографическая таблица за 2019 г.

В приведенной демографической пирамиде можно отметить много демографических ям, повторяющихся с промежутком 25 лет (рис. 1) [2]. Исходя из данной статистики, можно сказать, что молодое поколение немногочисленно. Молодое поколение ассоциируется с «завтрашним днём», а точнее с будущим и прогрессом. Но обращая внимание на статистику, можно сказать, что для влияния на политические процессы нужно апеллировать к 40-летним гражданам страны, так как они являются самой многочисленной демографической группой. Чтобы влияние молодежи было заметнее, её численно должно стать существенно больше.

Обратимся к политическому аспекту, а именно к участию в выборах. На графике можно заметить, что поколение 65+ стабильно участвует в выборах, нежели молодое поколение (рис. 2) [2]. Можно отметить, что в определенные годы уровень явки у молодого поколения проседает, и вследствие того, что молодёжь мало участвует в политике путём выборов, без неё принимаются политические решения.

Таким образом, можно заключить, что положение молодежи на политической арене очень шаткое и неустойчивое, так как, во-первых, молодежь находится в демографической яме и ее численности не хватает для принятия политических решений. Во-вторых, это непостоянное участие в политике, особенно в выборах.

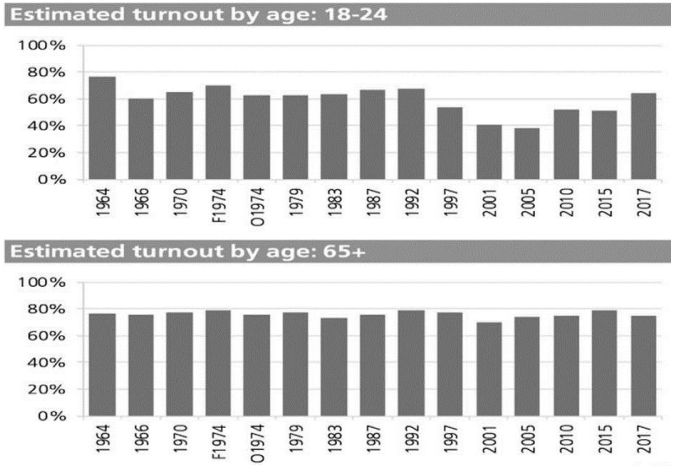


Рис. 2. Таблица участия в выборах молодежи и старшего поколения

Почему молодёжь обращается к протестам и митингам? Поколение молодёжи обладает сильным протестным потенциалом, зачастую выражает свою готовность к радикальным мерам. Для данной социальной группы характерен такой аспект, как обостренное чувство несправедливости и яркая эмоциональная окраска жизненных событий. Это является катализатором для того, чтобы противостоять власти. Также благодаря данному аспекту молодое поколение зачастую не может аргументировать свои политические взгляды, а основывается лишь на чувствах.

За счёт эмоциональной подвижности и неустойчивости молодого поколения его можно легко подвести к протестным проявлениям за счёт многих аспектов. Следует выделить причины их формирования: протестная журналистика, которая формирует нелицеприятный облик

власти [3]. Действие таких источников влияет на дезорганизацию общества и обостряет конфликт между поколениями.

Интернет-ресурсы и социальные сети. С помощью социальных сетей многие оппозиционные силы распространяют информацию, тем самым формируя общественное недовольство. Задачей организаторов протестов является показ массовости события, и для этого они привлекают молодёжь. Для данной социальной группы характерен аспект самоидентификации, потому что в это время человек ищет своё место в этом обществе, стране, мире, среди разных социальных групп, и политический протест – это одна из форм, в которой можно высказать своё мнение [3]. К причинам отнесем интерес и желание узнать о том, как проходят митинги, а также экономические и социальные вопросы [4]. К сожалению, не каждого гражданина устраивает, как работает система и её институты. Так происходит и с молодёжью, которая наблюдает за ситуацией в стране сквозь собственную призму представлений о том, как было бы идеально, и поэтому начинает активные действия в более агрессивном виде политического участия – протесте.

Несовпадение с собственными политическими ожиданиями. Также стоит сказать, что у многих есть установка «изменить» [4]. Например, изменить жизнь в стране, изменить политическую систему и тому подобное. Но здесь следует отметить, что дальнейшей аргументации такого подхода нет, поскольку молодые люди сами не представляют, что конкретно они хотят изменить. И в этом случае большую роль играет эмоциональный аспект, поскольку конкретных и конструктивных решений зачастую не предлагается.

Нередко среди причин протестных проявлений выступает **получение выгоды** [5]. Такие случаи в последние несколько лет стали очень распространены. Благодаря социальным сетям и сети Интернет, оппозиционным и иным организациям стало легче искать молодёжь и привлекать её для участия в протестных акциях. Если аргументы недостаточно убедительны, то в таких случаях используют некое «вознаграждение» за явку на митинг/протест, что является инструментом манипуляции, поскольку зачастую молодёжь остро нуждается в финансовых средствах.

Таким образом, подводя итоги, мы можем сказать, что к причинам, по которым молодёжь выбирает протестные акции, относятся: провокации оппозиционных журналистов и СМИ; интернет-ресурсы и социальные сети, благодаря которым распространяется информация о предстоящих политических протестах; факторы самоидентификации; экономические и социальные вопросы; желание защиты своего мнения и принятия самостоятельных решений; внешняя политика; несов-

падение с собственными политическими ожиданиями; желание быть причастным к протесту; интерес к тому, как проходят выборы. Вышесказанное инициирует актуальную потребность в политической интеграции молодежи, важность формирования гражданского самосознания и активной гражданской позиции с целью стабилизации российского общества.

ЛИТЕРАТУРА

1. Белоногова Е.К. Политическое участие в современной России // Вести научных достижений. – 2020. – № 9. – С. 27–30.
2. Смена поколений и политическое поведение: кто делает современное политику – молодые или старшие? [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=Lz2VKjyQAew&ab_channel (дата обращения: 11.02.2023).
3. Андреев А.И. Молодежь, патриотизм и протесты: краткий анализ и некоторые предложения // Инновационный потенциал молодежи: информационная, социальная и экономическая безопасность: матер. Междунар. молодеж. науч.-исслед. конф.; Екатеринбург, 4–5 декабря 2017 г. – Екатеринбург: УрФУ, 2017. – С. 3–10.
4. Аринина К.И. Абсентеизм в политике: причины и последствия [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/absenteizm-v-politike-prichiny-i-posledstviya/viewer (дата обращения: 08.02.2023).
5. Молоткова Е.М. Причины политического абсентеизма молодежи и пути его минимализации [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/prichiny-politicheskogo-absenteizma-molodezhi-i-puti-ego-minimizatsii/viewer (дата обращения: 11.02.2023).
6. Распоряжение Правительства Российской Федерации от 29.11.2014. № 2403-р «Об утверждении Основ государственной молодежной политики Российской Федерации на период до 2025 года».
7. Конституция Российской Федерации от 12.12.1993 // Официальный интернет-портал правовой информации. – 2020 г. – Ст. 31 с изм. и доп. в ред. от 01.07.2020.
8. Конституция Российской Федерации от 12.12.1993 // Официальный интернет-портал правовой информации. – 2020 г. – Ст. 32 с изм. и доп. в ред. от 01.07.2020.
9. Алмонд Г.А. Гражданская культура и стабильность демократии / Г.А. Алмонд, С. Верба [Электронный ресурс]. – Режим доступа: http://www.civisbook.ru/files/File/1992-4-Almond_Verba.pdf (дата обращения: 08.02.2023).
10. Васильева Е.И. Мотивы и ценностные доминанты протестов в оценках лидеров протестных акций и молодежи / Е.И. Васильева, Т.Е. Зерчанинова [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/motivy-i-tsennostnye-dominanty-protestov-v-otsenkah-liderov-protestnyh-aktsiy-i-molodezhi/viewer (дата обращения: 10.02.2023).

УДК 167.1

ЧЕЛОВЕК В МИРЕ ТЕХНИКИ: АКТУАЛЬНЫЕ ВОПРОСЫ И ОСОБЕННОСТИ

А.Д. Левит, студент каф. КУДР

Научный руководитель М.Ю. Раитина, доцент каф. ФиС, д.филос.н.

г. Томск, ТУСУР, levit.aleesandra@mail.ru

Рассмотрены некоторые вопросы взаимодействия философии, техники, человека и общества.

Ключевые слова: человек, общество, философия техники, технический прогресс, технологическая сингулярность.

Сегодня в мире информационных технологий и всеобщей цифровизации вопросы отношения человека и техники становятся особенно актуальными и своевременными. Как известно, философия техники зародилась в середине XIX в. в Германии как новая возможность понять и осмыслить возможности научно-технического прогресса [1]. Термин «философия техники» иногда может привести к заключению, что в данном разделе происходит анализ техники. Но так ли это на самом деле?

Сегодня такие разделы, как «Философия искусства», «Философия науки», «Философия природы», «Философия техники» рассматриваются скорее, как исторические формы философского знания. Рассматривая их, мы неизбежно ставим вопрос о природе человека. Что есть человек? На что он способен? Для каких целей он живет? Многие подобные вопросы встают в жизни любого разумного человека, решившего постичь тайну своего существования. Удивительно, как человек пытается найти ответы на вопросы, на которые невозможно дать однозначный ответ. Но попробуем понять, что же создает человек? Опираясь на историю, мы может ответить: человек всегда создает что-то уникальное, ранее не существовавшее. Несмотря на всю свою бессильность и некую беспомощность, человек всегда пытался взять под контроль саму природу бытия, создавая искусственный мир [2].

Рассуждая о взаимоотношениях человека и техники, обратимся к известному испанскому философу Хосе Ортега-и-Гассету. Итак, Хосе Ортега-и-Гассет утверждает, что природа человека слаба сама по себе, что делает нас, людей, беспомощными [3]. Трудно не согласиться с этим, ведь человек поистине скован своей физической оболочкой, которая является для нас и безмерным сокровищем, и мешающим фактором. До появления техники человек действительно считал себя ограниченным и не мог даже подумать о том, что однажды его безумные мечты смогут стать реальностью. Каким представлялся мир для

человека, живущего в 1950-е годы? Явно не таким, каким мы видим его сейчас. Человечество и представить не могло, что будет в будущем, опять же, из-за стойкого ощущения собственной слабости. Но все сомнения и страхи исчезают, когда начинается стремительное развитие техники. Именно в этот момент человек чувствует в своих руках безграничную власть. Также Хосе Ортега-и-Гассет пишет, что несмотря на прежние сомнения, которые тем не менее все еще остаются, человечество может осуществить все свои планы и мечты с помощью техники. Покорить космос, изменить будущее сегодня подвластно человечеству. И из-за полной безграничности в техническом плане человек постепенно теряет свой прежний облик. Сила, дарованная ему им самим, становится для него врагом? Сложно ответить на этот вопрос однозначно. Возникает вопрос, который был задан еще в самом начале: что есть человек?

В далеком прошлом люди начинали делать каменные орудия, чтобы сражаться и покорять природу по мере своей возможности. Каменные орудия были заменены более сложными конструкциями. Люди сплотились, начали строить поселения, облегчать себе жизнь. Так человек постепенно превращался в социальное существо, в том числе и ради облегчения собственной жизни. История подтверждает, что техника, простая или сложная, всегда развивалась вместе с человеком. Но лишь сейчас, когда прогресс идет все стремительнее, мы начинаем задумываться о том, что вообще такое техника и стоит ли нам ожидать от нее опасности. Человек – существо сложное, непознаваемое, уникальное и творческое. Техника в руках человечества – это лишь инструмент для изменения мира, для удовлетворения нужд и адаптации к среде.

Мыслители разных направлений не раз высказывали и продолжают высказывать опасение о возможном выходе техники из-под контроля людей. Современный мир с каждым днем неотвратимо приближается к моменту своего перехода к максимально технологизированному обществу.

Так, термин «технологическая сингулярность», введенный В. Винджем, включает в себя то, что нас ждет в будущем. Согласно Винджу, технологическая сингулярность – это момент времени, когда мощность компьютерных программ превысит вычислительную мощность человеческого мозга [4]. Как можно было понять, мыслитель утверждает, что искусственный интеллект в будущем будет гораздо более могущественным, чем человеческий. Иными словами, мир преобразится за счет быстродействия все более разумных систем. Тем не менее В. Виндж не утверждает, что сингулярность обязательно насту-

пит. Вполне возможно, что человечество может создать компьютеры с необходимой аппаратной мощностью, но ему не удастся организовать компоненты так, чтобы машина обрела разум, равноценный человеческому. Из слов писателя мы можем уловить лишь то, что облик человека может сильно измениться. Но обязательно ли это случится? Можно еще долго размышлять на эту тему, приводя трактовки различных мыслителей и намечать основные пути будущих дискуссий в данной области.

Закономерно лишь одно – человек всегда остается человеком, в чем-то сильным и в чем-то слабым, способным как к разрушению, так и созиданию, но это всегда человек, не утративший своей сущности вне зависимости от возможностей и времени.

Таким образом, в связи с бурным ростом промышленного производства, технологических инноваций, всеобщей информатизации отметим важность философского анализа феномена техники, а также деятельности человека по ее созданию.

ЛИТЕРАТУРА

1. Ленк Х. Размышления о современной технике. – М.: Аспект-пресс, 1996. – 181 с.

2. Касавина Н.А. Человек и техника: амбивалентность электронной культуры // Epistemology & Philosophy of Science. – 2018. – №4. – С. 129–141.

3. Ортега-и-Гассет Х. Размышления о технике // Избранные труды пер. с исп.; сост., предисл. и общ. ред. А.М. Руткевича. – М.: Весь Мир, 1997. – С. 164–232.

4. Виндж В. Сингулярность. – М.: АСТ, 2019. – 224 с.

УДК 339

ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННОГО СЕРВИСА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Ю. Нечушкина, студентка каф. ФиС

Научный руководитель В.В. Орлова, проф. каф. ФиС, д.соц.н.

г. Томск, ТУСУР, orlova_vv@mail.ru

Рассмотрено влияние современных цифровых технологий на развитие сервисных услуг. Отмечена необходимость обращения к ценностным основаниям культуры, анализу роли человека в мире цифровых технологий.

Ключевые слова: сервис, цифровизация, технический подход, операционный подход, общество.

В настоящее время рост научных знаний и технологий идет быстрыми темпами. Благодаря этому мир постоянно изменяется, и вместе с ним меняются области жизнедеятельности человека. Изменения видны каждому, однако их значение и возможные последствия не всегда очевидны. Цель данной статьи заключается в том, чтобы оценить характер последствий научно-технического прогресса для общества, цифровых технологий на сферы жизнедеятельности человека, а также прогнозировать возможные тенденции событий в будущем.

На данный момент сложно представить жизнь современного человека без цифровых технологий, ведь сейчас почти у каждого, если не у каждого, члена общества есть результат цифровых инноваций, таких как смартфон, планшет, ноутбук или же любое другое устройство. Таким образом, получается, что любой человек в современном мире находится под неким воздействием цифровизации.

Термин «цифровизация» часто соотносят с термином «оцифровка», считая, что они обозначают одно и то же, но это совершенно два разных понятия. Термин «оцифровка» на английском понимается как «digitization» и определяется как процесс преобразования информации с бумажного носителя в электронный формат. Оцифровка предполагает упрощение функционирования работы во всех сферах деятельности общества, при этом минимизируя различные ошибки. Как видно из определения, оцифровка никаким образом не относится к изменению. Все это больше подходит термину «digitalization», в переводе с английского – цифровизация. Под данным определением понимается совокупное употребление цифровых технологий и оцифрованной информации в результате процесса оцифровки, при этом цифровизация также способна на модернизирование различных процессов деятельности человечества [1].

Данная мысль прослеживается и в немецком языке: термин «цифровизация» объясняется двумя разными подходами. Первый подход – технический. Он предполагает, что цифровизация – это «перевод аналоговой информации в цифровую» [2], что очень схоже с термином «digitization» – оцифровка из английского языка. Второй подход – операционный, который предполагает перемещение задач на компьютер, т.е. в цифру, ранее выполняемое человеком.

Е.Л. Вартанова и М.И. Максеенко представляют термин «цифровизация» в широком смысле как системное решение, которое охватывает культурную сферу, сферу менеджмента, а также инфраструктуру и образ действий людей. Цифровизация понимается авторами как использование способов онлайн и инновационных интернет-технологий различными участниками экономической системы от частных лиц до

юридических, отмечая, что все процессы цифровизации в большей степени относятся к экономической сфере деятельности человека. Данная позиция подтверждается на государственном уровне, указы Президента Российской Федерации [3] направлены на развитие именно цифровой экономики, а именно увеличивать численность кадров, интеллектуальные и технологические возможности, создавая при этом нормативную базу.

В узком смысле термин «цифровизация» рассматривает Т.В. Фомичёва и представляет под ним «преобразование информации в цифровую форму, которая в дальнейшем приводит к оптимизации издержек, появлению новых перспектив развития» [4].

Из вышесказанного можно сделать вывод, что основным направлением цифровизации в Российской Федерации является сфера экономики. Сфера сервиса напрямую относится к сфере экономики. На данный момент с развитием цифровой экономики и ее проникновением во все отрасли жизни людей сферу сервиса это не может обойти стороной. Сейчас многие крупные предприятия, частные предприниматели, да и просто обычные граждане-покупатели переходят в режим онлайн, потому что это проще, быстрее, в каких-либо моментах даже выгоднее. Именно поэтому многие офлайн-представители сервисной деятельности стараются перенести свои услуги в цифровую среду, в первую очередь. для того, чтобы не потерять своих потенциальных клиентов, а в последующем и прибыль. Конечно, все услуги в онлайн-режим перенести невозможно, но электронные сервисы по записи клиентов, по приему заказов или же оплата через онлайн-банк уже внедрены почти в каждое предприятие, кафе/ресторан, салон красоты, магазин разных товарных категорий, и даже государственные учреждения, например, Многофункциональный центр (МФЦ), Государственная инспекция безопасности дорожного движения (ГИБДД), государственные банки и больницы и т.д.

Таким образом, цифровизация – это сложный и многоуровневый процесс, который имеет как ряд положительных последствий, так и отрицательных в виде рисков, выраженных в изменении качества жизни общества и изменении рынка труда. Данный процесс длится с начала XXI в., т.е. с момента информационного прорыва, а именно: модернизации портативных информационно-коммуникативных устройств, интеллектуально-роботизированных систем, повсеместного перехода на использование интернет-устройств.

ЛИТЕРАТУРА

1. Кудрявцева Т.Ю. Основные понятия цифровизации / Т.Ю. Кудрявцева, К.С. Кожина [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/osnovnye-ponyatiya-tsifrovizatsii (дата обращения: 17.02.2023).

2. Данилова Л.Н. Основные подходы к пониманию цифровизации и цифровых ценностей / Л.Н. Данилова, Т.В. Ледовская, Н.Э. Солынин, А.М. Ходырев [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/osnovnye-podhody-k-ponimaniyu-tsifrovizatsii-i-tsifrovyh-tsennostey (дата обращения: 15.02.2023).

3. О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ президента РФ от 09.05.2017 № 203 [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 15.02.2023).

4. Фомичёва Т.В. Ценности россиян в контексте цифровизации российской экономики / Т.В. Фомичёва, В.И. Катаева // Уровень жизни населения регионов России. – 2019. – № 2. – С. 80–84 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/tsennosti-rossiyan-v-kontekste-tsifrovizatsii-rossiyskoy-ekonomiki (дата обращения: 02.03.2023).

УДК 338.48

ЭКОЛОГИЧЕСКИЙ ТУРИЗМ: ОСНОВАНИЯ, ПУТИ ПРОДВИЖЕНИЯ

С.А. Рыжова, студентка каф. ФиС

Научный руководитель В.В. Орлова, проф. каф. ФиС, д.соц.н.

г. Томск, ТУСУР, orlova_vv@mail.ru

Рассмотрена роль технического прогресса в индустриальную эпоху популяризации и доступности туризма. Отмечена необходимость обращения к прошлому, обусловленности религиозными, экономическими, политическими и социально-психологическими факторами. Цель статьи – обосновать исследование экологического туризма как феномена, наиболее успешных путей развития и продвижения экологических туров.

Ключевые слова: индустриальная эпоха, туризм, экологический туризм, молодежь, человек, общество.

