ТУСУР | TUSUR UNIVERSITY

НАУЧНАЯ СЕССИЯ ТУСУР–2025

МАТЕРИАЛЫ МЕЖДУНАРОДНОЙ
НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ
СТУДЕНТОВ, АСПИРАНТОВ
И МОЛОДЫХ УЧЕНЫХ
21–23 мая 2025 г. (в четырех частях)

Часть 3

г. Томск

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

НАУЧНАЯ СЕССИЯ ТУСУР–2025

Материалы

**международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2025»**

21–23 мая 2025 г., г. Томск

В четырех частях

Часть 3

ТУСУР
В-Спектр
Томск, 2025

УДК 621.37/.39+681.518 (063)
ББК 32.84я431+32.988я431
Н 34

Н 34 **Научная сессия ТУСУР–2025:** материалы международной научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2025», Томск, 21–23 мая 2025 г.: в 4 частях. – Томск: ТУСУР (заказчик); В-Спектр (ИП Бочкарева В.М., исполнитель). – Ч. 3. – 220 с.

ISBN 978-5-902958-42-0
ISBN 978-5-902958-43-7 (Ч. 1)
ISBN 978-5-902958-44-4 (Ч. 2)
ISBN 978-5-902958-45-1 (Ч. 3)
ISBN 978-5-902958-46-8 (Ч. 4)

Материалы международной научно-технической конференции студентов, аспирантов и молодых ученых посвящены 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 978-5-902958-42-0
ISBN 978-5-902958-45-1 (Ч. 3)

Международная научно-техническая конференция студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2025», 21–23 мая 2025 г.

ПРОГРАММНЫЙ КОМИТЕТ

- Рулевский В.М. – председатель Программного комитета, ректор ТУСУРа, д.т.н., проф.;
- Куксенко С.П. – заместитель председателя Программного комитета, директор департамента науки и инноваций, д.т.н., доцент;
- Афанасьева М.А., нач. отд. международного сотрудничества ТУСУРа;
- Афонасова М.А., зав. каф. менеджмента ТУСУРа, д.э.н., проф.;
- Бабур-Каратели Г.П., к.т.н., PhD (TU Delft), научный сотрудник лаборатории радиооптики 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., с.н.с.;
- Дмитриев В.М., проф. каф. КСУП ТУСУРа, д.т.н.;
- Еханин С.Г., проф. каф. КУДР ТУСУРа, д.ф.-м.н., доцент;
- Зариковская Н.В., доцент каф. АОИ ТУСУРа, к.ф.-м.н.;
- Зейниденов А.К., PhD, зав. каф. радиофизики НАО Карагандинский университет им. академика 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., доцент;
- Костина М.А., доцент каф. УИ, к.т.н.;
- Костюченко Е.Ю., и.о. зав. каф. БИС ТУСУРа, к.т.н., доцент;
- Коцубинский В.П., зам. зав. каф. КСУП ТУСУРа, доцент каф. КСУП, к.т.н.;
- Красинский С.Л., декан ЮФ ТУСУРа, к.и.н.;
- Крозер В., проф., Университет Гёте, Франкфурт-на-Майне (Германия) (по согласованию);
- 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., проф., г. Москва (по согласованию);

- Малютин Н.Д., гл.н.с. НИИ Систем электрической связи, проф. каф. КУДР ТУСУРа, д.т.н.;
- Медовник А.В. – начальник научного управления, д.т.н., доцент;
- Мицель А.А., проф. каф. АСУ ТУСУРа, д.т.н.;
- Одинцов С.Д., гл.н.с., Институт пространственных исследований, ICE-CSIC, Барселона (Испания) (по согласованию);
- Озеркин Д.В., доцент каф. РЭТЭМ ТУСУРа, к.т.н.;
- Орлова В.В., зав. каф. ФиС ТУСУРа, д.соц.н., доцент;
- Оскирко В.О., технический директор ООО «Прикладная электроника», к.т.н. (по согласованию);
- Перин А.С., директор Передовой инженерной школы «Электронное приборостроение и системы связи» им. А.В. Кобзева, доцент каф. СВЧиКР, к.т.н.;
- Покровская Е.М., зав. каф. ИЯ ТУСУРа, к.фил.н., доцент;
- Разинкин В.П., проф. каф. ТОР, декан факультета радиотехники и электроники Новосибирского государственного технического университета, д.т.н., г. Новосибирск (по согласованию);
- Рогожников Е.В., зав. каф. ТОР ТУСУРа, к.т.н., доцент;
- Ромашко Р.В., член-корреспондент РАН, директор ИАПУ ДВО РАН, д.ф.-м.н., проф., г. Владивосток (по согласованию);
- Семенов В.Д., проф. каф. ПрЭ ТУСУРа, к.т.н., с.н.с.;
- Семенов Э.В., проф. каф. РСС ТУСУРа, д.т.н., доцент;
- Сенченко П.В., доцент каф. АОИ, к.т.н.;
- Суровцев Р.С., доцент каф. ТУ ТУСУРа, д.т.н.;
- Титов В.С., зав. каф. вычислительной техники Юго-Западного государственного университета, д.т.н., проф., заслуженный деятель наук РФ, академик международной академии наук ВШ, г. Курск (по согласованию);
- Троян П.Е., проф. каф. ФЭ ТУСУРа, д.т.н.;
- Труханов А.В., академик-секретарь Отделения химии и наук о Земле Национальной академии наук Беларуси, д.ф.-м.н., проф., г. Минск (Республика Беларусь) (по согласованию);
- 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 проектной деятельности и инноваций в промышленности института машиностроения, материалов и транспорта Санкт-Петербургского политехнического университета Петра Великого, к.т.н., г. Санкт-Петербург (по согласованию);
- Чжан Е.А., зам. директора по информационной политике Института космических и информационных технологий (ИКИТ), ФГАОУ ВО «Сибирский федеральный университет», к.т.н. (по согласованию);
- Шелупанов А.А., президент ТУСУРа, директор ИСИБ, д.т.н., проф.
- Шелупанова П.А., зав. каф. ЭБ ТУСУРа, к.э.н., доцент;
- Шурыгин Ю.А., советник при ректорате по комплексным вопросам функционирования университета ТУСУРа, зав. каф. КСУП, д.т.н., проф.;
- Шумилин А.Г., академик-секретарь Отделения физики, математики и информатики Национальной академии наук Беларуси, д.э.н., проф., г. Минск (Республика Беларусь) (по согласованию);