Технический прогресс и его развитие в индустриальную эпоху дал большой толчок в популяризации и доступности туризма. В настоящее время в деятельности человечества научно-техническое направление занимает ключевое место, а рост и накопление научных знаний и технологий идет быстрыми темпами. Туризм сейчас является буквально одной из самых масштабных и всеобъемлющих индустрий. Несмотря на то, что большую часть своего развития он приобрел в индустриальную и постиндустриальную эпохи, туризм как феномен уходит своими корнями далеко в прошлое, был обусловлен религиозными, экономическими, политическими и социально-психологическими факторами. На протяжении тысячелетий человек был вынужден осваивать новые земли, искать новые торговые пути, а также – иско-

паемые. Но время идет, теперь туризм обретает новые грани и новые направления, позволяя людям открывать для себя мир, абстрагируясь на время от работы, учебы и увлечений.

В широком смысле слова «туризм» означает определенный образ жизни, который представляется всем людям по-разному. Помимо обычных «пляжных курортов», не так давно внимание людей все больше начинает привлекать более неординарные виды туристического отдыха: экологические, научные, полярные и даже экстремальные. На появление экологического туризма сильно повлияла нарастающая кризисная экологическая ситуация, именно эта проблема побуждает многих людей сменить фокус с активного потребительского отношения к недрам, ископаемым и природным ресурсам, на её защиту, сохранение и последующее восстановление, в также привлечение внимания общественности к глобальной проблеме.

Сейчас общая доля экотуризма в мировом туризме составляет, по разным данным, от 10 до 30%, и увеличение этой доли прямым образом свидетельствует о повышении экологической сознательности, человеческом неравнодушии и желании спасти планету [1].

С точки зрения экономики расширение влияния экотуризма повлечет за собой множество выгод – территории, вовлеченные в рекреационное использование, станут более экономически устойчивы, тенденция появления новых рабочих мест, повышение жизненного уровня местного населения.

Экологический туризм уникален тем, что он не только связан с бизнесом, но и представляет собой целое социальное явление, базирующееся на гуманистических принципах и желании помочь природе. Также он является более доступным, в отличие от других направлений туризма он не требует значительных капиталовложений, поскольку преимущественно не связан с высокоразвитым сервисом, в котором обычно нуждаются другие категории туризма [2].

В настоящее время в обществоведческой литературе представлены разные виды экотуризма:

1. Научный. Предполагает собой изучение местной флоры и фауны путем наблюдения и исследования, не вредя природе.

2. Природный. Преимущественно означает посещения заповедных зон и национальных парков.

3. Активный. Вбирает в себя походы, велопрогулки и пешие прогулки.

4. Исторический. Позволяет познакомиться с национальной, культурной и традиционной составляющими местности.

5. Агротуризм. Предполагает собой как изучение земледелия, так и высадку и расширение численности зеленых насаждений.

Вместе с тем процесс включения человека в экологический туризм выполняет определенные функции. Всего различают экономическую, природоохранную, рекреационную и просветительскую функции экологического туризма.

1. Экономическая. Эта функция предполагает собой создание новых рабочих мест как для местного, так и для мигрирующего населения; позволяет расширить традиционные методы природопользования; привлечь внимание покупателей на экологически чистые продукты питания и пользования; способствует увеличению инвестиций в сервис, а также охрану природы; при повышении процента перерабатываемых отходов, позволяет заново использовать ресурсы, не вредя природе и сохраняя ресурсы.

2. Природоохранная. Предотвращение или уменьшение вмешательства в природу путем запретов и штрафов.

3. Рекреационная. Восстановление как природных, так и человеческих ресурсов.

4. Просветительская. Увеличение уровня сознательности к природопользованию и экологии способствует формированию у людей, пребывающих на природе, экологической культуры и любви к природе.

Таким образом, экологический туризм – важная часть образа жизни современного человека, приобщения его к культурно-историческим, этническим особенностям, вносит существенные изменения во всю систему общечеловеческой культуры, что заставляет обращаться к ее ценностным основаниям и анализу места человека в современном мире.

ЛИТЕРАТУРА

1. Абрамова И.В. Экологические туры: разработка и продвижение. – Минск, 2011. – 166 с.

2. Мельцов А.В. Актуализация экологического туризма и выявление необходимых предложений для продвижения экологических туров // Экономические исследования и разработки. – 2021. – № 4. – С. 28–32.

УДК 001.38

К ВОПРОСУ О СОЦИАЛЬНЫХ ПОСЛЕДСТВИЯХ НАУЧНО-ТЕХНИЧЕСКОГО ПРОГРЕССА

С.Ю. Василенко, студент каф. КУДР

Научный руководитель М.Ю. Раитина, доцент каф. ФиС, д.филос.н.

г. Томск, ТУСУР, step.vasilenko.official@gmail.com

Рассмотрена противоречивая роль социальных последствий научно-технического прогресса. Отмечена необходимость обращения к

ценностным основаниям культуры, анализу места человека в мире технологий.
Ключевые слова: научно-технический прогресс, виртуальность, молодежь, человек, общество.

В настоящее время в деятельности человечества научно-техническое направление занимает ключевое место, а рост научных знаний и технологий идет быстрыми темпами. Благодаря этому мир постоянно изменяется, и вместе с ним меняется наше общество. Изменения видны каждому, однако их значение и возможные последствия не всегда очевидны. Цель данной статьи заключается в том, чтобы оценить характер последствий научно-технического прогресса для общества, а также прогнозировать возможный ход событий в будущем.

Научно-технический прогресс существенно меняет повседневную жизнь человека уже не первое десятилетие, однако в последние годы изменения стремительно наращивают темп. Накопленный за годы исследований опыт приблизил нас к созданию искусственного интеллекта, позволил связать всех людей сетью интернета и вместе с тем перенес большую часть нашей социальной жизни в виртуальное пространство. Благодаря технологиям мы не только можем круглосуточно быть на связи с друзьями из реальной жизни, но и заводить онлайн-друзей, общаться с программами-ботами и находить виртуальных партнеров. Интернет каждый день заполняет наше сознание массивом информации, причем скорость потока сведений не позволяет оценить их качество.

В условиях роста размеров городов реальные места во многом теряют актуальность, если есть легкодоступные виртуальные аналоги. Человека со всех сторон окружает огромное количество рекламы, смешных видео, сообщений, предложений и интересных фактов, причем большая часть подобного контента абсолютно бесполезна, но от этого не теряет своей привлекательности. Таким образом, человек каждый день частично живет в виртуальном мире. Удобства данного подхода на первый взгляд очевидны – экономия времени на дорогу, быстрота обмена информацией, большое разнообразие этой информации и т.д.

Яркой иллюстрацией современной технологичной жизни является ситуация в современном Китае. После экономической революции жизнь в стране изменилась – стремительный рост городов, кардинальное различие уровня жизни в деревне и в городе ведут к тому, что молодые люди, в поисках лучшей жизни переезжающие в города, теряют всякую связь с родственниками.

Высокотехнологичная жизнь требует от людей многого – жители городов не стремятся создавать семьи, так как непрерывная работа не оставляет шансов найти партнера, а высокая стоимость жизни делает рождение и воспитание детей крайне дорогим и неблагодарным занятием. Здесь на помощь приходят технологии – онлайн-сервисы друзей заменяют настоящее общение, которое отнимает больше сил и не всегда проходит гладко, 3D-персонажи заменяют партнеров – они красивее реальных и с ними невозможно поссориться, кроме того, они всегда рядом с вами, а все, что нужно, – несколько юаней в месяц.

Спрос рождает предложение, и вместо того, чтобы остановиться, запретить проникновение технологий в те сферы жизни человека, в которых их вмешательство изначально не планировалось, люди активно стимулируют развитие всего, что может принести краткосрочную выгоду, вне зависимости от потенциальных рисков. В итоге общество в больших городах Китая на данный момент является обществом одиночек, отчасти пребывающих в виртуальном мире [1].

В реальности такая жизнь не приносит настоящего счастья, в иллюзии нельзя жить постоянно, кроме того, она сильно отличается от того, что остается обычному человеку в качестве реальной жизни – бесконечной работы, пробок на дорогах, огромного количества незнакомцев, ощущения растерянности и одиночества. Подобная ситуация не может не вызывать вопросов, и главный из них – насколько виртуальный мир способен заменить настоящий? Это действительно серьезная проблема, так как человек пока что остается биологическим существом, имеет соответствующие потребности и, кажется, не может переселиться в виртуальный мир полностью, но, судя по направлению прогресса, технологии сейчас развиваются как раз в направлении полной цифровизации человека.

Ряд авторов в научной литературе обозначали проблему дальнейшей эволюции науки и техники и их влияния на человечество, например, Р. Коэн, выпустивший в 1980 г. свою статью «Социальные последствия технического прогресса». Философ рассуждал о последствиях научно-технического прогресса, выделяя роль Запада в развитии технологий. Р. Коэн поставил в своей статье ряд проблем, на данный момент представляющих для человечества серьезную угрозу: проблема ядерного вооружения, проблема тотальной войны и т.д.

Опасные последствия технологического прогресса Коэн разделил на 3 категории: политические, социальные и идеологические. Он говорил о том, что наука не может быть беспристрастной и потому всегда будет являться формой оружия, угрожающего человеческому обществу. В заключение Роберт Коэн обратился к участникам Пражско-

го симпозиума ЮНЕСКО, на котором была представлена статья, со словами: «Среди множества различных технических альтернатив мы – учёные, техники и философы – должны научиться предвидеть опасности и благоприятные возможности, должны осуществлять свой выбор с чувством реальной возможности следовать подлинно человеческим ценностям» [2].

Отечественные мыслители также рассуждали над данной проблемой. Так, в статье А.И. Столетова и К.Р. Мухаметзяновой «Технический прогресс и общество» обсуждается понятие технократического общества и последствия трансформации социума в данный вид общества. По словам ученых, бурное развитие научно-технического прогресса ведет к неизбежной технологической катастрофе.

Развитие технологий отрицательно влияет на экологию планеты, бесконечная потребность в сырье истощает природные запасы ископаемых, а люди, постоянно живущие в обществе риска, перестают адекватно воспринимать приближающиеся проблемы. Виной всему, по мнению философов, антропоцентрическое отношение к природе, а также экстенсивное развитие человечества.

Для решения проблем необходимо сформировать новый тип личности, «чьим основанием являлось бы творчество, но направленное не вне, а внутрь человека» [3]. Очевидно, что указанные выше авторы призывают обратить свой взгляд на человеческие ценности. По мнению философов, именно смена образа мышления, переход к новой системе ценностей (а точнее, возвращение к системе ценностей, привычной для людей до начала бурного развития научного прогресса), отмена фетиширования науки и технологий могут помочь решить вызываемые прогрессом проблемы.

Согласимся с вышеуказанной позицией, человечеству действительно стоит сосредоточиться больше на интенсивном, а не экстенсивном развитии, ограничив культуру потребления. В худшем случае актуальная сейчас ситуация может вылиться в полное проникновение технологий во все уровни нашей жизни. Это повлечет за собой полное обесценивание социальных связей, разрушение понятий семьи и брака, возведение технологий в культ и в будущем, возможно, гибель человечества как вида в результате тотальной войны или несчастного случая – и это, не говоря о психологических и физических проблемах, которые также могут постигнуть людей в данной ситуации.

Если же развитие технологического прогресса вновь получится контролировать, возможен другой сценарий – люди более медленными темпами все же придут к высокотехнологичному обществу, но при этом не потеряют человечности; социальные связи будут сохраняться,

а внимание общества будет направлено на развитие не только материального, но и на изучение, познание мира, а также сознания человека.

Очевидно, если в ближайшее время не произойдет катастрофа или некое глобальное изменение, способное акцентировать все внимание людей на себе, темп изменений будет лишь нарастать. Многие компании, к сожалению, развивают именно те технологии, которые при чрезмерном присутствии в нашей жизни несут вред, и совершенно не собираются останавливаться. Большинство людей с радостью отказывается от старых ценностей, накладывавших некоторые ограничения, в пользу новых безграничных технологических удовольствий. Постоянное материальное легкодоступное наслаждение быстро заменяет духовное, поскольку частью духовного постижения является трудный и долгий путь к его обретению. Однако именно способность и тяга человека к развитию и наполнению духовной сферы может спасти человечество от технологической катастрофы.

Таким образом, научно-технический прогресс вносит существенные изменения во всю систему общечеловеческой культуры, что заставляет обращаться к ее ценностным основаниям и анализу места человека в мире технологий.

ЛИТЕРАТУРА

1. Котельникова Н.Н. Одиночество в толпе: феномен «молодежи пустого гнезда» в медиаурбанистическом дискурсе современных китайских мегаполисов // III Готлибовские чтения: Востоковедение и регионоведение Азиатско-Тихоокеанского региона в фокусе современности: матер. междунар. науч. конф. – Иркутск: Иркут. гос. ун-т, 2019. – С. 257–265.

2. Столетов А.И. Технический прогресс и общество / А.И. Столетов, К.Р. Мухаметзянова // Молодой ученый. – 2017. – № 1 (135). – С. 576–579 [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/135/37912/ (дата обращения: 12.02.2023).

3. Cohen R.S. The Social Implications of the Scientific and Technological Revolution. – Paris: UNESCO Press, 1981. – PP. 365–370.

УДК 331.548

РАЗРАБОТКА СИСТЕМЫ ПРОФОРИЕНТАЦИИ СТУДЕНЧЕСКОЙ МОЛОДЕЖИ В ВУЗЕ

Т.А. Зайцева, аспирант каф. ФиС

Научный руководитель В.В. Орлова, проф. каф. ФиС, д.соц.н.

г. Томск, ТУСУР, oderova-t@mail.ru

Трудоустройство выпускников вузов имеет особое значение, в том числе для развития высокотехнологичных отраслей. Грамотная

профориентация и развитие индивидуальных карьерных траекторий студентов помогут повысить эффективность трудоустройства молодых специалистов. Проведен анализ трудоустройства выпускников и ситуации на рынке труда молодых специалистов. Предложена система профориентации студентов с целью ее внедрения в работу Центра карьеры ТУСУРа.
Ключевые слова: профориентация, карьерные траектории, студенты.

Профессиональное развитие молодого специалиста и его карьерная траектория в последние несколько лет привлекают особое внимание вузов, Минобрнауки РФ, работодателей и т.д. Важно не просто трудоустройство выпускников вуза, а подготовка молодых специалистов, готовых к условиям рынка труда и требованиям компаний, занятость и применение полученной квалификации в востребованных для развития экономики государства отраслях.

Цель работы – разработать систему профориентации для Центра карьеры ТУСУРа, направленную на формирование индивидуальной карьерной траектории студента и повышение эффективности трудоустройства выпускников.

В 2021 г. исследована занятость выпускников трех томских вузов: ТУСУР, НИ ТПУ, ТГУ на основании опроса 418 респондентов. Результаты исследования: каждый третий выпускник не работает по специальности (33%), а 14% не трудоустроены.

Таким образом, примерно в половине случаев выпускники не используют полученное образование и полученные навыки. Одна из причин трудоустройства молодежи на вакансии без применения своей квалификации – отсутствие понимания применимости конкретных знаний и навыков, страх перед представителями компаний, принимающих карьерные решения. Выстроить свою карьерную траекторию мешает большой поток информации об актуальных профессиях, данных по рынку труда, которые студент не в состоянии проанализировать и оценить самостоятельно [1].

Проблему трудоустройства молодых специалистов на вакансии по образованию и полученной квалификации отражает и ситуация на рынке труда. По данным HeadHunter, в 2022 г. индекс конкуренции среди молодых специалистов – 7 человек на место, а в пик достигал 9 человек на место. Спрос на молодых специалистов отражается в 17% доступных вакансий для данной категории соискателей [2].

На основании анализа тенденций на рынке труда молодых специалистов РФ необходима профориентационная работа по построению индивидуальной карьерной траектории.

Профессиональный ориентир студентов имеет свойство часто перестраиваться в зависимости от влияния внутренних установок, внешних агентов и уровня развитости HR-бренда (привлекательности) компаний из соответствующей отрасли. Данный факт необходимо учитывать при профориентационном консультировании и формировании плана индивидуальной карьерной траектории студента.

Для организации HR-бренд является инструментом по позиционированию на рынке труда и демонстрации кадровой политики. Сильный HR-бренд компании позволяет экономить в среднем около 20% затрат на персонал [3].

Студенты знакомятся с HR-брендом компаний, а также сравнивают свои карьерные ожидания и формируют представления через посещение встреч, прохождение практики, стажировки, транслируемой информации в сети Интернет и т.п.

Совокупность представлений о крупных работодателях, предлагаемых трудовых условиях и их корпоративной культуре создает стереотип о карьерных возможностях отрасли в целом, соответственно оказывают влияние на выбор профессии. Молодые соискатели обращают внимание помимо уровня заработной платы, возможности гибкого или гибридного графика и иных условий работы, на отзывы бывших сотрудников и корпоративные ценности [4]. Примерами такого эффекта могут быть: IT-отрасль, космическая, оборонная отрасль и т.д.

По результатам опроса и анализа данных по трудоустройству молодых специалистов, тенденций на рынке труда молодежи разработана система профориентации, позволяющая студенту самостоятельно или с помощью профконсультанта построить индивидуальную карьерную траекторию.

Система профориентации молодежи по построению индивидуальной карьерной траектории и развития состоит из шести этапов: от абитуриента до выпускника. Каждый этап сопровождается своевременной работой, направленной на:

– выбор специальности и профессий с учетом индивидуальных способностей;

– знакомство с центром карьеры и возможностями;

– построение карьерной траектории с учетом влияния HR-бренда компаний в отрасли: карьерная цель, карта и план профессионального и надпрофессионального развития;

– подготовку документов для трудоустройства: резюме, сопроводительное письмо, портфолио, оформление страниц на внешних платформах (например, GitHub, Behance, Факультетус и т.п.), контроль продвижения по карьерной карте;

– привлечение к участию в карьерных мероприятиях и стимулирование к трудоустройству;

– индивидуальную работу по обращениям;

– направление работы выпускник-стейкхолдер.

Исследование трудоустройства выпускников томских вузов и анализ ситуации на рынке труда молодых специалистов помогли в разработке системы профориентации студентов, направленной на повышение эффективности трудоустройства выпускников. Данная система была включена в профориентационную работу Центра карьеры ТУСУРа и применяется для формирования карьерных траекторий студентов.

ЛИТЕРАТУРА

1. Верниенко Л.В. Стратегии построения карьеры студентами в процессе получения высшего образования // Век качества. – 2018. – № 2 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/strategii-postroeniya-kariery-studentami-v-protsesse-polucheniya-vysshego-obrazovaniya-1 (дата обращения: 05.03.2023).

2. Рынок труда молодых специалистов в 2022 году [Электронный ресурс]. – Режим доступа: https://tomsk.hh.ru/article/31181 (дата обращения: 02.03.2023).

3. Половинко В.С. Роль и структура HR-бренда в процессе профессионального самоопределения и управления человеческими ресурсами // Вестник ОмГУ. – Сер.: Экономика. – 2018. – № 4 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/rol-i-struktura-hr-brenda-v-protsesse-professionalnogo-samoopredeleniya-i-upravleniya-chelovecheskimi-resursami/viewer (дата обращения: 05.03.2023).

4. Рекрутеры рассказали об ожиданиях молодых специалистов при поиске работы // Информационный портал газеты «Известия» [Электронный ресурс]. – Режим доступа: https://iz.ru/1115056/2021-01-25/rekrutery-rasskazali-ob-ozhidaniiakh-molodykh-spetcialistov-pri-poiske-raboty (дата обращения: 02.03.2023).

ПОДСЕКЦИЯ 5.7

АКТУАЛЬНЫЕ ВОПРОСЫ ЧАСТНОГО ПРАВА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

*Председатель – **Мельникова В.Г.**, зав. каф. ИГПиПОИД ТУСУРа, к.ю.н., доцент;*
*зам. председателя – **Часовских К.В.**, ст. преп. каф. ИГПиПОИД ТУСУРа*

УДК 347.6

К ВОПРОСУ О НАСЛЕДОВАНИИ АККАУНТОВ

В.В. Шаклеин, ст. преп. каф. ГП
г. Томск, ТУСУР, ppkuitsuSV@mail.ru

Рассматривается вопрос о наследовании аккаунтов. Делается вывод о принципиальной возможности наследования аккаунтов, однако представляется некорректным наследование любого аккаута.
Ключевые слова: аккаунты, наследование, пользовательское соглашение.

Достаточно дискуссионным вопросом, который прямо вытекает из правовой природы аккаунта, представляется наследование аккаунта. В соответствии со ст. 1112 ГК РФ в состав наследственной массы входит все имущество, принадлежавшее лицу на момент смерти, включая имущественные права и обязанности, кроме прав и обязанностей, которые непосредственно связаны с личностью усопшего. При этом гражданское законодательство не регулирует вопросы наследования аккаунта умершего.

Самой первой проблемой в области наследования аккаунтов, естественно, является отсутствие их или чего-то подобного в перечне объектов гражданских прав.

На настоящий момент высказывается точка зрения, что аккаунты должны быть встроены в существующую систему объектов гражданских прав (см., например, [1]). В рамках данной статьи не рассматривается вопрос о правовой природе аккаунтов, однако предполагается, что аккаунт является составной частью имущества умершего. Вопрос о том, к какому конкретно виду объектов гражданских прав относится аккаунт, достаточно дискуссионный, и единого мнения в литературе

на этот счёт нет. Однако вывод об оборотоспособности аккаунтов можно сделать хотя бы потому, что многие аккаунты имеют имущественную ценность (например, там содержится приобретённый контент, или же такой аккаунт используется для предпринимательских целей, а некоторые аккаунты в компьютерных играх вообще выставляются на продажу).

Обращаясь к зарубежной практике, можно прийти к выводу, что зарубежная практика даёт возможность наследовать аккаунты и включать их в наследственную массу [2].

Например, решением Верховного суда Германии от 12 июля 2018 г. III ZR 183/17 было признано право родителей девочки, покончившей жизнь самоубийством в 2012 г., на наследование ее аккаунта в социальной сети Facebook с целью получения информации о деталях случившегося [3].

В целом в вопросе наследования достаточно частно руководствуются пользовательским соглашением. Например, аккаунт в системе Google разрешает пользователю наследовать аккаунт, а также установить степень доступа к нему наследников. Социальная сеть Instagram (признана экстремистской на территории России, однако продолжает широко использоваться) не предусматривает возможности унаследования аккаунта, а лишь исключительно его удаление по запросу наследника умершего [4].

Последние версии продуктов Apple (начиная с iOS 15.2, iPadOS 15.2 и macOS 12.1) также позволяют выбрать цифрового наследника [5].

Однако отдавать вопрос о наследовании исключительно на откуп пользовательским соглашениям нельзя, поскольку такие соглашения могут как начать противоречить объективной реальности или же закону, либо невозможно будет реально проконтролировать его соблюдение. Данные вопросы будут рассмотрены ниже.

Тем не менее не все аккаунты можно считать наследуемыми. Очевидно, что личный аккаунт, не связанный с предпринимательской деятельностью, наследованию не подлежит: сложно представить себе ситуацию, когда наследник умершего пользователя социальной сети будет общаться под именем умершего. Коммерческий же аккаунт (например, созданный для заключения различных договоров), по сути, составляет часть имущества, используемого в предпринимательской деятельности. Соответственно, правопреемство тут возможно. Но и тут возникают проблемы фактического характера. Например, наследодатель ведёт группу в социальной сети, которую использует для продвижения своих товаров/работ/услуг. Поскольку группа уже имеет популярность, создавать аналогичную наследнику может быть до-

вольно затратно: аудиторию необходимо привлекать, на что нужно время. В этом случае встаёт вопрос о наследовании аккаунта, который используется для предпринимательской деятельности, а пользовательское соглашение запрещает его передачу. Конечно, возможно решение вопроса с администраторами социальной сети, однако что делать, если наследнику будет отказано? Ведь такой отказ повлечёт для него убытки, связанные с повторным созданием и раскруткой группы.

Также сложными являются вопросы о наследовании аккаунтов, содержащих купленные объекты (например, аккаунты в Steam) или же смешанного характера (например, страница «ВКонтакте», которую индивидуальный предприниматель использовал как для личного общения, так и для предпринимательской деятельности). Относительно первого можно снова попытаться отдать всё на откуп пользовательским соглашениям. Однако текущие соглашения, в основном, запрещают передавать аккаунты третьим лицам. Хотя фактически проконтролировать это довольно сложно (например, тот же Steam не запрашивает паспортные данные при регистрации), а изменение ip-адреса можно объяснить переездом.

Аналогичная ситуация будет, если оставить логин и пароль наследнику напрямую или же указать в завещании. С такой позиции пользовательские соглашения с запретами о передаче аккаунтов фактически перестанут отражать реальную действительность, при этом реальных инструментов это изменить ни у владельцев сервиса, ни у законодателя нет. Относительно второго, вероятно, наследование стоит признать невозможным, поскольку нельзя разделить предпринимательскую и личную составляющую, хотя содержание переписок может иметь критически важное значение для предпринимательской деятельности. Возможно, в данном случае имеет смысл некое половинчатое решение о предоставлении доступа к перепискам без возможности писать сообщения.

В качестве решения проблемы наследования можно встретить мнение о возможности наследования путём прямого выражения воли наследодателя через завещание и выставления соответствующих настроек [6]. Сама по себе данная позиция вполне логична, однако с учётом неразвитости культуры завещания в России и малого уделения внимания настройкам, напрямую не связанным с функционированием аккаунта, представляется, что таким образом можно разрешить лишь меньшую часть из практических ситуаций. Кроме того, не снимается вопрос, если владельцем аккаунта будет являться несовершеннолетний, не обладающий способностью к написанию завещания.

Ещё одним возможным противоречием можно обозначить ситуацию, когда аккаунт содержит результаты интеллектуальной деятельности. Естественно, что владелец аккаунта имеет авторские права на данные результаты интеллектуальной деятельности. Однако при запрете наследования, согласно пользовательскому соглашению, наследник фактически лишается части наследственной массы (см., например, [7]).

Таким образом, ввиду отсутствия научного консенсуса касательно как правовой природы аккаунта, так и возможности его наследования, равно как и пределов наследования, необходимо проводить дальнейшие исследования в данной области.

ЛИТЕРАТУРА

1. Суслова С.И. Объекты гражданских прав в условиях формирования информационного пространства России / С.И. Суслова, У.Б. Филатова // Пролог: журнал о праве. – 2019. – № 2. – С. 23–28.

2. Кирсанова Е.Е. Аккаунт как объект гражданских прав // Вестник арбитражной практики. – 2020. – № 2. – С. 44–48.

3. BGH, 12.07.2018 – III ZR 183/17 [Электронный ресурс]. – Режим доступа: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=12.07.2018&Aktenzeichen=III%20ZR%20183%2F17

4. Амбарцумов Р.А. Аккаунты социальных сетей как объекты наследственных правоотношений // Вопросы российской юстиции. – 2019. – № 1.

5. Как добавить цифрового наследника для вашего идентификатора Apple ID [Электронный ресурс]. – Режим доступа: https://support.apple.com/ru-ru/HT212360

6. Галкина М.Л. Вопросы наследования аккаунтов в социальных сетях / М.Л. Галкина, Н.А. Развейкина // Управление в условиях цифровизации социально-экономических процессов: сборник науч. статей. – Чебоксары: СНИУ, 2020. – С. 85–95.

7. Панарина М.М. Наследование аккаунта в социальных сетях и вопросы цифрового наследования: правовое исследование // Наследственное право. – 2018. – № 3. – С. 27–28.

ПОДСЕКЦИЯ 5.8

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ РОССИЙСКОГО ПРАВА

*Председатель секции – **Ахмедшин Р.Л.**, проф. каф. ГПДиПД, д.ю.н.;*
*зам. председателя – **Алексеева Т.А.**, доцент каф. ГПДиПД, к.ю.н.*

УДК 343.95, 343.98

СМЫСЛОВАЯ НАГРУЗКА СИМВОЛА «РОДИНА» В РЕЧИ СЕНЗИТИВНОГО И ЗАСТРЕВАЮЩЕГО АКЦЕНТУИРОВАННОГО ТИПА: ЛИНГВИСТИЧЕСКИЙ, ПСИХОЛОГИЧЕСКИЙ И КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТЫ

Д.Р. Ахмедшина, студентка ФилФ НИ ТГУ
Научный руководитель Т.А. Алексеева, доцент каф. ГПДиПД
г. Томск, ТУСУР, montague_cake@mail.ru

Рассматривается вопрос трактовки в речи неидентифицированного лица символа «родина» в целях решения задачи групповой идентификации этого лица и возможности построения его психологического профиля.
Ключевые слова: психотип, сензитив, застревающий, символ, Родина.

По замечанию Ф. де Соссюра, мышление представляет собой бесформенную массу, в которой нет реальных единиц. Включение в неё звуковой цепи происходит посредством языка – таким образом, объединение неизбежно приводит к обоюдному разграничению единиц. В этой системе лингвистический знак наделен не столько значением, сколько значимостью, при этом, например, значение слова в лексической системе одного языка может отличаться от значения этого слова в другом языке [1]. Сказанное предельно важно при решении ряда прикладных задач криминалистической направленности, в том числе определения полного авторства текста либо доли в нем, а также вероятностного вывода о факте правок, внесенных в текст третьим лицом. Возможность решения указанных задач определяется невысокой временной продолжительностью исследования личности автора по анализируемому тексту, что положительно скажется, например, на сроках расследования.

Такое несоответствие значимости одного слова в преломлении восприятия можно выделить и у разных психологических типов. Рассмотрим преломление слова «Родина» в восприятии пары акцентуированных психологических типов – сензитива и застревающего – на примере двух поэтических текстов.

Обрисованная в стихотворении С. Есенина «Русь» малая родина (а следовательно, проекция Родины во всех смыслах) представляет собой картину всеобъемлющего космоса, в котором доминирует эмоциональное начало. В представлении о символе на примере лингвистического знака родины для сензитива важно, в первую очередь, эмоциональное восприятие. «Родина» наполняет в себе всё, что охватывает лирический субъект, всё, что отдаётся в нём на чувственном уровне, даже если объяснений этому он не находит.

«Но люблю тебя, родина кроткая!
А за что – разгадать не могу.
Весела твоя радость короткая
С громкой песней весной на лугу».

Сензитив считается самым эмоциональным типом, что проявляется не только в особенностях характера (характерные черты: эмпатия, отзывчивость, тревожность, мнительность [2, с. 501–502]), но и в наполнении в его сознании лингвистического знака глубиной личного переживания. Этот тип приписывает эмоции миру вне зависимости от того, как они преломляются через призму его восприятия. Объективированная эмоциональная насыщенность реальности – яркий пример проявления интровертного начала, в котором автор нередко дистанционируется от антропоцентрического сценария, подавая себя как элемент окружающего универсума в его многообразии. Нельзя сказать, что смысловая насыщенность символов вообще и символа «Родина» в частности полностью выведена из области объект-объектных представлений. Скорее, в определенной мере игнорируется сама целесообразность позиционирования реального объекта в познании бытия.

Иное изображение встречаем в стихотворении М. Матусовского «С чего начинается Родина?». В нём лирический космизм с эмоциональной доминантой изображаемого пространства родины уходит на задний план. Теперь во внешнем изображении доминирует то, что объективно наполняет этот образ – то, что обусловлено не столько чувственным началом, сколько началом рациональным, объективируемым.

«С чего начинается Родина?
С картинки в твоем букваре,
С хороших и верных товарищей,
Живущих в соседнем дворе».

В приведенном фрагменте проявляется особенность восприятия символа Родины застревающим акцентуированным психотипом. Идея упорядоченности, лежащая в основе характера, подчеркивается идеей патриотизма, сосредоточиваемой в конце стихотворения. Алгоритмизация восприятия накладывается на привычные механизмы разворачивания символа – ему подвергается даже эмоциональное его наполнение.

Сказанное проистекает из того, что рассматриваемый тип считается выраженно рациональным типом, что проявляется не только в особенностях характера (характерные черты: системность, последовательность, высокая степень концентрации внимания на внешней деятельности в текущий момент времени [2, с. 504–505]), но и в наполнении в его сознании лингвистического знака осознанием целесообразности анализируемого феномена. Этот тип приписывает априорную организованность миру – в контексте принятых в его микростратосе представлений. Объективированная деятельностная насыщенность реальности – яркий пример проявления экстравертного начала, в котором автор в большинстве случаев представляет антропоцентрический сценарий как аксиому, представляя окружающий универсум как объект воздействия человека. Можно сказать, что смысловая насыщенность символов вообще и символа «Родина» в частности полностью локализована в области объект-субъектных представлений. Четко пропагандируется принципиальная целесообразность позиционирования реального объекта в познании бытия.

Сказанное еще раз актуализирует идею необходимости исследования сложных феноменов и деятельности человека как наиболее сложного из них на уровне междисциплинарном, в том числе с привлечением достижений лингвистики.

ЛИТЕРАТУРА

1. Соссюр Ф. Курс общей лингвистики / пер. А.М. Сухотин; под ред. Р.О. Шор. – М.: Изд-во «Юрайт», 2023. – 303 с. – (Антология мысли).

2. Ахмедшин Р.Л. Криминалистическое профилирование: учеб. для вузов / Р.Л. Ахмедшин, Н.В. Ахмедшина. – М.: Изд-во «Юрайт», 2023. – 514 с. – (Высшее образование).

УДК 343.91

ПСИХОФИЗИОЛОГИЧЕСКОЕ ИССЛЕДОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ПОЛИГРАФА ЛИЦ, СКЛОННЫХ К АГРЕССИИ

Т.А. Алексеева, доцент каф. ГПДиПД ЮФ
г. Томск, ТУСУР, tanyaalek@yandex.ru

Психофизиологическое исследование с использованием полиграфа является одним из наиболее перспективных исследований в области криминалистики и психологии, которые всегда находятся в поиске новых способов выявления свойств личности. В статье рассматриваются возможности исследований при помощи полиграфа, в том числе диагностика психофизиологического состояния человека, склонного к агрессивному поведению.

Ключевые слова: опрос при помощи полиграфа, психофизиологическое исследование, диагностика психофизиологического состояния человека, агрессивное поведение.

Психофизиологические исследования с использованием полиграфа набирают все большую популярность в различных сферах, начиная от расследования преступлений (в рамках назначения психофизиологической экспертизы), заканчивая кадровыми проверками и решением частных вопросов. Несомненно, определенный интерес такие исследования вызывают и у ученых-психологов, криминалистов, в процессе которых расширяются исследовательские задачи, ставятся новые вопросы, требующие своего решения.

Цель, поставленная автором статьи, – проанализировать возможность проведения психофизиологического исследования с использованием полиграфа лиц, склонных к агрессивному поведению.

При написании статьи использовались следующие методы: анализ информации, методы опроса при помощи полиграфа, связанные с опознанием стимулов (вопросов) и диагностикой различной степени эмоциональной напряжённости (в данном случае агрессивного поведения) при их предъявлении.

Самая распространенная диагностическая задача, решаемая при помощи психофизиологических исследований с использованием полиграфа, – это определение лжи, а точнее фиксация изменений физиологических реакций организма человека на предъявляемые стимулы, по которым возможно установление признаков недостоверности сообщаемой информации. Однако возможности диагностики на этом не заканчиваются. Ученых все больше интересуют вопросы определения психологических особенностей личности, которые возможно под-

твердить инструментально при помощи полиграфа. Так, например, коллективом исследователей О.Г. Венериной и А.П. Сошниковым с целью диагностики и прогноза поведения типа личности человека был разработан специализированный программный модуль оперативной психодиагностики, который в настоящее время встроен в компьютерный полиграф «Диана».

Другая группа исследователей, изучая влияние индивидуально-типологических различий испытуемых на физиологические показатели стрессового реагирования во время процедуры тестирования на полиграфе, пришли к выводу, что индивидуально-типологические особенности оказывают значимое влияние на формирование индивидуального симптомокомплекса. Под индивидуальным симптомокомплексом понимается уникальный набор параметров физиологических реакций, возникающий при предъявлении исследуемому лицу стимулов, имеющих для него субъективное значение, обусловленный его оптимальным функциональным состоянием в ходе всего процесса психофизиологического исследования с применением полиграфа.

Кроме того, в результате исследования было выявлено, что среди психофизиологических особенностей испытуемых наибольшее влияние на формирование симптомокомплекса оказывают свойство силы нервной системы и свойство переключаемости нервных процессов. Среди психологических характеристик наиболее значимыми для формирования симптомокомплекса исследуемых авторы выделяют такие характеристики, как демонстративность, педантичность, гипертимность, тревожность и эмотивность.

Таким образом, если существует возможность диагностировать наличие некоторых перечисленных индивидуально-психологических особенностей личности, то есть и вероятность определения такого свойства, как агрессивность.

Определим понятие «агрессивность» через призму психологии. Агрессивность – это психическое явление, выражающееся в стремлении к насильственным действиям в межличностных отношениях, проявляющееся как ситуативный кратковременный процесс или состояние.

Кроме того, агрессивность выступает одним из основных способов решения проблем, связанных с сохранением индивидуальности или причастности себя к определенной социальной группе, с защитой и ростом чувства собственной ценности, самооценки, уровня притязаний, а также сохранением и усилением контроля над существенным для субъекта окружением. Помимо этого, агрессивность выступает в качестве средства достижения какой-либо значимой цели, способа психологической разрядки, способа удовлетворения потребности в самореализации или самоутверждении.

Автор предлагает в рамках психофизиологического исследования, использовать ряд вопросов для выявления физической или косвенной агрессии у обследуемого, основанных на опроснике агрессии Басса-Дарки и адаптированных для тестирования на полиграфе.

Вопросы для выявления склонности к физической агрессии:

1. Вам хочется причинять вред другим людям?
2. Вы способны ударить человека?
3. Если кто-нибудь первым ударит вас, вы обязательно ответите?
4. Если кто-то вас ударит, вы ввяжетесь в драку?
5. В гневе вы способны на насилие?
6. Вы деретесь не реже, чем другие?
7. Если для защиты ваших прав потребуется физическая сила, вы примените её?

Вопросы для выявления склонности к косвенной агрессии:

1. Вы часто сплетничаете о людях, которые вам не нравятся?
2. Вы способны на грубые шутки?
3. Если что-то идет не так, как хочется, вы обижаетесь?
4. Будучи злым, вы ломали вещи?
5. В гневе вы можете стучать кулаком по столу?
6. Вы раздражительный человек?
7. Будучи в гневе, вы можете кидаться предметами, хлопать дверью?

В качестве вывода предлагаются возможные перспективы исследования лиц, склонных к агрессивному поведению, главным образом имеющие криминалистическое значение:

1. Психофизиологическое исследование лиц, совершивших насильственные преступления. Сегодня психофизиологическое обследование с использованием полиграфа хотя и не является доказательством по уголовному или гражданскому делу, однако активно используется сторонами для подтверждения определенного события (действия). Обозначенное направление исследований будет иметь значение в рамках изучения личности преступника и составления портрета неизвестного преступника. Имея данные о индивидуально-психологических особенностях лиц, совершивших насильственные преступления, склонных к агрессивному поведению, появится возможность использовать их при поиске других преступников с похожим профилем совершения преступлений.

2. Психофизиологическое исследование лиц, склонных к насилию, по результатам психологического исследования. Здесь имеются в виду лица, не привлекавшиеся к уголовной ответственности, не совершавшие преступлений, но в силу агрессивного поведения способ-

ные на жестокие действия по отношению к другим людям. Исследования в рамках указанного направления носят профилактический характер с тем, чтобы вовремя выявить склонность лица к агрессии и скорректировать поведение. Наибольшая ценность такого исследования представляется среди несовершеннолетних.

3. Психофизиологическое исследование остальных лиц для выявления склонности к насилию. Последнее направление содержит в себе целиком исследовательские цели и задачи. Автор понимает, что агрессивное поведение и выявление такого индивидуально-психологического свойства, как агрессия, не означает, что человек совершит преступление в будущем. Однако увеличение количества респондентов позволит выявить или опровергнуть наличие такого свойства, как агрессивность, в том числе и в связке с принадлежностью лица к определенному психологическому типу, что расширит способы изучения личности, в том числе и личности преступника.

Одним из способов определения психологического типа является прохождение тестирования. Согласно исследованиям К. Леонгарда, наиболее агрессивным психотипом является этипептоидный тип. Психофизиологическое исследование при помощи полиграфа позволит получить инструментальное доказательство наличия агрессивности как психологического свойства личности.

ЛИТЕРАТУРА

1. Венерина О.Г. Оперативная психодиагностика личности в ходе психофизиологического исследования с применением полиграфа / О.Г. Венерина, А.П. Сошников // Вестник МГГУ им. М.А. Шолохова. – 2005. – № 7. – С. 10–12.