- Щербаков С.С., академик-секретарь Отделения физико-технических наук Национальной академии наук Беларуси, д.ф.-м.н., проф., г. Минск (Республика Беларусь) (по согласованию).

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

- Медовник А.В. – председатель Организационного комитета, начальник научного управления, д.т.н., доцент;
- Алябьева А.Д., студентка каф. ЭП, председатель Студенческого научного сообщества «Система»;
- Боберь Ю.Н., специалист по учебно-методической работе ОАиД;
- Климов А.С., председатель Совета молодых ученых, с.н.с. лаборатории плазменной электроники каф. физики, д.т.н.;
- Коротина Т.Ю., зав. аспирантурой, ОАиД, к.т.н.;
- Михальченко Т.С., специалист по работе с молодежью ОПиРШ;
- Покровская Е.М., зав. каф. ИЯ, к.фил.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 секции – Аникин Алексей Сергеевич, доцент каф. РТС, к.т.н.; зам. председателя – Мещеряков Александр Алексеевич, доцент каф. РТС, к.т.н.

Подсекция 1.2. Проектирование и эксплуатация радиоэлектронных средств. Председатель секции – Озёркин Денис Витальевич, доцент каф. РЭТЭМ, к.т.н., доцент; зам. председателя – Понамарев Дмитрий Евгеньевич, преподаватель каф. КИПР.

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

Подсекция 1.4. Интеллектуальные видеоинформационные технологии. Председатель секции – Курячий Михаил Иванович, проф. каф. ТУ, к.т.н., с.н.с.; зам. председателя – Каменский Андрей Викторович, доцент каф. ТУ, к.т.н.

Подсекция 1.5. Системы беспроводной связи и интернета вещей. Председатель секции – Рогожников Евгений Васильевич, зав. каф. ТОР, к.т.н., доцент; зам. председателя – Дмитриев Эдгар, старший преподаватель каф. ТОР.

Подсекция 1.6. Интеллектуальные системы проектирования технических устройств. Председатель секции – Шурыгин Юрий Алексеевич, советник при ректорате по комплексным вопросам функционирования университета, 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 секции – Еханин Сергей Георгиевич, проф. каф. КУДР, д.ф.-м.н., доцент; зам. председателя – Славникова Марина Михайловна, доцент каф. КУДР.

Подсекция 2.2. Разработка контрольно-измерительной аппаратуры. Председатель секции – Бомбизов Александр Александрович, начальник СКБ «Смена», к.т.н.; зам. председателя – Тренкаль Евгений Игоревич, доцент каф. КУДР, к.т.н.

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

Подсекция 2.4. Промышленная электроника. Председатель секции – Семенов Валерий Дмитриевич, проф. каф. ПрЭ, к.т.н., с.н.с.; зам. председателя – Михальченко Сергей Геннадьевич, зав. каф. ПрЭ, д.т.н.; Оскирко Владимир Олегович, технический директор ООО «Прикладная электроника», к.т.н.

Подсекция 2.5. Оптические информационные технологии, нанофотоника и оптоэлектроника. Председатель секции – Перин Антон Сергеевич, директор Передовой инженерной школы «Электронное приборостроение и системы связи» им. А.В. Кобзева, доцент каф. СВЧиКР, к.т.н.; зам. председателя – Долгирев Виктор, ассистент каф. СВЧиКР, инженер ЛФИС Передовой инженерной школы «Электронное приборостроение и системы связи» им. А.В. Кобзева.