2. Иванов Р.С. Индивидуальный симптомокомплекс как инструмент интерпретации результатов психофизиологического исследования с применением полиграфа // Национальный психологический журнал. – 2014. – № 3 (15). – С. 90–97.

3. Ермаков П.Н. Индивидуальные особенности стрессорного реагирования во время психофизиологического исследования с применением полиграфа / П.Н. Ермаков, Е.В. Воробьева, Г.Г. Яцык // Российский психологический журнал. – 2016. – Т. 13, № 2. – С. 156–168.

4. Харский К.В. Благонадежность и лояльность персонала. – СПб.: Питер. – 2003. – 496 с.

5. Леонгард К. Акцентуированные личности. – Ростов н/Д: Изд-во «Феникс», 2000. – 544 с.

УДК 343.95, 343.98

СИМВОЛ «БЕСКОНЕЧНОСТЬ» В УСТНОЙ И ПИСЬМЕННОЙ РЕЧИ ШИЗОИДА И ЦИКЛОИДА: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

А.А. Коркина, студентка каф. ИГПиПОИД
Научный руководитель Р.Л. Ахмедшин, проф. каф. ГПДиПД
г. Томск, ТУСУР, nastakorkina40@gmail.com

В целях идентификации нередко необходимо определить авторство текста при наличии нескольких подозреваемых. Анализ символической составляющей текста позволяет идентифицировать автора на уровне психологического типа.
Ключевые слова: циклоид, шизоид, интроверт, экстраверт, бесконечность.

При расследовании преступлений часто возникает необходимость идентификации автора текста хотя бы на групповом уровне.

Человек по своей природе является либо экстравертом, либо интровертом, что позволяет условно выделить две группы. Каждая группа включает в себя определенные психотипы личности. Так, шизоид является интровертом, а циклоид относится к экстравертам. Поэтому данные психотипы кардинально отличаются друг от друга и у них совершенно разные «взгляды» на окружающий мир.

Рассмотрим представленные психотипы личности. Циклоид – это человек, который является психически амбивалентным, соединяет в себе противоположности, интеллектуальный и циничный [1]. Для данного психотипа характерно активное использование в речи таких категорий, как противоположность, глобальность, космичность, жизнь-смерть. Шизоиды – это созерцатели, имеющие слабо развитые навыки общения и выраженный аналитический склад ума [2]. Для данного психотипа характерно использование в речи таких категорий, как отсутствие границ, чуждость, негативизм, мрачность, самодостаточность и погружение в свои мысли и личное восприятие.

Видение мира у данных психотипов разное, и каждый символ они расценивают с точки зрения своего восприятия. Для того чтобы определить, что такое «бесконечность» для шизоида и циклоида, рассмотрим некоторые понятия.

Термин «символ» представляет собой некоторую единицу, которая несет в себе значение и отчетливо обозначает границы, которые позволяют ясно выделить его из окружающего контекста [3].

Так какое же отличие символа «бесконечность» у шизоида и циклоида? Как смысловой подтекст данного символа позволит идентифицировать тот или иной психотип?

Как уже было сказано выше, шизоид и циклоид являются абсолютно противоположными друг другу. Можно сказать, что циклоид – это такой психотип личности, который уверен, что люди поодиночке намного сильнее морально, чем те, которые имеют сочувствие и сострадание к другим индивидам. Он использует людей, получая от них нужную информацию, и удовлетворяет свои потребности от взаимодействия с ними. Можно предположить, что именно такое восприятие мира не позволяет ему выйти за рамки своего видения. Именно поэтому он является равнодушным, эгоистичным и нечувствительным к чужому горю. Бесконечность циклоида заключается в том, чтобы попытаться познать мир с другой стороны. Попытаться сочувствовать людям, помогать, быть менее строгим и требовательным к другим, стать к ним ближе. Смысловой контекст символа «бесконечность» для циклоида – даль.

Шизоид – это человек, который обособлен от мира. Он мало общается с людьми, отдан сам себе и своим мыслям. Но у него очень богатый внутренний мир и красивая речь, много мыслей, которые он не может выразить. Скорее всего, он не доверяет обществу и боится, что его не поймут, не примут. Шизоидный психотип личности не умеет выражать свои мысли, он скуп на эмоции. Бесконечность шизоида заключается в том, чтобы открыться миру. Пытаться разговаривать с людьми, выражать и правильно доносить свои мысли. Смысловой контекст символа «бесконечность» для циклоида – глубина.

Как для циклоида, так и для шизоида бесконечностью является новое восприятие мира. Два данных психотипа настолько разные, что они встречаются в одной точке в бесконечности. Им тяжело понять друг друга, один из них интроверт, другой экстраверт, но у них есть общее – они пытаются дистанцироваться и держать людей как можно дальше от себя. Бесконечность циклоида заканчивается там, где начинается бесконечность шизоида.

ЛИТЕРАТУРА

1. Алексеева Т.А. Криминалистическая характеристика содержательности как структурного элемента устной речи // Вестник Том. гос. ун-та. – 2014. – № 378. – С. 159–161.

2. Литинская Д.Г. Конструктор шизоидности и одиночества в мире постмодерна // Вестник РГГУ. Сер.: Психология. Педагогика. Образование. – 2016. – № 2(4). – С. 93–101.

3. Тетерук В.А. Культурно-исторический анализ понятия «символ» // Система ценностей современного общества. – 2010. – № 12. – С. 167–174.

УДК 343.95, 343.98

ИДЕНТИФИКАЦИЯ СЕНЗИТИВА И ИСТЕРОИДА В КОНТЕКСТЕ ИСПОЛЬЗОВАНИЯ В ИХ РЕЧИ СИМВОЛА «ЧУВСТВО»

Д.В. Краус, студент каф. ИГПиПОИД
Научный руководитель Р.Л. Ахмедшин, проф. каф. ГПДиПД
г. Томск, ТУСУР, dashadff@yandex.ru

Рассматривается вопрос трактовки в речи допрашиваемого символа «чувство» в целях решения задачи изучения личности допрашиваемого и его групповой идентификации.
Ключевые слова: психотип, сензитив, истероид, символ, чувство.

Психологические типы всегда были обсуждаемой темой в достаточно далекие времена. Так, в 1921 г. К.Г. Юнг издал книгу «Психологические типы», в которой основывал свою теорию на достаточно существенном признаке – на направленности сознания и внимания человека вовне или вовнутрь, а именно что для типа важнее – объекты внешнего мира (экстраверт) или внутренние процессы души (интроверт) [1]. И в настоящее время прикладная психология стала не только предметом изучения, но и элементом практики, особенно когда речь идет, например, о допросах, выявлении преступника.

Сейчас есть множество различных психологических типологий, но наиболее удобным и усовершенствованным является типологический подход, основанный на выделении акцентуированных типов личности. В нем выделяют десять типов, которые обладают поведенческой уникальностью. Пять из них имеют выраженную экстравертную природу, а пять – выраженную интровертную. При этом у каждого психотипа имеются речевые предпочтения определенного набора символов, т.е. предметов, явлений, словесных или пластических образов, которые имеют личностный смысл [2].

Так, сензинтив является интровертным типом и самым эмоциональным, что выражается в речи в виде многотональности голоса и широком диапазоне. Из особенностей характера стоит отметить его тревожность, мнительность, эмпатию, гиперкомпенсацию, повышенную ранимость, стыдливость и стеснительность, склонность к капризам.

Истероид же является экстравертным типом, общение для него – средство продемонстрировать себя, поэтому характеризуется громким голосом, быстрым темпом и средним диапазоном голоса. Из особенностей характера стоит выделить эгоцентризм, эгоизм, сосредоточенность мыслей на себе, аморальность, неустойчивость настроения, завышенную самооценку, обидчивость при задевании личности [3].

Рассмотрев типовые свойства психотипов, можно выделить символы данных типов. Так, речь истероида характеризуется такими символами, как избранность, исключительность, «я», игра, сцена. Речь же сензентива характеризуется такими символами, как гармония, единение, связь с семьей, дорога, природа. Символы помогают идентифицировать тот или иной психотип, так как они индивидуализируют его. Однако есть одинаковые символы у совершенно разных на первых взгляд психотипов, которые затрудняют его определение. У исследуемых психотипов – это символ «чувство». Поэтому возникает вопрос: как отличить символ «чувство» у сензитива и истероида?

Слово «чувство» трактуется как бессознательный оценочный психофизиологический процесс, т.е. реакции на материальные и абстрактные факторы. Чувства – это внутренняя, изначально скрытая причина действий, которые являются реакциями на испытываемые переживания [4].

При этом, как было сказано выше, сензитив и истероид совершенно противоположны друг другу. Отталкиваясь от этого и основываясь на том, что сензитив является интровертом, можно сказать о том, что для него чувство имеет объективное основание. Сензитив видит чувственную основу явления. Чувство для него стоит в согласовании с объективными ценностями. Сензитив называет объект прекрасным или добрым не потому, что находит по субъективному чувству таким, а потому, что такое название является подходящим и другое обозначение нарушит общую ситуацию. Так, в песне «Звездный мальчик» группы «Сегодня в мире» можно увидеть психотип сензитив. В тексте четко прослеживаются очень нежные чувства о комфортности, доброте, которые имеют внешний источник. Это прослеживается в следующих строках: «он верит, что все люди могли быть добрее; …когда-то мир был большим и прекрасным» [5].

Истероид же является экстравертом, говорит о чувствах, которые он сейчас переживает, которые привязаны к нему. Чувство у истероида не привязано к объекту, можно сказать, оно над этим объектом, так как говорят они только о своих чувствах. Можно сказать и том, что чувство вне истероида не существует. С помощью выражения чувств он заявляет о себе, показывает себя. Объекты для него дают некий толчок, чтобы выразить то или иное чувство.

Таким образом, исходя из вышеизложенного, можно сделать вывод о том, что смысл, вкладываемый в символ «чувство» у истероида и сензитива, совершенно отличается. Это обусловлено разницей в психологической основе психотипов. Сензитив приписывает эмоции миру, поэтому у него наиболее ярко проявляется способность к эмпа-

тии, способность поставить себя на место другого. Объективное основание для него – важная составлявшая, поэтому его выражение чувств – это прекрасная природа, добрые люди и т.д. Чувства же у истероида идут через призму его самого. Он показывает самого себя через чувства, демонстрацию своего образа. Для него чувства – это он сам, что является типичной экстравертной позицией.

ЛИТЕРАТУРА

1. Юнг К.Г. Психологические типы [Электронный ресурс]. – Режим доступа: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://lib.unidubna.ru/search/files/psy_yung/1.pdf (дата обращения: 06.03.2023).

2. Алексеева Т.А. Криминалистическая характеристика содержательности как структурного элемента устной речи // Вестник Том. гос. ун-та. – 2014. – № 378. – С. 159–161.

3. Ахмедшин Р.Л. Лекции по правовой психологии: учеб. пособие. – Томск: ИД Том. гос. ун-та, 2019. – 454 с.

4. Ильин В.И. «Чувства» и «эмоции» как социальные категории // Вестник СПБГУ. – 2016. – № 4. – С. 28–40.

5. Сегодня в мире – «Звездный мальчик» [Электронный ресурс]. – Режим доступа: https://tekst-pesni.online/segodnya-v-mire-zvyozdnyj-malchik/ (дата обращения: 06.03.2023).

УДК 343.95, 343.98

СМЫСЛОВАЯ НАГРУЗКА СИМВОЛА «АКТИВНОСТЬ» У ГИПЕРТИМА И ЭПИЛЕПТОИДА: КРИМИНАЛИСТИЧЕСКИЙ И ПСИХОЛОГИЧЕСКИЙ АСПЕКТ

В.Д. Новикова, студентка каф. ИГПиПОИД

Научный руководитель Р.Л. Ахмедшин, проф. каф. ГПДиПД

г. Томск, ТУСУР, vdnovikova123@gmail.com

Рассматривается вопрос, посвященный отличиям символа «активность» у двух разных типов личности, а именно у гипертима и эпилептоида, а также причинам этих отличий. Использование полученных данных видится в области решения задачи криминалистического исследования личности подследственного в процессе подготовки и проведения следственного действия.

Ключевые слова: тип личности, гипертим, эпилептоид, символ «активность».

Гипертим и эпилептоид – это термины, используемые в психологии для описания некоторых особенностей характера и поведения людей.

Термин «гипертим» относится к типу личности, характеризующемуся высоким уровнем энергии, креативности и энтузиазма. Люди, обладающие данным типом личности, обычно высокомотивированы.

Их часто характеризуют как «идущих вперед» и имеющих сильное желание достичь своих целей. Они очень креативны и инновационны и часто преуспевают в таких областях, как бизнес, искусство и технологии [1].

Одной из определяющих характеристик гипертимов является их склонность к позитивной аффективности. Они склонны испытывать положительные эмоции чаще и интенсивнее, чем другие люди. Это может сделать их очень харизматичными и привлекательными, и они часто умеют мотивировать и вдохновлять других.

Гипертимы также склонны к высокому уровню уверенности в себе и самоуважения. Они не боятся рисковать и часто готовы взять на себя роль лидера. Они обладают высокой адаптивностью и могут преуспевать в самых разных ситуациях и условиях. Однако они также могут быть импульсивными и испытывать трудности с задачами, требующими внимания к деталям и структуре [2].

Термин «эпилептоид» относится к типу личности, характеризующемуся эмоциональной нестабильностью и склонностью к импульсивному и агрессивному поведению. Эпилептоиды, как правило, эмоционально чувствительны и могут испытывать сильные колебания настроения, а также трудности с регулированием своих эмоций, что влечет за собой острое реагирование на незначительные раздражения или неудачи [1].

Одной из определяющих характеристик эпилептоидов, в отличие от гипертимов, является их склонность к негативной аффективности. Они испытывают негативные эмоции чаще и интенсивнее, чем другие люди. Это может сделать их крайне раздражительными и легко расстраивающимися.

Кроме того, они остро реагируют на перемены и испытывают тревогу или расстройство, когда нарушается их привычный распорядок дня. Это может сделать их менее адаптируемыми, чем другие люди.

Что касается сильных сторон эпилептоидов, то они обладают высокой эмпатией и могут глубоко понимать эмоции и переживания других людей. Они также часто бывают очень творческими и интроспективными и могут преуспевать в таких областях, как искусство, музыка или писательство [3].

Символ «активность» в гипертимических и эпилептоидных личностях – это один из способов представить фундаментальные различия в их темпераменте. Быстро движущаяся, направленная вверх стрелка символизирует динамичную, целеустремленную натуру гипертимов, в то время как медленно движущаяся, направленная вниз

стрелка символизирует эмоциональную нестабильность эпилептоидных личностей.

Гипертим может быть очень активным и иметь много идей, проектов и планов. Однако у него присутствует склонность к поверхностности, неосторожности и несерьезности в отношении своих обязательств.

У эпилептоида, в отличие от гипертима, активность связана скорее с желанием контролировать ситуацию, чем с энтузиазмом и творческими идеями. Кроме того, он может быть склонен к принятию решений без должной оценки ситуации и последствий.

Одно из возможных объяснений этих различий в темпераменте лежит в основе нейробиологических механизмов, регулирующих поведение. Считается, что у гипертимов от природы высокий уровень активности дофамина в мозге, который связан со склонностью испытывать положительные эмоции. Напротив, у эпилептоидных людей естественный низкий уровень активности дофамина, что может привести к большей восприимчивости к негативным эмоциям и склонности к импульсивности и агрессии.

Другое возможное объяснение этих различий в темпераменте коренится в опыте раннего детства. Гипертимичные люди могли воспитываться в среде, которая поощряла исследование, рискованность и достижения, в то время как эпилептоидные люди могли чаще подвергаться стрессу, травмам или пренебрежению, что может привести к большему риску эмоциональной дисрегуляции и поведенческих проблем.

Хотя гипертимические и эпилептоидные личности часто рассматриваются как две крайности на континууме темперамента, важно признать, что люди могут проявлять черты обоих типов личности. А символы активности являются полезным инструментом для понимания сложного взаимодействия между нейробиологией, окружающей средой и темпераментом, которые способствуют индивидуальным различиям в поведении.

Таким образом, активность у гипертима и эпилептоида может отличаться по своей мотивации и организации. У гипертима активность обычно связана с высоким настроением и творческой энергией, а у эпилептоида – с желанием контролировать и управлять ситуацией.

ЛИТЕРАТУРА

1. Алексеева Т.А. Криминалистическая характеристика содержательности как структурного элемента устной речи // Вестник Том. гос. ун-та. – 2014. – № 378. – С. 159–161.

2. Савинков С. Гипертимный тип личности [Электронный ресурс]. – Режим доступа: https://www.b17.ru/article/hiperthimos/ (дата обращения: 06.03.2023).

3. Савинков С. Эпилептоидный тип личности [Электронный ресурс]. – Режим доступа: https://www.b17.ru/article/epilept/ (дата обращения: 06.03.2023).

УДК 343.95, 343.98

ТАКТИКО-КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ СМЫСЛОВОГО НАПОЛНЕНИЯ СИМВОЛА «ДВИЖЕНИЕ» У ЭПИЛЕПТОИДА И ПАРАНОИДА

Т.Д. Рыбак, студент каф. ГПДиПД

Научный руководитель Р.Л. Ахмедшин, проф. каф. ГПДиПД, д.ю.н.

г. Томск, ТУСУР, Snaketen@mail.ru

Анализируются различия на смысловом уровне в речевом использовании символа «движение» у разных психотипов на примере представителя экстравертного типа личности – эпилептоида и интровертного типа личности – параноида. Результаты проведенного исследования актуальны в рамках криминалистического изучения личности и могут быть использованы для групповой идентификации автора речевого сообщения (письменного или устного).

Ключевые слова: психотип, движение, эпилептоид, параноид.

Во время общения с другими людьми возникает проблема понимания разных смысловых конструкций между собеседниками. Данная особенность человеческой природы берет свое начало во вкладывании разного смысла в одно и то же понятие у разных психотипов, но это не единственный фактор, который влияет на разность восприятия одного и того же понятия. Сюда можно отнести и ограниченность словарного запаса, различные словообразования, национальные особенности языка и т.д.

В контексте особенностей различия в восприятии символа «движение» у эпилептоида и параноида. Стоит начать с того, что представленные психотипы являются в некоторых сферах антиподами друг другу. Так, эпилептоид является экстравертным типом. Речевые особенности данного психотипа весьма развиты, речь организована и понятна. Разговаривает эпилептоид четко и громко [1, с. 91–92]. При этом эмоциональная составляющая общения для данного психотипа остается недостаточно определенной. В общении привык доминировать, но бывают случаи, когда эпилептоид вынужден подчиняться. Несмотря на это, в речи будет сделан заметный акцент на его мнение со свойственной данному типу перманентной агрессивностью речи.

Импульсивен, за счет чего в его речи наблюдаются интонационные «скачки» в сторону усиления интонации.

Параноид является представителем интровертного типа личности. Речь среднего темпа, тон голоса ровный, речь достаточно артикулирована, без перепадов. В общении данный психотип агрессивен во время дискуссии на значимые для параноида темы, часто данные ситуации перерастают в конфликт [1, с. 95–96]. Но по сравнению с эпилептоидом более спокоен в контексте обсуждения нейтральной тематики. Данный тип старается объяснять свою позицию простыми словами, говорит четко и конкретно.

Обращаясь к символу «движение», нельзя не заметить отличное друг от друга отношение двух психотипов к восприятию и пониманию данного символа. Для эпилептоида само по себе движение является весьма значимым, он получает удовольствие от преодоления каких-либо препятствий во время самого движения. Иными словами, для эпилептоида не столь важен результат его деятельности, сколько полученные эмоции в процессе реализации этой самой деятельности, а также усилия, предпринятые во время эмоционально окрашенной деятельности. Данный психотип находится в постоянной конкуренции с другими людьми, именно поэтому характерные символы эпилептоида, такие как доминирование, действие, борьба, месть [2, с. 160], так хорошо передают его отношение к символу «движение».

Для параноида символ «движение» обозначает целевое стремление к чему-либо, у его движения всегда есть четко поставленная цель, так как его природа выражается в склонности к какой-либо сверхидее, для реализации которой параноид не пожалеет ни сил, ни средств. Из-за того, что данный тип является интровертом, его особенность к пониманию символа «движение» больше сосредоточена на внутренних ценностях, по сравнению с эпилептоидом. Характерными символами для параноида выступают: единство, самопожертвование, противостояние, путь, воля [2, с. 160], что, в свою очередь, наглядно демонстрирует отношение данного типа к символу «движение». Однако если сравнивать борьбу эпилептоида и параноида, то второй тип действует более целенаправленно и фанатично.

Таким образом, разное отношение к пониманию одного и того же символа, в первую очередь, исходит из экстравертности или интровертности типа. В последующем отличия начинают затрагивать внутренние и внешнее составляющее самого движения как деятельности, а также отличается конечный результат этой деятельности. Эпилептоид стремится преодолевать трудности или превосходить своих конкурентов, параноид стремится совершать определенную деятельность для

достижения своей сверхценной идеи. При этом эмоциональная составляющая у эпилептоида играет важную роль в процессе деятельности, возможно, агрессивность данного типа способствует его стремлению превосходить других ради самоутверждения. Параноид же не стремится получать эмоции во время реализации своей деятельности, так как мнение «чужих» для него не играет роли, а мнение «своих», по идее, совпадает с его личным.

ЛИТЕРАТУРА

1. Ахмедшин Р.Л. Лекции по правовой психологии: учеб. пособие. – Томск: ИД Том. гос. ун-та, 2019. – 454 с.

2. Алексеева Т.А. Криминалистическая характеристика содержательности как структурного элемента устной речи // Вестник Том. гос. ун-та. – 2014. – № 378. – С. 159–161.

УДК 343.144

ТАКТИЧЕСКИЙ ПОТЕНЦИАЛ АНАЛИЗА ЗРИТЕЛЬНОГО КОНТАКТА ПРИ ДОПРОСЕ

В.О. Сижук, студентка ЮИ ТГУ

Научный руководитель Р.Л. Ахмедшин,
проф. каф. уголовного права, д.ю.н.
г. Томск, ТУСУР, raist@sibmail.com

Выявлена потенциальная ценность исследования зрительного контакта для работы с подозреваемыми. Высказано предположение о взаимосвязи зрительного контакта с правдивостью озвучиваемых высказываний.

Ключевые слова: зрительный контакт, допрос, криминалистика, подозреваемые, уголовный процесс.

В российской культуре длительный зрительный контакт преимущественно оказывает подавляющее воздействие при ведении диалога и неосознанно может быть сигналом агрессии по отношению к собеседнику. Вследствие этого существуют рекомендации по минимизации по возможности зрительных контактов в стрессовых ситуациях, к примеру, контактов с преступниками при захвате заложников [1] либо с людьми в толпе, подверженной паническим настроениям [2].

Однако также зрительный контакт может сигнализировать о стремлениях лица скрыть определённые факты от собеседника или же, наоборот, озвучить правдивые высказывания. Многим людям во время разговора с трудом удаётся постоянно смотреть в глаза человеку, с которым они ведут беседу. Существует несколько версий относительно природы данного феномена. Некоторые учёные полагают,

что люди, которые откровенно избегают зрительного контакта, опасаются, что их ложь будет раскрыта [3].

В связи с этим выдвинут тезис для практического исследования о том, что целенаправленный постоянный зрительный контакт либо же его полное отсутствие может указывать на намерение собеседника сокрыть определённые факты. Тогда как возникновение зрительного контакта на последних фразах ответа на вопрос либо поднятие взгляда сразу по окончании озвученной фразы свидетельствует о правдивости сказанного.

По результатам проведенных наблюдений над группой людей возраста 20 лет в количестве 6 человек на протяжении 4 дней было выявлено, что в повседневной жизни большинство людей при приветствии поднимают взгляд на человека и сразу отводят его в сторону. Учитывая, что ежедневное приветствие практически не может быть расценено как действие, выполняя которое, человек скрывает свои истинные намерения, это свидетельствует о том, что в спокойной обстановке людям не свойственно подолгу удерживать зрительный контакт с людьми, которым они доверяют.

Также установлено, что перед тем как озвучить правдивый факт либо искреннее мнение по поводу определённой ситуации, люди отводят взгляд в сторону при начале фразы и поднимают его, произнося её окончание, либо смотрят несколько в сторону от собеседника на протяжении всего диалога, изредка поднимая взгляд. Поднятие взгляда по окончании фразы может также свидетельствовать о подсознательном запросе говорящего на доверие слушателя.

При озвучивании откровенно ложных фактов поведение наблюдаемых разнилось: некоторые старались смотреть в глаза собеседнику на протяжении всего диалога, другие начинали фразу с поднятия взгляда, третьи старались сократить любые зрительные контакты до минимума, однако никогда не применяли последовательность «взгляд в сторону в начале фразы – взгляд в глаза в конце». Вследствие этого можно заключить, что вынести окончательный вердикт о ложности сказанного подозреваемым, руководствуясь исключительно наблюдениями за его взглядом практически невозможно, однако даже на основании этого одного факта можно сделать определённые выводы.

В целом поднятие прямого и устойчивого взгляда на задающего вопрос свойственно лицам, склонным ко лжи, поскольку, как верно отмечает в своей статье К.П. Малянова [4, с. 63], произнося ложный факт, человек зачастую испытывает потребность смотреть собеседнику в глаза, чтобы последний не смог заметить его желания избежать прямого зрительного контакта.

Однако следует отметить, что простое избегание взгляда не обязательно демонстрирует неискренность. Оно также может демонстрировать, что человеку неприятна тема разговора, ему неловко отвечать на подобные вопросы, он испытывает дискомфорт от ситуации, в которой оказался.

Так, по результатам наблюдений изначальные предположения о взаимосвязи зрительного контакта и степени правдивости высказываний были подтверждены.

Технически изучение зрительных контактов людей при различных ситуациях может быть использовано при проведении допросов подозреваемых с целью выдвижения предварительных предположений о ложности либо истинности озвученных допрашиваемыми фраз.

Разумеется, откровенная ложь не всегда является показателем причастности к преступлению. Она может выступать в качестве защитной реакции допрашиваемого, при которой с помощью лжи он старается защититься от ошибочных подозрений, опасаясь неблагоприятного толкования истинных фактов. Однако выявление ложных высказываний может помочь охарактеризовать мотивы деятельности подозреваемого и позволить уточнить обстоятельства дела, в том числе, путём выявления лжи в высказываниях невиновных лиц с последующим указанием на данный факт.

Таким образом, исследование значения зрительного контакта может помочь при допросе подозреваемого и установлении реальных обстоятельств дела.

ЛИТЕРАТУРА

1. Правила поведения при захвате в заложники [Электронный ресурс]. – Режим доступа: https://69.mchs.gov.ru/deyatelnost/poleznaya-informaciya/pri-ugroze-terroristicheskih-aktov/pravila-povedeniya-pri-zahvate-v-zalozhniki, свободный (дата обращения: 06.03.2023).

2. Правила поведения в толпе: как выжить во время давки [Электронный ресурс]. – Режим доступа: https://ria.ru/20080804/150102236.html, свободный (дата обращения: 08.03.2023).

3. Психологи разобрались, почему люди редко смотрят в глаза собеседнику [Электронный ресурс]. – Режим доступа: https://www.mk.ru/science/2016/11/28/psikhologi-razobralis-pochemu-lyudi-redko-smotryat-v-glaza-sobesedniku.html, свободный (дата обращения: 08.03.2023).

4. Малянова К.П. Тактика выявления ложных показаний при проведении допроса // Криминалистика: вчера, сегодня, завтра. – 2020. – № 4 (16). – С. 60–66.

УДК 343.95, 343.98

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ СИМВОЛОВ НА ПРИМЕРЕ СИМВОЛА «ПОРЯДОК» В ТИПОВОЙ РЕЧЕВОЙ МОДЕЛИ ЗАСТРЕВАЮЩЕГО И ПАРАНОИДА

К.А. Третьякова, студентка каф. ИГПиПОИД
Научный руководитель Р.Л. Ахмедшин, проф. каф. ГПДиПД
г. Томск, ТУСУР, tretyakovakristina1312@gmail.com

Рассматривается вопрос, трактовки в речи допрашиваемого символа «порядок» в целях решения задачи изучения личности допрашиваемого в процессе групповой идентификации. Различие в смысловой трактовке символа «порядок» продемонстрировано на примере типовой речевой модели застревающего и параноида. Полученные выводы могут быть использованы как для построения модели личности подследственного, так и для решения ряда идентификационных задач.

Ключевые слова: психотип, застревающий, параноид, символ, порядок.

В настоящее время существует множество различных психологических типологий, но наиболее распространенным является подход акцентуированных типов личности, в котором есть 5 типов интровертов и 5 типов экстравертов. Все психотипы в одно понятие вносят разный смысл, поэтому рассмотрим более подробно такие типы, как застревающий и параноид. Застревающий акцентуированный тип – это типовая совокупность психологических свойств, предопределенная существованием у лица склонности к дисциплине, повышенной упорядоченности деятельности и скрупулезности. Параноидный акцентуированный тип – это типовая совокупность психологических свойств, предопределенная существованием у лица склонности к формированию сверхценных идей [1, с. 448], которые могут варьироваться у данного типа в достаточно широком диапазоне.

Стоит отметить, что параноид является интровертом, а застревающий, наоборот, экстравертом. Ярким примером параноида является Н.М. Водянова, застревающего – Ева Грин. Параноиды живут в рамках осознания своего мессианства, у данного типа черно-белое восприятие, промежутка для них не существует (т.е. либо добро, либо зло).

Примером застревающего являются носители военного архетипа, они живут правильно, по представлению их среды. Примером параноида являются носители архетипа подпольщика, они живут в согласии с целостностью системных для них идей.

В соответствии со словарем Ожегова, понятие «порядок» понимается как правила, по которым совершается что-либо, последова-

тельный ход чего-нибудь, а также правильное, налаженное состояние, расположение чего-нибудь.

«Порядок» для параноида сводится как жесткое структурирование, отсутствие лишнего, категоричность. Речь идет о сути явления, а у застревающего речь идет о самом действии (положить сюда, взвесить вот столько).

Как отмечает Т.А. Алексеева, застревающему параллельны такие символы-идеи, как дисциплина, конкретность, порядок, правила. В том числе ему присущи символы-образы – обязательства, ответственность, факт. Параноиду присущи символы-идеи – противостояние, предательство, свои/чужие, и такие символы-образы, как дело, путь, воля и судьба [2].

Поэтому, если застревающий работает в полиции, он не склонен к поиску компромисса с уголовным миром (преступниками), так как он работает в полиции, а это противоречит правилам, порядку и дисциплине. Данный тип характеризуется неготовностью преступить нормы и законы. Экстравертная ориентированность застревающего акцентуированного типа предопределяет порядок как совокупность правил, принятых в микростратосе, в котором он функционирует. Если правила нелогичны, несистемны и противоречивы, но разделяются представителями этого микростратоса, для застревающего они олицетворяют порядок. Порядок для застревающего – это устойчивая деятельность представителей его стратоса, порой безотносительно эффективности данной деятельности. Если в стратосе застревающего не осуждается или даже поощряется написание доносов, он будет их писать. Если поощряется физическое наказание доносчиков, он будет их наказывать.

В то время как параноиды. Наоборот, пластичны, они могут ради достижения сверхидеи взаимодействовать с уголовным миром, но в конце все равно накажут преступников, так как для данного типа не характерна готовность преступить нормы и законы.

Интровертная ориентированность параноидного акцентуированного типа предопределяет порядок как совокупность идей, системообразующих само существование человека, мир, в котором он функционирует. Если правила нелогичны, несистемны и противоречивы, но разделяются представителями этого микростратоса, для параноида они не будут олицетворять порядок. Параноиды склонны к ориентированию на небольшое количество системно непротиворечивых аксиом, предполагающих возможность простых решений. Порядок для параноида – это устойчивая деятельность его соратников или его одного, предопределяющая эффективность данной деятельности и даже

повышение этой эффективности. Если в стратосе параноида не осуждается или даже поощряется написание доносов, а он склонен к «каноническим» человекоориентированным правилам, он доносы писать не будет. Если в стратосе параноида осуждается написание доносов, а он склонен к стратоориентированным правилам, он, даже будучи принятым как аутсайдер, будет информировать стратоориентированные властные структуры о проблемах этой страты (государства, области, города, организации).

Таким образом, символ «порядок» у застревающего и параноида отличается тем, что для параноида порядок – это скорее символ благого мировосприятия, а для застревающего – это действие, направленное на это благо, признаваемое его окружением. Соответственно, и в своей речи (письменной или устной) застревающий при использовании символа «порядок» будет ориентироваться на внешнюю признанность оптимальности, а параноид – на его идейную непротиворечивость. В своей речи застревающий апеллирует к действиям людей, параноид – к категориям «правильно-неправильно», «добро-зло» и «черное-белое».

ЛИТЕРАТУРА

1. Ахмедшин Р.Л. Лекции по правовой психологии: учеб. пособие – Томск: ИД Том. гос. ун-та, 2019. – 454 с.

2. Криминалистическая характеристика содержательности как структурного элемента устной речи // Вестник Том. гос. ун-та. – 2014. – № 378. – С. 159–161.

СЕКЦИЯ 8

POSTGRADUATE AND MASTER STUDENTS' RESEARCH IN ELECTRONICS AND CONTROL SYSTEMS

Председатель секции – ***Покровская Е.М.****, зав. каф. ИЯ, доцент, к.филос.н.;*
зам. председателя – ***Шпит Е.И.****, ст. преп. каф. ИЯ;*
Соболевская О.В.*, ст. преп. каф. ИЯ;*
Таванова Э.Б.*, ст. преп. каф. ИЯ*

UDC 004.942

A MODEL FOR INVESTIGATING THE DEGRADATION OF CAPACITOR CAPACITANCE

N.M. Dubinin, PhD student, junior researcher, assistant of the Department of Computer Systems in Management and Design;
A.G. Yudintsev, Candidate of Technical Sciences, Director of the Research Institute of Automation and Electromechanics
Scientific supervisor T.V. Ganja, Doctor of Technical Sciences, Associate Professor of the Department of Computer Systems in Management and Design
Tomsk, TUSUR, nikita.d@inbox.ru

The article examines the lifetime of a capacitor. The authors used the method of component circuits of a multi-level computer model and built a model to determine the lifetime of the capacitor. The components of queries to the database of component parameters were also created. As a result of the constructed model and the created components of queries to the database of component parameters, the period after which the capacitor needs to be replaced was determined.
Keywords: method of component chains, methods of system analysis, databases, spacecraft, capacitor, degradation, multi-level computer model.

For a long time, the study and exploration of space has been taking place with the help of automatic spacecraft (satellites for various purposes and deep space exploration devices). Even with the current level of reliabil-

ity, spacecraft fail before the end of their active existence. This happens under various environmental influences, where degradation of different elements, including capacitors, occurs. It can lead to an increase in currents and voltages, which results in the devices failure and causes accidents [1].

The purpose of this work is to build a model to determine the lifetime of the capacitor and the current strength in the electrical circuit and to determine the period after which the capacitor needs to be replaced. In order to investigate the degree of degradation of elements and how it will affect all the device parameters, which can help to eliminate the possibility of an accident, we will use the method of component circuits of a multi-level computer model.

Structure of a multi-level computer model. To determine the frequency of how a particular component is degraded, we formed a database of component parameters. One of the columns records how the component degrades, and the other columns are filled with the values of parameters based on the results of the model (how the device will work during the degradation of the capacitor). To study the behavior of an object during degradation, a multi-level computer model was used, implemented in the domestic environment of multi-level computer modeling MARS, and it consisted of three levels: object, logical and visual.

At the object level, there is a model of the object under test, or models of its composite subsystems. The values of the parameters of the models are recalculated in intelligent control algorithms at the logical level and transferred to the object level [2].

The logical level receives data from the object level in the form of values of variables and elements, and data measuring the characteristics of a real system. It implements intelligent control algorithms, which include components that interact with databases of external influences and databases of object parameters (operational data, data on the current state and degradation of parameters).

At the visual level, which is a graphical panel of virtual instruments, an interface for visualization and intelligent control is formed, which receives data for visualization from the logical level. Based on them, the user generates setpoints, which are transmitted to the logical level with the help of controller components, where intelligent control algorithms are implemented from the components, including blocks for processing results.

The multi-level computer model is a set of components, each of which is described by its own model in the form of a system of algebra-differential equations. The universal computing core, which is part of the MARS software package, forms a system of algebra-differential equations by interrogating components from component and topological equations,

which are calculated in the time domain. In the model of the object under test, the variables whose values are to be processed and visualized are marked with measuring components that transmit the values of the variables of the analyzed model from the object level to the logical level [3].

Connecting a multi-level computer model to a database of component parameters. To connect a multi-level computer model to a database at the logical level, we used three components: the component of the database itself, which is physically connected to the database, the Select query component and the Update query component. The Select query is necessary to extract the values of the capacitance meters of the capacitor from the database and send these values to the object level and assign these values to the capacitor. The Update query is required to write the values of currents, voltage, time and other parameters to the database [4].

To implement the communication of a multi-level computer model with the database, a database was initially created in which there were several columns: nomer (degradation number), Degrad (degradation value), t (time) and I (amperage). The values from the Degrad column are extracted from the database with the help of the Select component and sent to the object level. In columns t (time) and I (amperage), the Update component records the value of the period after which the capacitor and the amperage values need to be replaced.

Figure 1 shows the database of object parameters from where data is extracted and written.

	nomer	Degrad	I	t
1	1	0,001	50	5
2	2	0,002	40	4
3	3	0,003	30	3
4	4	0,004	20	2
5	5	0,005	10	1

Fig. 1. The database of object parameters

Figure 2 shows the model at the logical level. It implements intelligent control algorithms, which include components that interact with the databases of object parameters. Figure 3 shows the model of the test object at the object level [5].

Conclusion. To determine the lifetime of the capacitor or other devices, and the current strength in them, we built a model on three levels. The analysis of the results allowed determining the deadline after which the capacitor should be replaced in order to avoid accidents on automatic spacecraft.

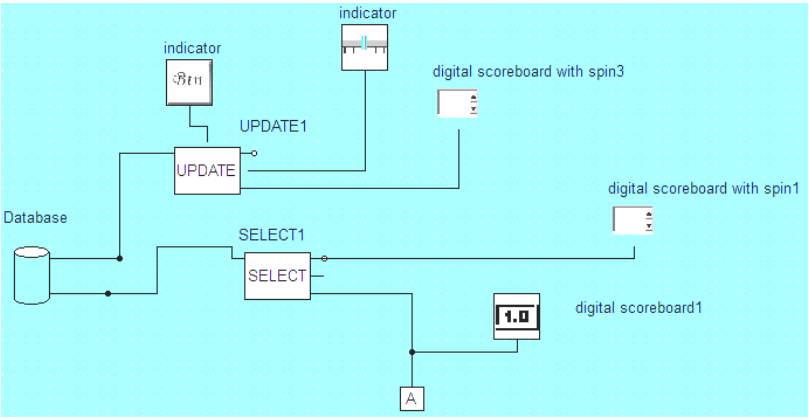


Fig. 2. The model for recording and retrieving data at the logical level

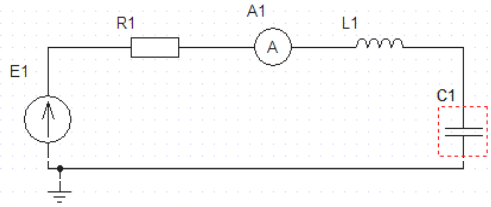


Fig. 3. The model of the test object

REFERENCES

1. Yudintsev A.G. Hardware and software complexes of simulation of power supply systems of spacecraft // Electrotechnical and information complexes and systems. – 2021. – Vol. 17, No. 1. – PP. 55–64.

2. MARS – environment for modeling technical devices and systems / V.M. Dmitriev, A.V. Shutenkov, T.N. Zaichenko, T.V. Ganzha. – Tomsk: V-Spektr, 2011. – 277 p.

3. Dmitriev V.M. Virtual laboratories and software and tools for their development / V.M. Dmitriev, A.V. Shutenkov // Computer technologies in education / Ed. by V.M. Dmitriev. – Tomsk: Publishing House un-ta, 2001. – Iss. 1. – PP. 86–94.

4. Dmitriev V.M. The principle of formation of multilevel computer models of SCADA systems for managing complex technological objects / V.M. Dmitriev, T.V. Ganzha // Informatics and control systems. – 2013. – No. 2 (36). – PP. 024–035.