Подсекция 2.6. Электромагнитная совместимость. Председатель секции – Суровцев Роман Сергеевич, доцент каф. ТУ, д.т.н.; зам. председателя – Белоусов Антон Олегович, доцент каф. ТУ, к.т.н.

Подсекция 2.7. Светодиоды и светотехнические устройства. Председатель секции – Туев Василий Иванович, зав. каф. РЭТЭМ, д.т.н., проф.; зам. председателя – Солдаткин Василий Сергеевич, доцент каф. РЭТЭМ, к.т.н.

Подсекция 2.8. Робототехника. Председатель секции – Коцубинский Владислав Петрович, доцент каф. КСУП, к.т.н.; зам. председателя – Шандаров Евгений Станиславович, старший преподаватель каф. ЭП.

Секция 3. Информационные технологии и системы

Подсекция 3.1. Интегрированные информационно-управляющие системы. Председатель секции – 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 секции – Сенченко Павел Васильевич, доцент каф. АОИ, к.т.н.; зам. председателя – Сидоров Анатолий Анатольевич, зав. каф. АОИ, к.э.н., доцент.

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

Подсекция 3.4. Вычислительный интеллект. Председатель секции – 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 секции – Костина Мария Алексеевна, доцент каф. УИ, к.т.н.; зам. председателя – Нариманова Гуфана Нурлабековна, зав. каф. УИ, декан ФИТ, и.о. проректора по УРиМД, к.ф.-м.н., доцент.

Подсекция 3.6. Инструментальные средства автоматизации проектирования, управления и обработки данных. Председатель секции – Хабибулина Надежда Юрьевна, 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 секции – 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 секции – Голиков Александр Михайлович, доцент каф. РТС, к.т.н., с.н.с.; зам. председателя – Громов Вячеслав Александрович, доцент каф. РТС, к.т.н.

Подсекция 4.3. Экономическая безопасность. Председатель секции – Шелупанова Полина Александровна, зав. каф. ЭБ, к.э.н., доцент; зам. председателя – Колтайс Андрей Станиславович, преподаватель каф. ЭБ.

Подсекция 4.4. Искусственный интеллект и его приложения. Председатель секции – Костюченко Евгений Юрьевич, и.о. зав. каф. БИС, к.т.н., доцент; зам. председателя – Новохрестова Дарья Игоревна, доцент каф. КИБЭВС, к.т.н.

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

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

Подсекция 5.2. Информационные системы в экономике. Председатель секции – 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 секции – Васильковская Наталья Борисовна, доцент каф. экономики, к.э.н.; зам. председателя – Цибульникова Валерия Юрьевна, зав. каф. экономики, к.э.н., доцент.

Подсекция 5.4. Проектный менеджмент и его использование в цифровой экономике. Председатель секции – 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 секции – Орлова Вера Вениаминовна, зав. каф. ФиС, д.соц.н., доцент; зам. председателя – Шевченко Лариса Владимировна, доцент каф. ФиС, к.филос.н.

Подсекция 5.6. Актуальные проблемы социальных коммуникаций в современном обществе. Председатель секции – Ким Максим Юрьевич, зав. каф. ИСР, к.ист.н., доцент; зам. председателя – Куренков Артем Валериевич, доцент каф. ИСР, к.ист.н.

Подсекция 5.7. Актуальные вопросы частного права в условиях цифровой трансформации. Председатель секции – Мельникова Валентина Григорьевна, доцент, зав. каф. ИГПиПОИД, к.ю.н.; зам. председателя – Часовских Кристина Викторовна, ст. преподаватель 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 секции – 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 секции – 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 секции – Покровская Елена Михайловна, зав. каф. ИЯ, доцент, к.филос.н.; зам. председателя – Шпит Елена Ирисметовна, ст. преподаватель каф. ИЯ; Соболевская Ольга Владимировна, ст. преподаватель каф. ИЯ; Таванова Эльвира Борисовна, ст. преподаватель 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

1 часть – 1-я секция (подсекции 1.1 – 1.6); 2-я секция (подсекции 2.1 – 2.8).

2 часть – 3-я секция (подсекции 3.1 – 3.6).

3 часть – 4-я секция (подсекция 4.1 – 4.4).

4 часть – 5-я секция (подсекция 5.1 – 5.8); 6-я секция

7 секция – для школьников издается отдельным сборником.

Генеральные спонсоры

АО «НИИПП»

Томское региональное отделение ООО «Союз машиностроителей России»

АО «НПФ «Микран»

ООО НПК «ТЕСАРТ»

АО «ИнфоТеКС»

ООО «Научные приборы и системы»

Спонсор

ООО «50ОМ ТЕХ.»