5. Dmitriev V.M. Computer modeling of devices and systems / V.M. Dmitriev, A.V. Shutenkov, I.V. Dmitriev // State University of Control systems and Radio electronics. – Tomsk: TML-Press, 2010. – 293 p.

UDC 004.4

DEVELOPMENT OF A WEB INTERFACE FOR INTERACTION WITH A REMOTE LABORATORY

L.A. Gembuh, Ph.D. student of the Department of Computer Systems in Management and Design

Scientific supervisor V.M. Dmitriev, Professor of the Department of Computer Systems in Management and Design, Doctor of Technical Sciences

Tomsk, TUSUR, lev.gembuh@mail.ru

The article describes the web interface for a remote laboratory. The authors present the means of implementing the web interface and consider the proposed interface of interaction with a remote laboratory.

Keywords: web interface, python, streamlit, remote laboratory.

Now, distance learning and, in particular, remote laboratories are becoming more and more relevant. This is due to an increase in the pace of life, as well as the need to master more and more information, which is why a student does not often have time to physically be present in the laboratory and conduct experiments. In this case, remote laboratories come to the rescue, which allow students to perform laboratory work at any convenient time and from any place where there is Internet connection and a computer.

This paper describes the web interface for a remote laboratory of robotic systems. The web interface is designed for students studying in a remote laboratory. It will allow remote control of the real laboratory stands that are located in the classroom [1].

This development is relevant because it is necessary for the remote laboratory at the Department of Computer Systems in Management and Design of TUSUR. The course «Elements and devices of robotic systems» will be conducted in this laboratory.

To implement the client-server interaction of the student with the laboratory, we considered several options: creating our own web application from scratch or creating a web interface using existing libraries. To create a web interface, we chose the option of using the «streamlit» library [2]. We chose this library because it makes it quite easy to implement the necessary functionality, namely, the control of the input parameters of the remote laboratory stand and the acceptance and visualization of data received from it.

With the help of the «streamlit» library, we formed an approximate web interface for the first laboratory work (Fig. 1-2). In the first laboratory work on the course of robotics, we considered the operation of a rectifier with a filter [3].

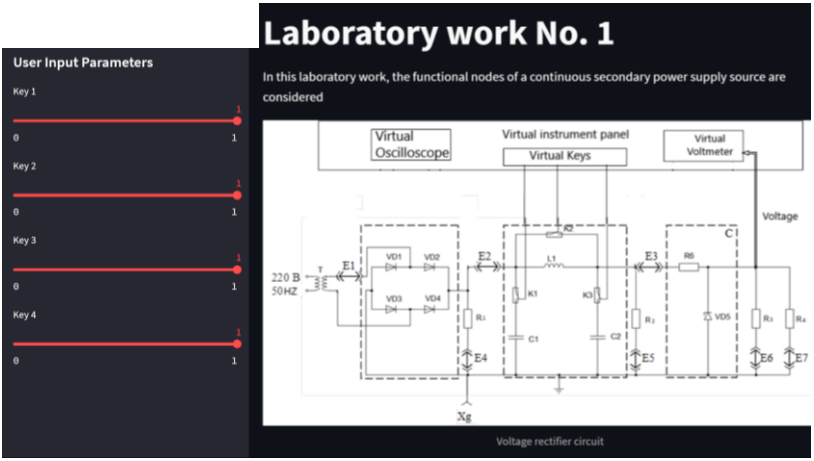


Fig. 1. Web interface for the first laboratory work

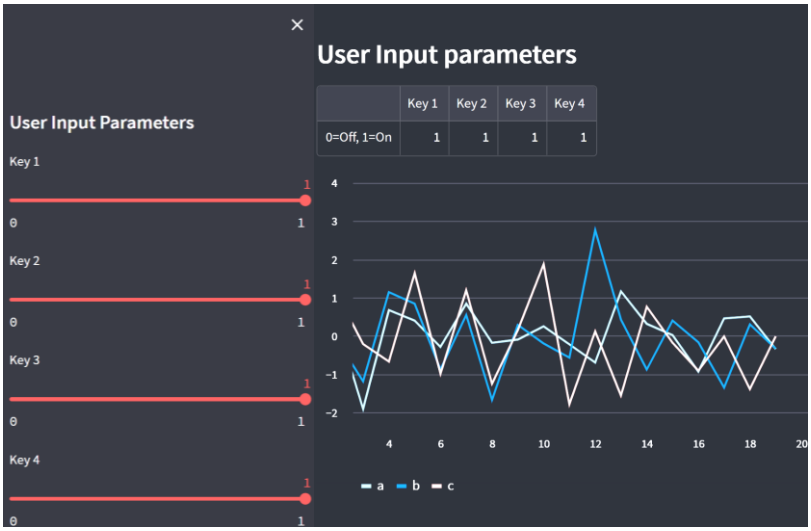


Fig. 2. Web interface for the first laboratory work

You can run the web interface in any default browser in the operating system. At the beginning, the user is presented with a diagram of the laboratory work as can be seen in Fig. 1. There are electronic keys in the diagram [4]. They can be used to control the electrical circuit, including or excluding components from the circuit. The user has the ability to manage these keys using the sidebar in the web interface. The current state of the

keys is also displayed in the table as seen in Fig. 2. After the user has set the position of the keys, a graph is plotted in the web interface illustrating the output voltage obtained from the eclectic circuit. By sequentially turning on the electronic keys, the user can observe changes in the voltage characteristic. This will allow the user to remotely study the behavior of the rectifier with a filter.

To conclude, the considered web interface makes it easy for students to interact with a remote laboratory. This web interface allows students to perform any laboratory work remotely. We will use this web interface in the laboratory of elements and devices of robotic systems in TUSUR.

REFERENCES

1. LARM: automated laboratory workshop on electrical engineering and electronics: textbook. Handbook for universities / V.M. Dmitriev, A.V. Shutenkov, T.V. Ganzha, A.N. Kurakolov. – Tomsk: V-Spektr, 2010. – 186 p. (in Russ.).

2. Streamlit [Electronic resource]. – Access mode: https://streamlit.io/ (accessed: 1.01.2022).

3. Dmitriev V.M., Gembuh L.A. Conducting laboratory work in a digital environment based on a real-virtual laboratory. In International Scientific and methodological conference «Transformation of education, science and production – the basis of technological breakthrough»: – 2022. – Vol. 1. – PP. 61–66 (in Russ.).

4. Kudryavcev I.A. Elektronnye klyuchi: uchebnoe posobie / I.A. Kudryavcev, V.D. Falkin [Electronic keys: study guide]. – Samara: Samara State Aerospace University: – 2002. 24 p. (in Russ.).

UDC 519.612

EVALUATING THE IMPACT OF SINGULARITY EXTRACTION APPROACHES ON THE EFFICIENCY OF ANTENNA SIMULATION BY THE METHOD OF MOMENTS

D.V. Klyukin, Ph.D. student of the Department of Television and Control
Scientific adviser S.P. Kuksenko, Professor of the Department of Television and Control, Doctor of Technical Sciences
Tomsk, TUSUR, dv_klyukin@tu.tusur.ru

This study investigates different methods for singularity extraction in antenna simulations by the method of moments. The methods are considered in terms of their impact on the accuracy and computational time while simulating a flat-symmetric half-wave dipole. Our results show that the numerical approach provides the highest level of accuracy, while the analytical approach provides the shortest computational time.

Keywords: antenna, computational electromagnetics, numerical methods, method of moments, singularity extraction.

The development of antenna elements with improved radio characteristics is a key task in the design of modern radio electronics. Therefore, computer-aided design (CAD) systems based on numerical methods of electrodynamics have been widely used [1, 2]. Among these methods, the method of moments (MoM) has become a popular choice in practice [3, 4]. This paper is devoted to one of the features of the MoM – the problem of singularity in the solution of electric field integral equations. The first part of the paper provides a brief overview of the MoM, explaining the singularity mechanism and discussing various approaches for its extraction. In the second part of the paper, we will review the results of numerical simulations using different approaches and discuss the accuracy and computational time.

In the MoM, the conductive surfaces of the antenna are replaced by equivalent surface currents, which are then used to solve the electromagnetic field excitation problem. To approximate the curved boundaries of antenna surface geometries, they are often represented as triangular polygonal meshes. The current within each mesh cell is described by Rao-Wilton-Glisson (RWG) basis functions. Each function is associated with a common edge between two adjacent triangles T_n^+ and T_n^- [5]. This function of the edge element approximately corresponds to a small but finite electric dipole [6]. The problem is reduced to solving a system of linear equations of the form $\mathbf{ZI} = \mathbf{V}$, where $\mathbf{Z}$ is the impedance matrix, $\mathbf{V}$ is the voltage excitation vector, and $\mathbf{I}$ is the desired vector of current density distribution on the model surface. The impedance matrix $\mathbf{Z}$ describes the interaction between different elementary dipoles. If the edge elements m and n are treated as small electric dipoles, the matrix element z_{mn} describes the contribution of dipole n (through the radiated field) to the electric current of dipole m, and vice versa [6]. This interaction is described by integrating the Green's function over the source triangles $T_n^{\pm}$ with observation points at the midpoint of the triangles $T_m^{\pm}$:

$$\int_{T_n} g(\mathbf{r})dS = \int_{T_n} \frac{\exp\left(-jk|\mathbf{r}-\mathbf{r}'|\right)}{|\mathbf{r}-\mathbf{r}'|} dS \,,$$

where $\mathbf{r}$ is the observation point and $\mathbf{r}'$ is the source point. However, when computing the diagonal elements of the matrix $\mathbf{Z}$, a singularity occurs due to the fact that $\mathbf{r}$ and $\mathbf{r}'$ are located at the same position, causing $|\mathbf{r} - \mathbf{r}'|$ being equal to 0.

Several approaches based on numerical and analytical solutions of integral equations are known to extract this computational specificity. The numerical approach involves dividing the triangular mesh element used for integration into nine sub-triangles [6, 7]. Assuming that the integrand re-

mains constant within each sub-triangle, the original integral can be simplified as follows:

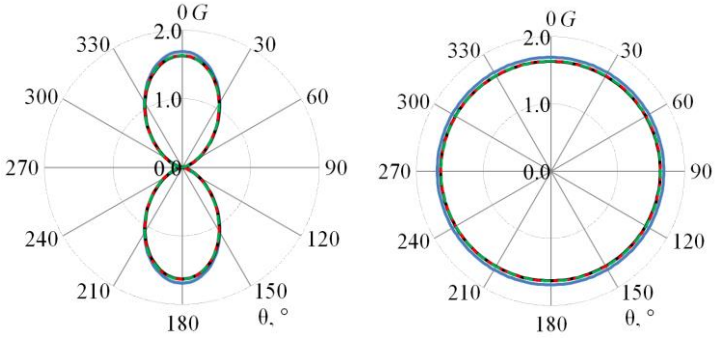
$$\int_{T_n} g(\mathbf{r})dS = \frac{S_n}{9}\sum_{k=1}^{9} g(\mathbf{r}_k^c)\,,$$

Where $\mathbf{r}_k^c$, $k = 1, \ldots, 9$ are the midpoints of nine sub-triangles and S_n is the area of the primary triangles.

An alternative approach is to calculate integrals in an analytical form [7–9]. This approach first simplifies the problem by using a Taylor series expansion [10, 11]. Afterwards, analytical expressions are used to evaluate the integral [12].

To compare the results of these approaches, we considered a model of a flat, symmetrical half-wave dipole at a frequency of 75 MHz. The antenna was simulated with λ/60 cells per wave-length. The obtained characteristics were compared with similar results obtained by finite-difference time-domain (FDTD) simulation in the EMPro software package [13]. In addition to the classical approaches, we also considered their combination. This involves using analytical expressions to calculate the diagonal elements of the matrix, while all other elements are calculated using barycentric subdivision into 9 sub-triangles.

Figure 1 shows a comparison of the antenna radiation pattern (RP) in the *E* and *H* planes. As can be seen, the results of all approaches are in good agreement with those of EMPro. The maximum deviation from the reference values is 0.05. Table shows the calculated values of the antenna input impedance. It can be seen that the numerical approach gives results that are closest to EMPro simulation, with a deviation of 0.18%. The maximum deviation was obtained for the combined approach with a deviation of 1.23%.



a *b*

Fig. 1. RPs of the dipole antenna in the *E* (*a*) and *H* (*b*) planes: EMPro (—), analytical (- - -), numerical (- - -), and combined (- - -) approaches

Calculated values of dipole input impedance (Ohm) and their deviations (in brackets) compared to EMPro

Approaches			EMPro
Analytical	Numerical	Combined	
95.32 + *j*43.52 (0.37%)	95.91 + *j*42.68 (0.18%)	94.18 + *j*43.81 (1.23%)	97.51 + *j*39.4

We estimated the time required to compute the matrix **Z**, which has dimensions of $N \times N$, for each approach as N sequentially increased from 941 to 27528 (Fig. 2). Our results indicate that the time required to compute the matrix **Z** increases exponentially with the matrix dimensions when applying numerical and combined approaches, whereas the analytical approach is more linear in nature. Specifically, when computing the matrix with a dimension of $N = 27528$, the analytical approach reduced the time required to generate the matrix by a factor of 8.5.

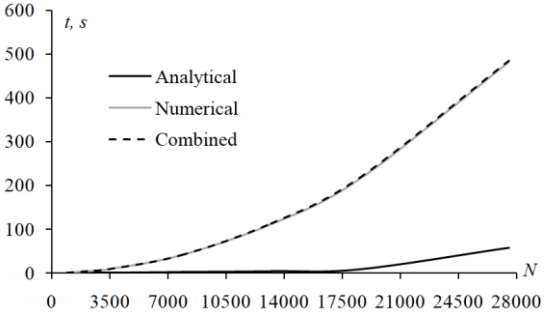


Fig. 2. Time required to compute the matrix **Z** as a function of its dimensionality

An evaluation of the impact of singularity extraction approaches on antenna simulation by the MoM has been conducted. Based on the example of a flat symmetric half-wave dipole, we demonstrated that the numerical approach yields more accurate results, while the analytical approach requires less computational time. Thus, we recommend employing the analytical approach when quick preliminary results are required, and the numerical approach for more accurate calculations.

This research was funded by the Ministry of Science and Higher Education of the Russian Federation project FEWM-2022-0001.

REFERENCES

1. Bankov S.E. Electrodynamics for UHF CAD users / S.E. Bankov, A.A. Kurushin. – M.: Solon-Press, 2017. – 316 p. (in Russ.).

2. Grigoryev A.D. Methods of computational electrodynamics. – M.: Fizmatlit, 2013. – 430 p. (in Russ.).

3. Balanis C.A. Antenna theory: analysis and design. – 3rd ed. – New York: John Wiley & Sons, 2005. – 1097 p.

4. Mitra R. Computational methods in electrodynamics. – M.: Mir, 1977. – 487 p. (in Russ.).

5. Rao S. Electromagnetic scattering by surfaces of arbitrary shape / S. Rao, D. Wilton, A. Glisson // IEEE Transactions on antennas and propagation. – 1982. – Vol. 30, No. 3. – PP. 409–418.

6. Kamen Y. Triangle rendering using adaptive subdivision / Y. Kamen, L. Shirman // IEEE Computer graphics and applications. – 1998. – PP. 95–103.

7. Makarov S.N. Antenna and EM modeling with MATLAB. – New York: John Wiley & Sons, 2002. – 288 p.

8. Makarov S.N. Low-frequency electromagnetic modeling for electrical and biological systems using MATLAB / S.N. Makarov, G.M. Noetscher, A. Nazarian. – New Jersey: John Wiley & Sons, 2015. – 598 p.

9. Kostarev I.S. Analytical estimation of elements of SLAE matrix in the problem of electromagnetic scattering by surfaces of arbitrary shape / I.S. Kostarev, T.R. Gazizov, Y.M. Kazantsev // Numerical methods and problems of organization of calculations. Notes of scientific seminars of the St. Petersburg branch of the Steklov Mathematical Institute of RAS. – 2013. – Vol. 419. – PP. 154–167 (in Russ.).

10. Analytical evaluation of the MoM matrix elements / L. Alatan, M.I. Aksum, K. Mahadevan et al. // IEEE Trans. Microw. Theory & Techn. – 1996. – Vol. 44, No. 4. – PP. 519–525.

11. Chua E.K. Accurate and efficient computation of MoM matrix involving 2D triangular basis function with line matching / E.K. Chua, K.Y. See, Z.N. Liu // International Journal of computational methods. – 2006. – Vol. 3, No. 3. – PP. 355–370.

12. Eibert T.F. On the calculation of potential integrals for linear source distributions on triangular domains / T.F. Eibert, V. Hansen // IEEE transactions on antennas and propagation. – 1995. – Vol. 43, No. 12. – PP. 1499–1502.

UDC 621.315.612

ELECTRON BEAM MODIFICATION OF CHARACTERISTICS OF MN-ZN-FERRITE POWDER

A.M. Lakoza, postgraduate student of the Department of Microwave and Quantum Radio Engineering;
V.P. Kosteletsky, Candidate of Technical Sciences, the Department of Television and Control
Scientific adviser A.M. Zabolotsky, Head of the Department of Microwave and Quantum Radio Engineering, D.E.Sc.
Tomsk, TUSUR, alexandrlakoza@mail.ru

The paper discusses the influence of electron beam processing on the characteristics of Mn-Zn ferrite powder. The plots of spectrum reflec-

tance for the modified and original samples in the range from 700 to 1500 nm have a noticeable discrepancy. For the samples under study, a family of frequency dependences of the impedance and transfer coefficient was obtained. The analysis of electrical conductivity of samples showed a decrease in the resistance index of the modified sample by 2.43 times relative to the original one.
Keywords: electrical conductivity, Mn-Zn ferrite powder, transmission coefficient, reflection spectrum, ohmic resistance.

In order to increase the efficiency of radioelectronic equipment, methods aimed at changing the structure and properties of the surface and near-surface layers of ferromagnetic materials are used. Works [1, 2] propose methods for changing the characteristics and properties of solid ferrite products, represented by toroids, bars, cups, etc. The main disadvantage of these methods is the fact that the structural processing of a monolithic material is carried out to a relatively shallow depth (of the order of 150 μm).

We have proposed a technical approach in which electron-beam processing of a material in a powdered state takes place [3]. This approach allows uniform processing of the entire volume of the ferrite material. In the future, the modified Mn-Zn-ferrite powder can be used by the industry as an independent shielding/radio-absorbing coating. In addition, it can be used as an alloying additive for the formation of monolithic ferrite products. The purpose of this work is to analyze the degree of influence of electron beam processing on the characteristics and properties of magnetically soft Mn-Zn-ferrite powder.

As the object of study, we used polycrystalline Mn-Zn material N27, which has the following characteristics: the inductance coefficient A_L is 3270±25% nH, the initial magnetic permeability is 2000, the frequency range is from 0.025 MHz to around 0.15 MHz [4]. The source material was crushed to a powder state. The resulting powder contained fractions no larger than 0.2x0.13 mm. To process the obtained powder fraction, we used an electron-beam installation presented in [5].

The processing was performed by a fore-vacuum plasma electron source. An electron beam less than 1 mm in diameter has a power density of up to 105 W/cm2 at pressures in the vacuum chamber of the order of 5–20 Pa. The temperature during the processing reached about 600 °C with a heating rate of 100 °C/min. The total processing time was 10 minutes. The obtained material in the modified and original versions was studied using a Shimadzu UV-3600 Plus spectrophotometer [6]. To carry out the measurements, we made washers from the studied samples of materials. The resulting sample washers had a net weight of about 2.7 mg. Based on the data obtained, a graph of the reflection spectrum of the studied modified and original ferrite powders was plotted (Fig. 1).

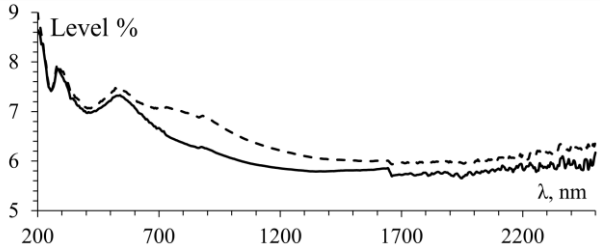


Fig. 1. Spectrogram of the studied samples of ferrite powder: original (---) and modified (—)

The sample measurement range was from 200 to 2600 nm. According to the results of measurements, in the wavelength range from 700 to 1500 nm, a significant difference was noted in the line of the modified powder relative to the original one. The analysis of the frequency dependences of the studied materials was performed using a vector network analyzer (VNA) P4226 «Panorama», with a connected coaxial camera [7].

Figure 2 and 3 show the frequency dependences of the impedance and transmission coefficients for the respective measurement options. It can be noted from the graphs that the transmission coefficient lines of the modified and original powder samples differ by about 6% in some frequency ranges. In this case, the dependence of the impedance samples at some peak frequencies fluctuates in the range from 2 to 9 ohm.

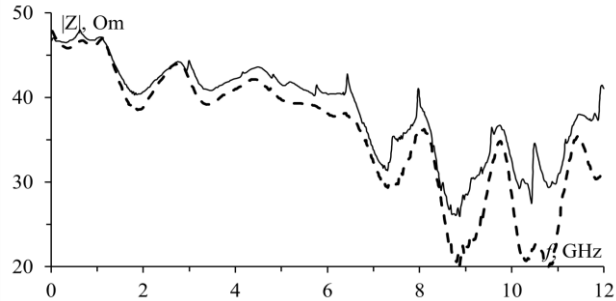


Fig. 2. Frequency dependences of impedance curves, chambers with original sample (---), chambers with modified sample (—)

Further, each of the samples was pressed into cylinders with dimensions of 14×14 mm. Then, a Rohde & Schwarz immittance meter (model Hameg HM8118) was connected to the samples, using wire contacts. According to the results of the experiment, it was found that the ohmic resistance of the original sample is 17 Ohm. The modified powder sample

showed an ohmic resistance value of 7 Ohm. Thus, the value of the ohmic resistance of the modified sample is 2.43 times lower than the original one.

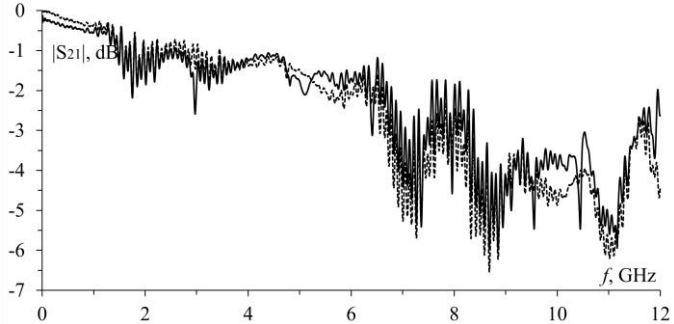


Fig. 3. Frequency dependences $|S_{21}|$: chambers with original sample (---), chambers with modified sample (—)

In this article, we investigated the effect of electron beam processing on the characteristics of Mn-Zn ferrite powder. We presented the graphs of the reflection spectrum, which show a significant difference between the line of the modified powder relative to the original one in the wavelength range from 700 to 1500 nm. Such a difference in the results is explained by a change in the composition of the substance during electron beam processing, as well as the presence of doping and binding impurities in the composition of the initial sample of the ferrite material.

The frequency dependences of the impedance and modulus S_{21} of the samples under study were also obtained. It is noted that the curves of the transfer coefficients of the modified and original powders are almost identical. In this case, the impedance curves reach a noticeable difference, which at some peak frequencies varies in the range from 2 to 9 ohm. The ohmic resistance of cylinders from the material samples was measured, according to the results of which the modified sample showed a decrease in ohmic resistance by 2.43 times relative to the original one.

REFERENCES

1. Klimov A.S. Electron beam sintering of Mn-Zn ferrites using a forevacuum plasma electron source / A.S. Klimov, I.Y. Bakeev, A.A. Zenin // Journal of Physics: Conference Series: 15, Ekaterinburg, 05–10 September 2021. – Ekaterinburg, 2021. – P. 012050.

2. Savruk E.V. Modification of the Mn-Zn-ferrite surface with a beam of low-energy electrons / E.V. Savruk, S.V. Smirnov, A.S. Klimov // Reports of the Tomsk State University of Control Systems and Radioelectronics. – 2012. – No. 2-2 (26). – PP. 172–174.

3. Lakoza A.M. Issledovanie elektricheskih harakteristik Mn-Zn-ferritovogo poroshka, modificirovannogo putem elektronno-luchevoj emissii / A.M. Lakoza,

V.P. Kosteletsky // Elektronnye sredstva i sistemy upravleniya. Materialy dokladov Mezhdunarodnoj nauchno-prakticheskoj konferencii. – 2022. – No. 1-1. – PP. 294–296.

4. Ferrite cores R40/24/16 (B64290L0659X027) [Electronic resource]. – Access mode: https://www.infinite-electronics.ru/datasheet/6e-B64290L0659X027.pdf, free (access date: 20.01.2023).

5. On the possibility of precision electron-beam processing of extended dielectric products by a plasma source of electrons in a forevacuum / I.Yu. Bakeev, A.A. Zenin, A.S. Klimov, E.M. Oks // Applied Physics. – 2017. – No. 3. – PP. 26–30.

6. UV-VIS-NIR Spectrophotometer UV-3600i Plus [Electronic resource]. – Access mode: https://www.shimadzu.ru/uv-3600-plus, free (access date: 12.01.2023).

7. Network analyzers vector series R4M-40. [Electronic resource]. – Access mode: https://dipaul.ru/catalog/element/analizatory_tsepey_vektornye_serii_r4m_40/, free (access date: 07.02.2023).

UDC 621.391.825

QUASISTATIC ANALYSIS OF AN MR-BASED STRUCTURE WITH CONDUCTORS ON THE OUTER LAYER OF THE PCB

A.V. Medvedev, postgraduate student of the Department of Television and Control

Scientific adviser T.R. Gazizov, DScTech, professor

Tomsk, TUSUR, medart20@rambler.ru

This paper presents the analysis of the characteristics of the structure with conductors on the outer layer of the printed circuit board (PCB) with modal reservation (MR). The authors consider the dependences of the difference of per-unit-length delays and the geometric mean impedances of the modes on the structure parameters. Recommendations for changing the geometric parameters to maximize the difference of per-unit-length delays are proposed.

Keywords: electromagnetic compatibility, modal reservation, printed circuit board.

When printed circuit boards (PCB) are created for critical electronic equipment, much attention is paid to electromagnetic compatibility and functional safety of electronic circuits [1]. Redundancy is a cardinal method for improving functional safety. Cold redundancy differs from hot redundancy in that if the reserved system fails, it switches over to the reserving system that was switched off. However, redundancy does not protect against the effects of systematic electromagnetic interference (EMI), since if the reserved system fails due to EMI, the reserving system will also fail.

Ultrashort pulses (USPs), which have high energy, are of short duration. To prevent the influence of USPs, technologies based on modal filter-

ing (MF) are used [2]. Modal reservation (MR) is an approach to layout and to route reserved conductors in a cold reserved system that implements MF [3]. There exist several ways to layout and route conductors of PCBs with MR. Their disadvantage is the difficulty in tracing conductors with a large number of electronic circuits. A tracing method was developed [5], which is distinguished by the presence of conductors on the outer and inner layers of the PCB. This method allows tracing conductors of the electronic circuits with a large number of components. A preliminary study of this method with non-optimized parameters was performed [6]. In further studies, it is necessary to consider the influence of the cross-sectional parameters of structures with conductors on the outer and inner layers of the PCB with MR in order to develop recommendations for optimizing the cross-sectional parameters.

The purpose of this work is to analyze the characteristics of the structure with conductors on the outer layer of the PCB with MR.

Figure 1, *a* shows the cross-sectional model. Simulating is performed in the TALGAT system [7] without taking into account losses in conductors and dielectrics. The cross-sectional parameters are: signal conductor width w = 200 μm, distance between conductors s = 200 μm, conductor thickness t = 18 μm, lower dielectric layer thickness h_1 = 200 μm, upper dielectric layer thickness h_2 = 200 μm, permittivities ε_{r1} = 10,2 and ε_{r2} = 4.

Figure 1, *b* shows the circuit diagram, which is a two-conductor structure (length l=1 m) with loads at the near and far ends, with a source of action in the active line. The load resistance $R1$–$R4$ is taken equal to the geometric mean of the even and odd mode impedances (67 Ω), while the impact has the following characteristics: the pulse shape is trapezoidal, EMF is 2 V, the duration of the rise, fall and flat top is $t_r = t_{fr} = t_d$ = 10 ps.

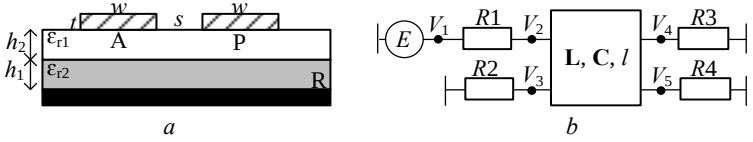
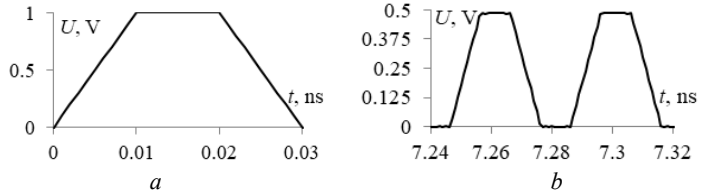


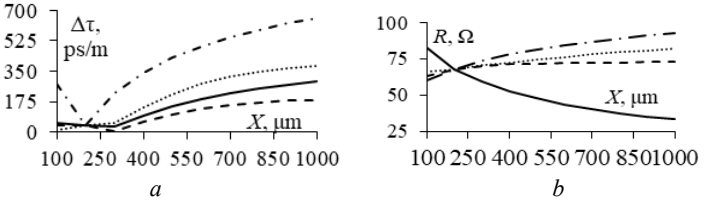
Fig. 1. Structure with conductors on the outer layer (*a*), where A is an active conductor, P is a passive conductor, R is reference; circuit diagram (*b*)

Figure 2 shows the waveforms at the near (Fig. 2, *a*) and far (Fig. 2, *b*) ends for the initial set of parameters. In what follows, all dependences of the parameters are considered with respect to this set. At the far end of the structure, two decomposition pulses of a smaller amplitude than at the near end are observed. The mode delay difference is Δt = 0.04 ns.



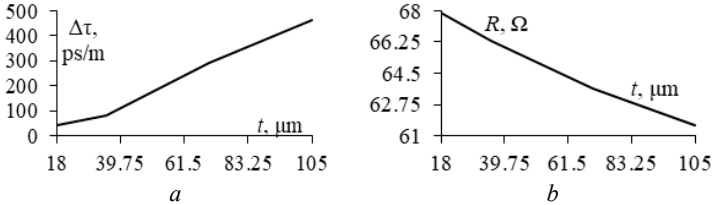
a *b*

Fig. 2. Waveforms at the near (*a*) and far (*b*) ends with the initial set of parameters



a *b*

Fig. 3. Dependences of Δτ (*a*) and *R* (*b*) on *X*, where *X* is equal to: *w* (–), *s* (---), h_1(-·-·-), h_2(…)



a *b*

Fig. 4. Dependences of Δτ (*a*) and *R* (*b*) on *t*

The presented results show that of all the considered parameters, the parameters h_1 and *t* most strongly affect Δτ. Thus, to increase Δτ, it is necessary to take each of the parameters the maximum possible, since the value of Δτ increases with an increase in each of the parameters. However, if the geometric parameters are changed as recommended, *R* will also change a lot. In cases where impedance control is required, it is necessary to monitor changes in *R*.

REFERENCES

1. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508, Available at: https://webstore.iec.ch/publication/5515 (Accessed: 03.04.2023).

2. Gazizov A.T. Measurement and Simulation of Time Response of Printed Modal Filters with Broad-Side Coupling / A.T. Gazizov, A.M. Zabolotskii, T.R. Gazizov // Journal of Communications Technology and Electronics. – 2018. – Vol. 63, No. 3. – PP. 270–276.

3. New concept of critical infrastructure strengthening /T.R. Gazizov, P.E. Orlov, A.M. Zabolotsky, S.P Kuksenko // AIP Conference Proceedings. – 2016. – Vol. 1738. – 4 p.

4. Optimization of stack parameters of multi-layer PCB for circuits with redundancy by genetic algorithm / P.E. Orlov, T.R. Gazizov, V.R. Sharafutdinov, I.F. Kalimulin // 2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). – Novosibirsk. – 2017. – PP. 463–467.

5. Gazizov T.R., Orlov P.E., Sharafutdinov V.R., Kuznetcova-Tadgibaeva O.M., Zabolotsky A.M., Kuksenko S.P., Buichkin E.N. Sposob komponovki pechatnih plat dla cepey s rezervirovaniem [PCB layout for circuits with reservation]. Patent RF, No. 2614156, 2017.

6. Medvedev A.V. Interconnect Routing on Two Signal Layers of a Modal Reservation PCB: a Case Study // 2022 International Ural Conference on Electrical Power Engineering (UralCon), 2022. – PP. 301–306.

7. Kuksenko S.P. [Preliminary results of TUSUR University project for design of spacecraft power distribution network: EMC simulation]. IOP Conference Series: Materials Science and Engineering. – Novosibirsk, – 2019. – Vol. 560. – P. 012110.

UDC 519.163

REPRESENTING COMBINATORIAL SETS DEFINED BY THE FUBINI NUMBERS IN THE FORM OF AND/OR TREE STRUCTURES

V.A. Polyuga, Master student, Department of Economic Mathematics, Informatics and Statistics

Scientific supervisor Y.V. Shablya, Associate professor, Department of Complex Information Security of Computer Systems, PhD

Tomsk, TUSUR, vadimiuspolyuga@gmail.com

This article discusses the process of developing combinatorial generation algorithms based on the use of AND/OR trees. Specifically, we study the dependence of the combinatorial generation algorithms on the cardinality functions for the same combinatorial set. As an example, we consider a combinatorial set defined by the Fubini numbers that have three different formulas satisfying the requirements of the research method.

Keywords: bijection, combinatorial set, combinatorial generation algorithms, ranking, unranking, Fubini numbers, ordered Bell numbers, AND/OR tree.

Combinatorial generation is a scientific field that combines computer science, programming, and combinatorics, and studies algorithms aimed at numbering and generating elements of a combinatorial set [1]. A combinatorial set is a finite set of elements having a certain structure, as well as

algorithms for constructing elements of this set. The simplest examples of combinatorial sets are permutations and combinations. Ranking is the process of assigning an individual number to each element of a combinatorial set. Unranking is the process of restoring an element of a combinatorial set by its rank. This article discusses the method for developing combinatorial generation algorithms based on AND/OR trees [2]. To apply this method, it is necessary to have the cardinality function of a combinatorial set that belongs to the algebra {N, +, ×, R} (only positive integers, addition, multiplication, and recursion operations).

In this article, we consider a combinatorial set defined by the Fubini numbers, also known as the ordered Bell numbers. In number theory and enumerative combinatorics, the ordered Bell numbers count several types of combinatorial sets that have a bijective correspondence (the weak orderings, the ordered multiplicative partitions of a square-free number [3], and the faces of all dimensions of a permuted polyhedron [4], etc.).

The sequence of the Fubini numbers

n	0	1	2	3	4	5	6	7	8	9	…
$F(n)$	1	1	3	13	75	541	4683	47293	545835	7087261	…

Combinatorial set. The n-th Fubini number $F(n)$ can be given by a summation formula that includes the Stirling numbers of the second kind counting the number of partitions of a set of n elements into k nonempty subsets [5, 6]:

$$F(n)=\sum_{k=1}^{n} k!\left\{{n \atop k}\right\}, \tag{1}$$

where the Stirling numbers of the second kind have the following formula:

$$\left\{{n \atop k}\right\}=k\cdot\left\{{n-1 \atop k}\right\}+\left\{{n-1 \atop k-1}\right\}, \qquad \left\{{n \atop n}\right\}=\left\{{n \atop 1}\right\}=1. \tag{2}$$

An alternative summation formula expresses the Fubini numbers using the Eulerian numbers counting the number of permutations of n elements with k sets of increasing elements:

$$F(n)=\sum_{k=0}^{n-1} 2^k\cdot\left\langle{n \atop k}\right\rangle, \tag{3}$$

where the Eulerian numbers have the following formula:

$$\left\langle{n \atop k}\right\rangle=(k+1)\cdot\left\langle{n-1 \atop k}\right\rangle+(n-k)\cdot\left\langle{n-1 \atop k-1}\right\rangle, \qquad \left\langle{n \atop n-1}\right\rangle=\left\langle{n \atop 0}\right\rangle=1. \tag{4}$$

There is a recurrence for the Fubini numbers:

$$F(n)=\sum_{k=1}^{n}\binom{n}{k}\cdot F(n-k), \tag{5}$$

where the following formula is used for calculating binomial coefficients:

$$\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}, \qquad \binom{n}{n}=\binom{n}{0}=1. \tag{6}$$

Bijection. All Formulas (1)–(6) satisfy the algebra $\{N, +, \times, R\}$. Hence, the method for developing combinatorial generation algorithms based on AND/OR trees is applicable to each formula. Based on Formulas (1)–(6), the corresponding AND/OR tree structures were constructed. Additionally, bijections between the combinatorial sets and the variants of the corresponding AND/OR tree were defined for each obtained AND/OR tree.

A bijection for Formula (1) is defined by the following rules:

1) the selected child element of the OR node determines the number of k subsets;

2) the subtree $S(n, k)$ defines the partition of a set of n elements into k non-empty subsets;

3) the subtree $P(k)$ defines the order of k subsets of elements.

A bijection for Formula (3) is defined the by following rules:

1) the selected child element of the OR node determines the number of k ascents in the ordering;

2) the subtree $E(k, n)$ defines the permutation of n elements with k ascents;

3) the subtree 2^k defines the combination of elements in k ascents.

A bijection for Formula (5) is defined by the following rules:

1) the selected child element of the OR node determines the number of k elements that together take the n-th place in a weak order of n elements;

2) the subtree $C(n, k)$ determines which k elements from the set of n elements will occupy the n-th place;

3) the subtree $F(n - k)$ determines the locations of the remaining $n - k$ elements.

Conclusion. A method for developing combinatorial generation algorithms based on AND/OR trees allows obtaining different algorithms for the same combinatorial set that have several cardinality functions. As a result, bijections between the combinatorial sets defined by the Fubini numbers and the variants of the corresponding AND/OR tree were derived. Based on the obtained results, algorithms for ranking and unranking combinatorial set can be developed.

The reported study was supported by the Russian Science Foundation (project no. 22-71-10052).

REFERENCES

1. Knut D.E. The art of computer programming. – Vol. 4A: Combinatorial algorithms, Part 1. – USA: Williams, 2013. – 960 p.

2. Kreher D.L. Combinatorial algorithms: Generation, enumeration, and search / D.L. Kreher, D.R. Stinson. – USA: CRC Press, 1999. – 329 p.

3. Sklar A. On the factorization of squarefree integers // Proc. Amer. Math. Soc. – 1952. – Vol. 3. – PP. 701–705.

4. Ziegler G.M. Lectures on polytopes. – USA: Springer, 2012. – 370 p.

5. Good I.J. The number of orderings of n candidates when ties are permitted // Fibonacci Quarterly. – 1975. – Vol. 13. – PP. 11–18.

6. Sprugnoli R. Riordan arrays and combinatorial sums // Discrete Mathematics. – 1994. – Vol. 132. – PP. 267–290.

UDC 378.14

SELECTING THE TRAINING PARAMETERS OF A CONVOLUTIONAL NEURAL NETWORK FOR RADAR IMAGE RECOGNITION

V.I. Weber, postgraduate student of the Department of Radio Engineering Systems

Scientific adviser V.Yu. Kupritz, Candidate of Engineering Sciences.
Tomsk, TUSUR, vladweber00@gmail.com

The article discusses preprocessing a heavy vehicles radar image dataset. The data has been taken from the open source Moving and Stationary Target Acquisition and Recognition (MSTAR). The authors propose a set of training parameters for a convolutional neural network to increase the probability of correct recognition of objects in a radar image.

Keywords: recognition, convolutional neural network, radar image, training database.

The problem of image recognition in various fields of human activity is still not resolved. In the image recognition task, various structures of neural networks were used in the past, for example, a multilayer perceptron. However, in 2010-2012 there was a breakthrough in the field of image recognition: convolutional neural networks (CNNs) were invented [1]. Using CNNs has increased the probability of correct image recognition. On the basis of such structures, many networks are created, and the development of these networks continues to advance. Currently, 'computer vision' algorithms (algorithms based on CNNs) are used in many different areas, such as face recognition, traffic sign recognition, autopiloting a car, etc.