Генеральный спонсор конференции – АО «НИИПП»

АО «НИИПП»
niipp@niipp.ru
www.niipp.ru

634034, г. Томск,
ул. Красноармейская, 99а
Т.: +7 (382-2) 28-82-88,
28-84-83

Акционерное общество «Научно-исследовательский институт полупроводниковых приборов» (АО «НИИПП») – одно из ведущих предприятий Госкорпорации «Ростех», флагман в области разработки и создания СВЧ-изделий и оптоэлектронных приборов ИК- и видимого диапазонов. Общество является одним из ведущих предприятий российской электронной промышленности, специализирующихся на разработке и выпуске полупроводниковых приборов в области СВЧ- и оптоэлектроники. По нескольким позициям ассортимента предприятие выпускает продукцию, не имеющую аналогов на отечественном рынке. Текущая деятельность АО «НИИПП» направлена на то, чтобы значительно повысить конкурентоспособность и технологический уровень, которые позволят поднять уровень производительности труда и занять устойчивые позиции на внутреннем и мировом рынках радиоэлектроники. В институте налажен полный цикл от разработки до выпуска готовых изделий.

Предприятие производит продукцию для ВПК и радиоэлектронную продукцию гражданского назначения (СВЧ-ЭКБ, светотехнику, медицинские приборы, промышленную электронику).

НИИПП основан в Томске в 1964 г. для разработки СВЧ- и оптоэлектронных изделий на основе полупроводниковых соединений АЗВ5. Исследование нового материала – арсенида галия – предопределило вектор развития предприятия на последующие 60 лет.

В 1967 г. на базе института заработал завод по серийному выпуску полупроводниковых приборов. Начинавшийся как научный институт, НИИПП и сегодня работает с ведущими вузами Томска: Томским государственным университетом систем управления и радиоэлектроники (ТУСУР), Томским политехническим университетом (ТПУ), Томским государственным университетом (ТГУ), Сибирским государственным медицинским университетом (СибГМУ). В 2022 г. у АО «НИИПП» появилась вторая площадка по производству металлокерамических изделий, которая расположена в Великом Новгороде.

АО «НИИПП» входит в состав Союза машиностроителей России, являясь опорным предприятием объединения в регионе.

С октября 2020 г. генеральный директор АО «НИИПП» Е.А. Монастырев возглавляет Томское региональное отделение «СоюзМаш России».

Научно-производственный потенциал АО «НИИПП»: 4 доктора наук, 5 аспирантов, 24 кандидата технических наук, 462 конструктора и технолога.

СВЧ-электроника – одно из главных направлений разработок на предприятии – это создание СВЧ-полупроводниковых приборов, таких как генераторные (диоды Ганна), смесительные, детекторные, настроечные диоды с барьером Шоттки и монолитные интегральные схемы. На предприятии разработаны настроечные корпусные и бескорпусные диоды дм-, см- и мм-диапазонов длин волн, кремниевые и арсенидогаллиевые варикапы и варикапные матрицы, предназначенные для применения в частотно-избирательных схемах дм-, м-, декаметрового и гектометрового диапазонов длин волн. Смесительно-детекторные диоды для ГИС мм- и субмиллиметрового диапазонов типа с балочными выводами стали основой для последующего создания широкого спектра монолитных интегральных схем (МИС) мм-диапазона.

Оптоэлектроника. Параллельно с СВЧ-электроникой в НИИПП развивалось направление оптоэлектроники – от создания первых ИК-диодов на арсениде галлия (базовая технология которых послужила основой для создания высокоскоростного светодиода и серии мощных излучающих ИК-диодов) до оптоэлектронных приборов. Оптоэлектронные приборы производства НИИПП нашли широкое применение в аппаратуре космического назначения, в системах атмосферной оптической связи, активно-импульсных приборах ночного видения, для управления движением объектов. Аппараты, в которых применялись изделия оптоэлектроники НИИПП, побывали в космосе.

Продукция гражданского назначения составляет около 30% от объемов производства и активно развивается в АО «НИИПП».

Лидирующее направление – **производство светотехнической продукции** (светодиодные светильники и лампы, более 100 наименований, более 25 патентов и авторских свидетельств в области разработки и конструирования светотехники). АО «НИИПП» предлагает энергоэффективную высококачественную светотехническую продукцию для освещения широкого спектра объектов. Светильники собраны на основе отечественной компонентной базы со степенью локализации в НИИПП, имеют все необходимые разрешительные сертификации, лицензии и соответствия.

В 2022 г. АО «НИИПП» представило уникальный для российского рынка продукт – **зондовые станции** собственного производства,

предназначенные для измерений в области СВЧ-электроники. В 2022–2023 гг. выполнены поставки ручных зондовых станций Omega Air-150 COAX на ведущие российские предприятия радиоэлектронной промышленности, в измерительные центры и научные лаборатории; заключены контракты на поставку полуавтоматических зондовых станций Terra-200 COAX; предприятие готово также выполнять поставки программно-аппаратных комплексов (ПАК) для измерения параметров монолитных интегральных схем на неразделенных полупроводниковых пластинах. Полностью российское решение задачи импортозамещения в условиях санкций, при этом более эффективное по соотношению цена/качество по сравнению с любыми импортными аналогами.