In the task of pattern recognition in a radar image generated using SAR (synthetic aperture radar), studies were also conducted on the use of neural network structures, which were quite successful [2]. This article will discuss the preprocessing of a database of radar images and the choice of training parameters for a CNN in order to increase the probability of correct recognition.

Figure 1 shows the structure of a CNN for object recognition (armored personnel carrier, tank, ZIL) in a radar image [3–5].

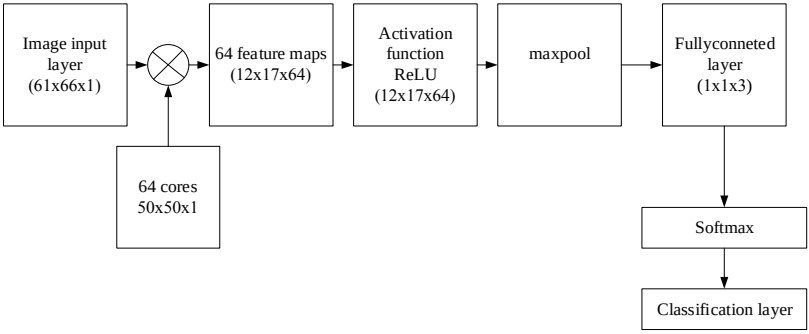


Fig. 1. Structure of a CNN in radar image recognition task

We simulated a CNN and trained it on the MSTAR database [6], which consisted of 1620 images of ground objects, of which 500 images for training were for each class of recognizable objects (armored personnel carrier, tank, ZIL), and 120 images were for validation. Also, a radar image of the airfield was taken from open sources and recognizable objects were placed on it. Examples of such images are shown in Fig. 2.

Fig. 2. An example of a radar image with the location of an armored personnel carrier

After that, using the clustering algorithm, objects were selected in the generated images (in total, 118 out of 120 images were selected) and fed to the CNN. Examples of the operation of the clustering algorithm are shown in Fig. 3 [5].

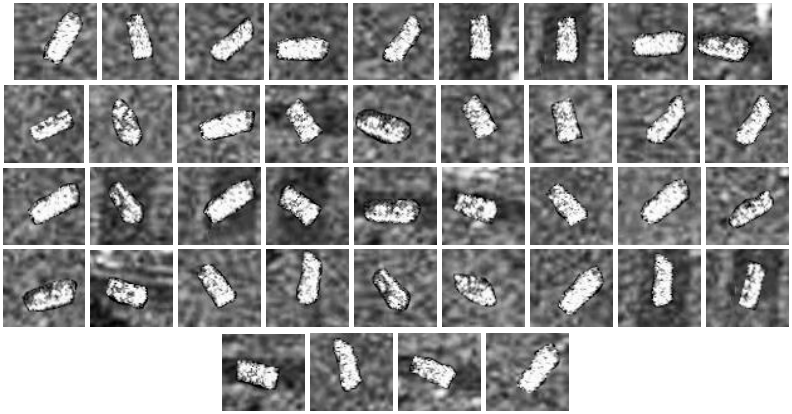


Fig. 3. Recognizable images of armored personnel carriers

Thus, the task was to determine the training parameters and to optimize the training set so that the neural network can correctly recognize the formed clusters on the radar image. The initial training parameters are shown in Fig. 4.

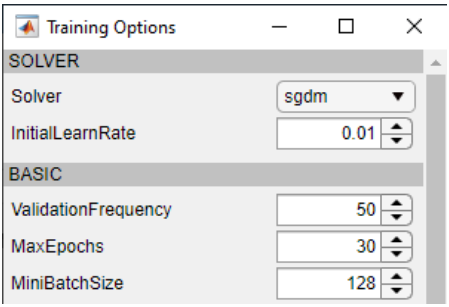


Fig. 4. Neural network training parameters for studying the dependence of correct recognition

When training the neural network on the original MSTAR database, the probability of correct recognition was not more than 50%. This result is explained by the fact that the objects have different rotations on the test set.

When importing a database for training and validation, it is possible to randomly rotate the image vertically and horizontally, along the rotation angle, and there is also the possibility of mirroring about the abscissa and ordinate axes. When choosing the values of these parameters, one should be guided by the fact that if the offset or angle deviation is too large, it is possible to cut off useful information about the target. After analyzing the training sample, the following parameters were chosen:

– mirror reflection about the axes;

– random rotation of the image vertically and horizontally: from –6 to +6 pixels;

– random image rotation: from –45 to 45 degrees.

By setting these parameters, we obtained the results showing that the network could not learn. The validation was approximately 60%. An example of training a neural network is shown in Fig. 5.

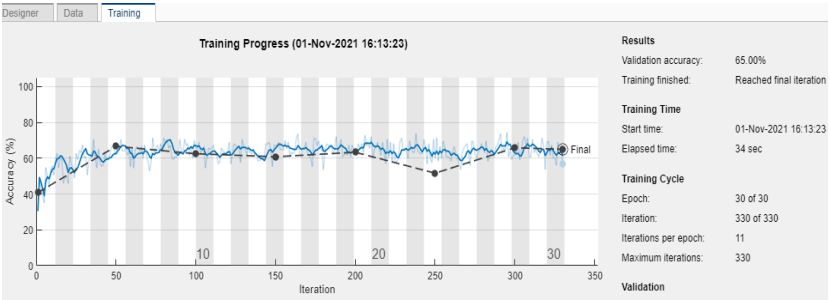


Fig. 5. Training and validation of the neural network

To improve the learning process, it is necessary to define learning parameters. Analyzing the literature and video lectures [7, 8], it was decided to double the number of epochs from 30 to 60 (each epoch contains the entire training set). This would allow reproducing all kinds of rotations and deviations that correspond to the parameters specified above. The neural network architect should also reduce the learning rate to 0.001, which means to reduce the number of corrections in the filter kernels.

As a result of network training with such parameters, the validation was 97.5%, which is shown in Fig. 6. The probability of correct recognition of the test set increased from 50 to 92.3%.

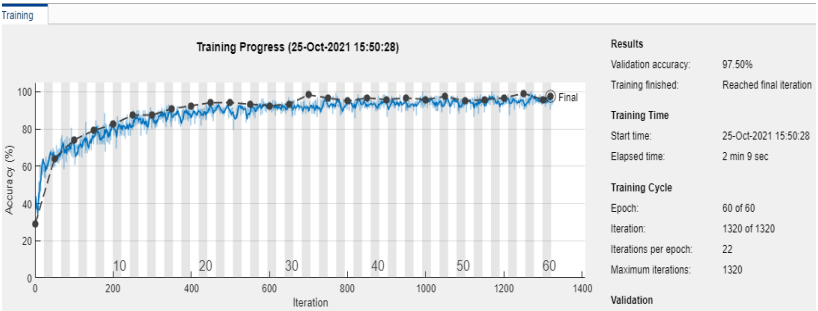


Fig. 6. Training and validation of a neural network with given training parameters

To conclude, it should be noted that data preprocessing for training the CNN can significantly improve the quality of recognition of ground objects. For example, after adding a shift and a rotation to the training set, the recognition quality increased from 50% to 92.3%.

The choice of training parameters for the neural network is necessary for correct training; without determining the parameters, the neural network will not be able to learn. For example, by defining the parameters for the training, it became possible to conduct training on a new sample with a shift and a rotation.

REFERENCES

1. What are convolutional neural networks (CNN)? [Electronic resource]. – Access mode: https://bdtechtalks.com/2020/01/06/convolutional-neural-networks-cnn-convnets/#:~:text=Convolutional%20neural%20networks%2C%20also%20called,a%20postdoctoral%20computer%20science%20researcher (Accessed: 19.04.2023).

2. Shkolny L.A. Radar systems of aerial reconnaissance, interpretation of radar images: a textbook for cadets of VVIA im. prof. NOT. Zhukovsky / L.A. Shkolny and others; ed. L.A. Shkolny. – M.: VVIA im. prof. NOT. Zhukovsky, 2008. – 531 p.

3. A visual introduction to neural networks using the example of digit recognition. [Electronic resource]. – Access mode: https://www.pvsm.ru/python/270162/print/ (Accessed: 01.15.2021).

4. Convolutional network in python. – Part 1. Determination of the main parameters of the model [Electronic resource]. – Access mode: https://proglib.io/p/neural-network-course (Accessed: 01.15.2021).

5. Weber V.I. Development of an algorithm for a recognition system using a convolutional neural network // Scientific session TUSUR–2021: materials of the International scientific and technical conference of students, graduate students and young people scientists, Tomsk, 2021: in 3 parts. – Tomsk: V-Spectr, 2022. – Part 1. – 286 p.

6. MSTAR Dataset. Dataset radar image dataset of heavy vehicle. Access mode: https://www.sdms.afrl.af.mil/index.php?collection=mstar (Accessed: 01.15.2021).

7. Gopi E.S. Pattern Recognition and Computational Intelligence Techniques Using Matlab. – Department of Electronics & Communications Engineering National Institute of Technology Trichy Tamil Nadu, India, 2020. – 263 p.

8. Knyaz V.A. Automatic target recognition based on deep learning in the tasks of homing aircraft weapons, FSUE 'GosNIIAS', 2019. – 11 p.

UDC 621.372.6

VERIFYING THE ALGORITHMS FOR CALCULATING CASCADE COUPLING OF MICROWAVE DEVICES

K.D. Zaikov, K.A. Yarkov, postgraduate students,
Department of Radio Engineering Systems
Scientifics adviser A.S. Anikin, Candidate of Engineering Sciences,
Tomsk State University of Control Systems and Radioelectronics,
Tomsk, TUSUR, kirill.d.zaikov@tusur.ru

The paper presents the calculation of the scattering matrix of cascade-connected microwave devices. The authors verified the methods for cascading microwave devices: the method of block S-matrices and the method of "free and coupled arms". The factors that reduce the calculation accuracy are listed, and one of these factors is demonstrated.
Keywords: multipole, wave matrix, cascade connection, S-parameters, S-matrix measurement process.

At the stage of designing microwave paths of radio engineering devices, the verification of selected components is carried out with the help of simulating or calculating device characteristics in CAD systems [1]. Usually, the manufacturers of UHF radio components provide scattering matrices in the datasheets. Using these matrices, engineers perform necessary calculations.

One way to check the resulting characteristics of a path (e.g., bandwidth, bandwidth irregularity) or of a module as a whole is based on the use of CAD. The user loads Touchstone files (files containing S-matrices for measured frequencies) into the CAD system and, after starting, analyzes the resulting data.

In relation to the Russian Federation, sanctions were introduced prohibiting foreign software. In addition, home-produced programs are limited. Therefore, engineers resort to implementing algorithms for cascade connection of microwave devices to analyze the designed microwave path.

Let us note the universal algorithms for calculating microwave devices:

- the block-based S-matrix method (method {1});
- the block-based T-matrix method (method {2});
- the method of «free and coupled arms» (method {3}).

Methods {1} and {2} are described in [2]. Method {3} is described in [3]. Method {2} is the most attractive due to the simplicity of calculating the scattering matrix of two cascade-connected devices. However, this method has a limitation related to the equal number of ports at the input and output of the devices, so we will not consider it further.

The verification of these methods was described in [4, 5]. In the conclusions, these articles mentioned the low correlation of the results, as well as the absence of the reason for such accuracy in calculations. In what follows, we repeat the verification step of these methods. Based on the verification results, we clarify the inaccuracies obtained in the works [4, 5].

To verify the algorithms, we measured S-parameters of two power dividers DMS2A-26-13p manufactured by «Micran» [6]. The measurements were made on a Planar series Cobalt C1220 vector circuit analyzer with pre-calibration.

The assembled divider circuit is shown in Fig. 1. Arabic numerals without a circle are numbers of ports (PN) of the divider according to the datasheet. Roman numerals represent the order of ports in measurements and calculations. Arabic numerals in circles are PNs of the resulting device.

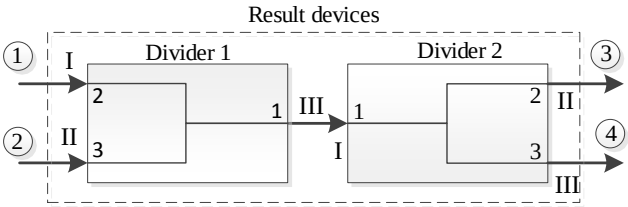


Fig. 1. Divider circuit

During the measurement process, it was found that the position of the coaxial cable affects the measured parameters. An example is shown in Fig. 2.

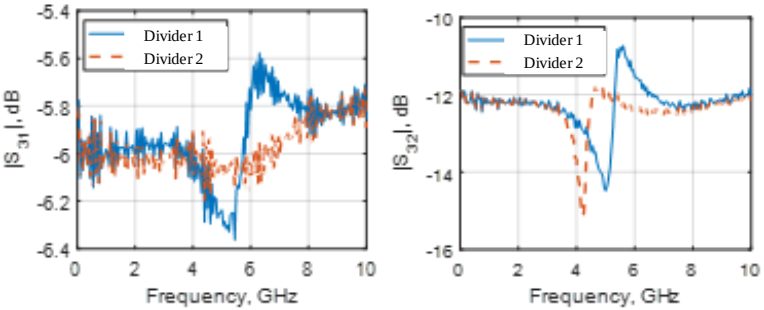


Fig. 2. Measured S_{31} and S_{32} parameters of Dividers 1 and 2

Figure 2 shows the anomalous measurements in the range from 3.5 to 6 GHz, which are caused by the position of the microwave cable. Table demonstrates the accuracy of the calculation with and without taking into account the anomalous frequency ranges (AFR).

Calculation accuracy of the scattering matrix of the final device

Coefficient	Reflections, dB	Transmissions, dB	Decoupling, dB
Excluding AFR	0.747	0.25	0.464
Including AFR	0.617	0.234	0.329

As can be seen from Table 1, the calculation accuracy increases. Note that both methods of calculating the scattering matrix of the final device produced similar results. Since the calculation error does not exceed 1 dB, the algorithms can be considered as verified.

Thus, we can distinguish the following main reasons that reduce the accuracy in calculating the scattering matrix of cascade-connected microwave devices:

1) use of low-quality coaxial cables;

2) ignoring S-parameter measurements of identical microwave devices;

3) application of partial calibration;

4) deviation from the measurement methodology.

Similarly, the works [4, 5] may have used low-quality tooling. As a result, it was impossible to say unequivocally about the verification of these algorithms.

REFERENCE

1. Active phased antenna arrays / V.L. Gostyukhin. [et al.]; ed. by V.L. Gostiukhin. – M.: Radiotekhnika, 2011. – 304 p.

2. Sazonov D.M. Microwave devices / D.M. Sazonov, A.N. Gridin, B.A. Mishustin. – M.: Higher School, 1981. – 295 p.

3. Handbook on the Calculation and Design of Microwave Banded Devices / S.I. Bakharev, V.I. Volman, Y.N. Lieb et al.; Ed. by V.I. Volman. – M.: Radio and Communications, 1982. – 328 p.

4. Zaikov K.D. Verification of algorithms for calculation of cascade connection of multipoles // Collection of selected papers of TUSUR Scientific Session. – 2021. – No. 1-1. – PP. 22– 25.

5. Kuular Ch.M. Calculation of the resulting wave matrix of the cascade connection of microwave devices / Ch.M. Kuular, K.D. Zaikov // Selected papers of the TUSUR Scientific Session. – 2021. – No. 1-1. – PP. 25–28.

6. Power dividers. Elements of the microwave path. JSC «Mikran» Available at: https://www.micran.ru/productions/IIS/accessory/divider/divider/, free (Accessed: September 21.09.2022).

СОДЕРЖАНИЕ

Секция 4
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Подсекция 4.1
МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
*Председатель – **Шелупанов А.А.**, президент ТУСУРа, директор ИСИБ, д.т.н., проф.;*
*зам. председателя – **Новохрёстов А.К.**, доцент каф. КИБЭВС, к.т.н.*

Подсекция 4.2

ЦИФРОВЫЕ СИСТЕМЫ РАДИОСВЯЗИ И СРЕДСТВА ИХ ЗАЩИТЫ

*Председатель – **Голиков А.М.**, доцент каф. РТС, к.т.н.*

Подсекция 4.3

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

*Председатель – **Кузьмина Е.А.**, директор Международной цифровой академии, к.т.н.;*
*зам. председателя – **Колтайс А.С.**, ст. преп. каф. ЭБ*

Секция 5

ЭКОНОМИКА, УПРАВЛЕНИЕ, СОЦИАЛЬНЫЕ И ПРАВОВЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ

Подсекция 5.1

МОДЕЛИРОВАНИЕ В ЭКОНОМИКЕ

*Председатель – **Мицель А.А.**, проф. каф. АСУ, д.т.н.;*
*зам. председателя – **Грибанова Е.Б.**, доцент каф. АСУ, к.т.н.*

Подсекция 5.2

ИНФОРМАЦИОННЫЕ СИСТЕМЫ В ЭКОНОМИКЕ

*Председатель – **Исакова А.И.**, доцент каф. АСУ, к.т.н.;*
*зам. председателя **– Григорьева М.В.**, доцент каф. АСУ, к.т.н.*

Подсекция 5.3

РЕАЛИЗАЦИЯ СОВРЕМЕННЫХ ЭКОНОМИЧЕСКИХ ПОДХОДОВ В ФИНАНСОВОЙ И ИНВЕСТИЦИОННОЙ СФЕРАХ

*Председатель – **Васильковская Н.Б.**, доцент каф. экономики, к.э.н.;*
*зам. председателя – **Цибульникова В.Ю.**, зав. каф. экономики, к.э.н.*

Подсекция 5.4

ПРОЕКТНЫЙ МЕНЕДЖМЕНТ И ЕГО ИСПОЛЬЗОВАНИЕ В ЦИФРОВОЙ ЭКОНОМИКЕ

*Председатель – **Афонасова М.А.**, зав. каф. менеджмента, д.э.н., проф.;*
*зам. председателя – **Богомолова А.В.**, доцент каф. менеджмента, декан ЭФ, к.э.н.*

Подсекция 5.5

СОВРЕМЕННЫЕ СОЦИОКУЛЬТУРНЫЕ ТЕХНОЛОГИИ В ОРГАНИЗАЦИИ РАБОТЫ С МОЛОДЕЖЬЮ

*Председатель – **Орлова В.В.**, зав. каф. ФиС, директор НОЦ «СГТ», д.соц.н.;*
зам. председателя – Корнющенко-Ермолаева Н.С., ст. преп. каф. ФиС

Подсекция 5.7

АКТУАЛЬНЫЕ ВОПРОСЫ ЧАСТНОГО ПРАВА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

*Председатель – **Мельникова В.Г.**, зав. каф. ИГПиПОИД ТУСУРа, к.ю.н., доцент;*
*зам. председателя – **Часовских К.В.**, ст. преп. каф. ИГПиПОИД ТУСУРа*

Подсекция 5.8

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ РОССИЙСКОГО ПРАВА

*Председатель – **Ахмедшин Р.Л.**, проф. каф. ГПДиПД, д.ю.н.;*
*зам. председателя – **Алексеева Т.А.**, доцент каф. ГПДиПД, к.ю.н.*

Секция 8

POSTGRADUATE AND MASTER STUDENTS' RESEARCH IN ELECTRONICS AND CONTROL SYSTEMS

*Председатель – **Покровская Е.М.**, зав. каф. ИЯ, доцент, к.филос.н.; зам. председателя – **Шпит Е.И.**, ст. преп. каф. ИЯ; **Соболевская О.В.**, ст. преп. каф. ИЯ; **Таванова Э.Б.**, ст. преп. каф. ИЯ*

Научное издание

Сборник избранных статей научной сессии ТУСУР

По материалам
международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2023»

17–19 мая 2023 г., г. Томск

В трех частях

Часть 3

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Сдано на верстку 25.05.2023. Подписано к печати 25.06.2023.
Формат 60×84 1/16. Печать трафаретная. Печ. л. 20,75
Тираж 100 экз. Заказ 7.

Издано ТУСУР (заказчик)
г. Томск, пр. Ленина, 40, к. 205, т. 70-15-24
Тираж отпечатан в издательстве ТУСУРа
(для нужд всех структурных подразделений университета и авторов)

Ред.-изд. подготовка оригинал-макета в эл. виде
В-Спектр (ИП Бочкарева В.М., исполнитель)
ИНН 701701817754
634055, г. Томск, пр. Академический, 13-24,
тел. 8-905-089-92-40, эл. почта: bvm-1@list.ru