Зарядные устройства для аккумуляторов «Кедр-Авто» производства АО «НИИПП» занимают первые места в рейтингах и конкурсах регионального и федерального уровня (в 2023 г. – «Автокомпонент года», «Лучшие товары Томской области»).

Генеральный директор АО «НИИПП» –
Монастырев Евгений Александрович

Генеральный спонсор конференции – АО «НПФ «МИКРАН»

АО «НПФ «Микран» Т.: +7 (382-2) 90-00-29
634041 г. Томск, Ф.: +7 (382-2) 42-36-15
пр-т Кирова, д. 51д 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.

Генеральный директор АО «НПФ «Микран» –
Парамонова Вера Юрьевна

Генеральный спонсор конференции – ООО НПК «ТЕСАРТ»

ООО НПК «ТЕСАРТ»
634015, г. Томск,
ул. Циолковского,
д. 19, каб. 318

Т./ф.: +7 (382-2)
90-05-30
Эл. почта:
office@tes-art.ru
www.tesart.ru

Научно-производственная компания «ТЕСАРТ» – высокотехнологичный бизнес полного цикла в области комплексных радиоизмерительных систем. Общество существует на рынке с 07 мая 2015 г. благодаря коллаборации инженеров, исследователей, конструкторов и технологов Томского научного центра.

Все технические решения компании основаны на инновационном подходе в области микроволновых измерений, электромехатронных систем, телекоммуникаций и радаров.

Основная продукция компании:

1. Опорно-поворотные устройства и прецизионные позиционеры.
2. Радиопоглощающий материал.
3. Безэховые экранированные камеры.
4. Автоматизированные измерительно-вычислительные комплексы.
5. СВЧ-электроника.

За 10 лет существования компании реализовано более 50 крупных проектов, основу которых составляет испытательное оборудование собственного отечественного производства. Благодаря квалифицированным сотрудникам, которых в 2025 г. насчитывается 120 человек, компания непрерывно модернизирует производственную базу и стремится расширить свои возможности. Поэтому нас выбирают такие заказчики, как Госкорпорации «Роскосмос» и «Ростех», АО «Концерн ВКО «Алмаз-Антей», АО Корпорация «Тактическое ракетное вооружение», ООО «Бюро 1440» и др.

Мы чутко подходим к каждому проекту и заботимся о качестве наших продуктов на всех стадиях жизненного цикла, включая техническое сопровождение в процессе эксплуатации. Нам важно, чтобы наше испытательное оборудование полностью соответствовало запросам, решало основные задачи, при этом улучшало качество и скорость работы заказчиков.

С самого старта своей деятельности НПК «ТЕСАРТ» активно развивает связи с ведущими университетами Томска и страны в области прикладных научных исследований по тематике, соответствую-

щей профилю компании. В нашей компании успешно реализуется программа стажировки для студентов и молодых специалистов технических специальностей. Участники стажировки получают возможность работать над реальными проектами компании под руководством опытных наставников и впоследствии стать частью нашей дружной команды.

Директор ООО НПК «ТЕСАРТ» –
Семкин Артем Олегович

Генеральный спонсор конференции – АО «ИнфоТеКС»

АО «ИнфоТеКС»
127083, Москва,
ул. Отрадная, 2Б, стр. 1

Т.: +7 (495) 737-61-92,
8 (800) 250-0-260
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 400 компаний. В штате трудоустроено более 1 700 сотрудников, а офисы открыты в 13 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 его помощью 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 партнерство и сотрудничество с образовательными учреждениями, поддержка научных разработок и исследовательских проектов, а также обучение и продвижение молодых специалистов. Поэтому уже более 12 лет «ИнфоТеКС» активно работает над развитием кадрового потенциала в ИТ- и ИБ-отраслях и реализует специальный проект «ИнфоТеКС Акаде-

мия». В рамках партнерской программы «ИнфоТеКС Академия» организует площадки по обмену опытом, взаимодействует с вузами, колледжами страны, организует стажировки для студентов, проводит грантовую и экспертную поддержку разработок в области информационной безопасности, интегрирует в учебный процесс экспертизу штатных специалистов ГК «ИнфоТеКС».

«ИнфоТеКС Академия» сотрудничает и заинтересована в сотрудничестве с:

1. Образовательными учреждениями различного уровня подготовки – школы, колледжи и вузы, желающими сотрудничать с отраслевым партнером по направлению образовательной, научной деятельности, проведения совместных мероприятий.

2. Партнёрами компании, которые нуждаются в квалифицированных специалистах.

3. Учредителями и регуляторами различных программ и проектов федерального и регионального уровня в области науки и образования.

4. Обучающимися и недавними выпускниками вузов, которые хотят получить опыт работы в крупной компании или повысить уровень своих знаний, а также принять участие в различных мероприятиях соревновательного плана.

Генеральный директор АО «ИнфоТеКС» –
Чапчаев Андрей Анатольевич

Генеральный спонсор конференции – Группа компаний «НАУЧНОЕ ОБОРУДОВАНИЕ»

Группа компаний «Научное оборудование»
630090, г. Новосибирск, ул. Николаева, 11/5

Т.: (383-3) 30-82-95
Эл. почта: sales@spegroup.ru
www.spegroup.ru

Группа компаний «Научное оборудование» более 25 лет существует на рынке высокотехнологичного оборудования и занимается разработкой собственных уникальных технологических решений и производством оборудования для их реализации.

Сегодня «Научное оборудование» представляет целую группу компаний, в которую входят торговые организации, специализирующиеся на поставке отдельных направлений оборудования, научно-производственное предприятие, занимающееся созданием радиоизмерительных комплексов, исследовательские команды, занятые разработкой наукоемких решений для приборостроительной, химической и биологической отраслей.

Большое внимание мы уделяем организации совместной работы с научными коллективами и промышленными предприятиями электронной и космической отраслей для решения широкого круга задач наших российских и иностранных партнеров. Сотрудничаем с научными организациями СО РАН, УРО РАН, ДВО РАН, промышленными предприятиями, технологическими компаниями, учебными заведениями высшего образования.

Выстраиваем партнерские отношения с представителями многих отраслей экономики, предлагаем комплексный подход к решению задач заказчика. Выступаем отраслевым интегратором и прорабатываем комплексно любые сложные задачи.

Среди реализованных проектов компании – оснащение учебных аудиторий в Региональном центре выявления, поддержки и развития способностей и талантов у детей и молодежи «Альтаир»; Физико-математической школе им. А.М. Лаврентьева при НГУ, разработки в области радиоизмерения и СВЧ, микроэлектроники, вакуумного, рентгеновского, испытательного и технологического оборудования, системы видеорегистрации, микроскопии, оптики и т.д.

В своей деятельности мы считаем важным следить за юридической чистотой и безопасностью, объективностью и достоверностью, открытостью и компетентностью.

Наши заказчики получают оборудование, оформленное с соблюдением всех необходимых формальностей. Мы предоставляем партнерам полную и достоверную информацию по всем интересующим вопросам и работаем на эффективный результат.

В нашем арсенале более 1 050 брендов и более 7 750 реализованных контрактов за три года. За каждым нашим проектом стоит большая команда высококвалифицированных технических специалистов в самых разнообразных отраслях науки и техники.

Нам доверяют такие заказчики, как «Росатом» и «Роскосмос», инновационный центр «Сколково», УК «Биотехнопарк Кольцово», филиал ПАО «Компания Сухой», НАЗ им. В.П. Чкалова, СибГУ им. М.Ф. Решетнева и др.

Надеемся на долгосрочное сотрудничество, будем рады новым партнерам и заказчикам.

Директор ООО «Научные приборы и системы» –
Гордеев Владимир Дмитриевич

Спонсор конференции – «50ohm Technologies»

50ohm Technologies

634045, г. Томск
info@50ohm.tech
50ohm.tech.ru

+7-923-408-04-08
fiftyohm
fiftyohm

«50ohm Technologies» – российская компания из г. Томска. Ее специализация – разработка программного обеспечения для автоматизации измерений, моделирования электронных компонентов и проектирования высокочастотных и сверхвысокочастотных радиоэлектронных устройств. 50ohm Technologies с 2016 г. успешно помогает предприятиям и инженерам ускорять разработку новых устройств. Миссия компании – помочь специалистам по СВЧ-электронике сосредоточиться на сложных и творческих задачах за счет использования удобных интеллектуальных инструментов, ускоряющих решение технических задач.

Основные направления деятельности 50ohm Technologies:

- **Автоматизация проектирования СВЧ-устройств.** Компания разрабатывает «умные» программные инструменты для проектирования СВЧ-интегральных схем. С помощью методов искусственного интеллекта такие программы автоматически генерируют варианты схем и топологий (например, усилителей, аттенюаторов, фазовращателей) на основе заданных требований и элементной базы. Инженер получает сразу несколько готовых проектов и выбирает оптимальный, что значительно ускоряет самый сложный этап разработки и избавляет от рутинных операций.
- **Моделирование электронных компонентов.** «50ohm Technologies» обладает большим опытом в создании точных моделей пассивных и активных компонентов, для полупроводниковых соединений группы $A^{III}B^{V}$. Компания поставляет эти модели в формате комплектом средств проектирования (PDK) для популярных САПР. Автоматизация расчётов и применение собственных методик экстракции позволяют значительно сократить затраты времени и средств при разработке новых изделий.
- **Автоматизация измерений и испытаний.** «50ohm Technologies» создаёт программно-аппаратные комплексы для автоматизированного тестирования радиоэлектронных устройств на базе оборудования заказчика. Готовые сценарии измерений для типовых компо-

нентов и приборов позволяют значительно сократить время испытаний и снизить вероятность ошибок. Внедрение таких решений повышает эффективность работы измерительной лаборатории предприятия без необходимости приобретения дорогостоящих сторонних систем.

Опираясь на передовые технологии и экспертизу команды, «50ohm Technologies» обеспечивает своим партнерам ускорение цикла разработки и улучшение качества результатов. Решения компании уже помогли ряду предприятий сократить сроки вывода продуктов на рынок и оптимизировать издержки. «50ohm Technologies» поддерживает научно-техническую конференцию и развитие профессионального сообщества. Компания открыта к сотрудничеству и нацелена и дальше оставаться надёжным партнёром для организаций радиоэлектронной отрасли.

Директор «50ohm Technologies» –
Калентьев Алексей Анатольевич

Секция 4

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(стр. 25 – 213)

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 519.246

ПРОЕКТИРОВАНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ИЗ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МЕТОДОВ КОМБИНАТОРНОЙ ГЕНЕРАЦИИ

И.Е. Авдеева, студентка каф. КИБЭВС
Научный руководитель Ю.В. Шабля, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, avdeeva.i.720-1@e.tusur.ru

Представлены результаты анализа эффективности генератора псевдослучайных чисел из изображений, основанных на теории комбинаторной генерации. Разработан алгоритм получения битовой строки из изображений с использованием класса алгоритмов ранжирования, проведена оценка его качества статистическими тестами NIST.
Ключевые слова: генерация псевдослучайных чисел, изображение, комбинаторная генерация, ранжирование, дерево И/ИЛИ.

Случайная генерация чисел важна в криптографии, статистическом моделировании и других областях. Традиционные генераторы псевдослучайных чисел часто предсказуемы и уязвимы к атакам. Использование изображений как источника энтропии актуально благодаря их высокой случайности и уникальности.

Цель данного исследования – оценка эффективности генерации псевдослучайных чисел из изображений с использованием методов комбинаторной генерации на основе деревьев И/ИЛИ. Основное внимание уделено анализу соответствия полученных битовых массивов критериям случайности.

Известные современные методы генерации случайных чисел на основе изображений включают:

– метод, преобразующий изображение в 8-битное серое и использующий гистограмму серых оттенков для генерации чисел на основе естественной случайности пикселей изображений [1];

– метод ECGA, применяющий к пикселям изображения инструмент эллиптических кривых для создания начальной последовательности, оптимизируемой генетическим алгоритмом [2];

– метод, использующий для изображения алгоритм k-средних (для кластеризации) и алгоритм Мерсенна (для генерации случайных выборок), а также обеспечивающий криптографическую стойкость [3].

Существование таких подходов подтверждает актуальность использования изображений для качественной генерации случайных чисел.

Основные результаты. Предложенный алгоритм использует метод ранжирования блоков пикселей изображения, предложенный в [4]. Каждый блок кодируется уникальным числом (рангом), вычисляемым по формуле

$$\mathrm{Rank} = \sum_{i=1}^{n} c^{i-1} \cdot m_i \ ,$$

где c – количество уникальных цветов в палитре изображения, m_i – порядковый номер цвета i-го пикселя ранжируемого блока в палитре, n – количество пикселей в ранжируемом блоке.

Данная формула была получена на основе представления комбинаторного множества всех возможных блоков пикселей изображения в форме структуры дерева И/ИЛИ. Полученные ранги, записанные в бинарный файл, формируют последовательность псевдослучайных чисел.

Статистические тесты пакета NIST 800-22 подтвердили соответствие генерируемых чисел критериям случайности. Наилучшие результаты достигнуты для цветных изображений с блоками размера 1×1024 и 64×64 (100,00 и 99,47% пройденных тестов соответственно) при длине последовательности $8 \cdot 10^8$ бит. Сравнение с известными методами показало, что предложенный алгоритм сопоставим или превосходит аналоги по случайности и устойчивости.

Заключение. В работе рассмотрена идея применения методов комбинаторной генерации на основе деревьев И/ИЛИ для создания псевдослучайной последовательности чисел. Алгоритм показал свою эффективность, обеспечив высокую случайность генерируемых последовательностей чисел, что подтверждено тестами NIST 800-22.

ЛИТЕРАТУРА

1. Dereli S. True-random number generator based on image histogram // Academic Perspective Procedia. – 2020. – Vol. 3, No. 1. – P. 301–307.

2. Haider T. A novel pseudo-random number generator based on multivariable optimization for image-cryptographic applications / T. Haider, S.A. Blanco, U. Hayat // Expert Systems with Applications. – 2024. – Vol. 240.

3. Крюков Д.А. Генерация псевдослучайных чисел на основе преобразований графических объектов / Д.А. Крюков, И.А. Тескер // Информационно-управляющие системы. – 2018. – Т. 2, № 93. – С. 2–7.

4. Меринов А.А. Сжатие изображений без потерь на основе методов комбинаторной генерации / А.А. Меринов, Ю.В. Шабля // Перспективы развития фундаментальных наук: сборник науч. трудов XXI Междунар. конф. студентов, аспирантов и молодых ученых (23–26 апреля 2024 г.): в 7 т. – Т. 3: Математика. – Томск: Изд-во НИ ТПУ, 2024. – С. 11–13.

УДК 004.056.5

ЗАЩИТА ОТ ВОЗВРАТНО-ОРИЕНТИРОВАННЫХ АТАК (ROP) В АРХИТЕКТУРЕ ARM: АНАЛИЗ УЯЗВИМОСТЕЙ И РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ

Э.Э. Белозерцев, аспирант каф. КИБЭВС;
С.С. Харченко, доцент каф. БИС, к.т.н.
Научный руководитель М.М. Немирович-Данченко,
проф. каф. КИБЭВС, д.ф.-м.н.
г. Томск, ТУСУР, bee@fb.tusur.ru

Рассматривается проблема уязвимостей программного обеспечения, приводящих к возможности выполнения произвольного кода через RoP-атаки. Описываются механизмы атак, использующие цепочки гаджетов – фрагментов кода программы, и способы защиты, такие как ASLR, DEP, Stack Canaries и CFI. Рассматриваются адаптивные методы защиты, направленные на противодействие модификациям RoP-атак, включая JoP и CoP. Также описаны разработка тестового стенда для проведения RoP-атак и инструмент для автоматизированного подбора гаджетов, который будет использоваться для оценки защищенности программ перед такими атаками.

Ключевые слова: возвратно-ориентированное программирование, RoP-атаки, JoP, CoP, архитектура ARM, информационная безопасность.

Одной из значимых проблем в области информационной безопасности являются уязвимости программного обеспечения, позволяющие злоумышленнику выполнить произвольный код в контексте уязвимого приложения.

Современные процессорные архитектуры препятствуют классическим методам удаленного исполнения кода, например, посредством прямой загрузки и выполнения вредоносных инструкций. Однако злоумышленник может воспользоваться уже существующими в памяти программы фрагментами инструкций, называемыми «гаджетами», чтобы составить требуемый алгоритм.

Суть RoP-атак заключается в том, что атакующий вместо загрузки собственного исполняемого кода в память жертвы использует уже имеющиеся в бинарном коде программы фрагменты инструкций, называемые гаджетами (gadgets). Эти гаджеты, заканчивающиеся инструкцией возврата, могут быть объединены в цепочки, реализующие произвольный алгоритм. Таким образом, злоумышленник может управлять выполнением программы, изменяя адреса возврата в стеке и формируя последовательность переходов между гаджетами, обходя запрет на исполнение стека.

На данный момент не существует универсального защитного механизма, однако активно используются различные подходы, направленные на предотвращение или минимизацию использования цепочек гаджетов:

– ASLR (Address Space Layout Randomization);
– DEP (Data Execution Prevention);
– Stack Canaries и контроль целостности стека;
– Control Flow Integrity (CFI).

Важным аспектом разработки эффективных методов противодействия RoP-атакам является их адаптивность к новым методам эксплуатации уязвимостей [1]. Современные техники атак включают не только классическое RoP, но и его модификации, такие как Jump-Oriented Programming (JoP) и Call-Oriented Programming (CoP) [2], которые используют альтернативные механизмы управления потоком выполнения. Это требует создания защитных решений, способных выявлять и блокировать не только традиционные RoP-атаки, но и их более сложные вариации, что повышает общую устойчивость системы к компрометации.

Архитектура ARM является одной из наиболее широко используемых в мобильных устройствах и встроенных системах. Это связано с её низким потреблением энергии, высокой производительностью и возможностями для создания компактных и эффективных процессо-

ров. Однако архитектура ARM также имеет свои особенности, которые могут быть использованы как для защиты, так и для реализации атак [3].

Процессоры ARM поддерживают несколько встроенных механизмов защиты, которые делают их устойчивыми к некоторым типам атак:

– Thumb-инструкции – ARM поддерживает два режима команд: ARM и Thumb, где Thumb-инструкции позволяют сократить размер исполнимого кода. Это создает дополнительные трудности для атакующих при попытке найти подходящие гаджеты, так как фрагменты кода могут быть представлены в разных формах.

– Control Flow Integrity (CFI) – один из методов защиты, который используется для предотвращения изменений в потоке управления программы. Это важный аспект защиты от RoP-атак, так как он может препятствовать атакующему в изменении порядка выполнения инструкций.

– Адаптивные механизмы защиты – механизмы, такие как ASLR, могут использоваться для перемешивания расположения кода в памяти, что усложняет задачу поиска подходящих гаджетов для атаки. В ARM-процессорах существует возможность динамического изменения расположения данных и кода в памяти, что добавляет дополнительный уровень защиты.

Для дальнейшего изучения уязвимостей и эффективности защитных механизмов в рамках исследования разрабатывается тестовый стенд, предназначенный для проведения простых RoP-атак. Он будет включать целевую уязвимую программу, которая имитирует реальные уязвимости, а также инструменты для генерации и выполнения RoP-цепочек. Такой стенд позволит на практике исследовать различные методы эксплуатации уязвимостей, а также анализировать поведение защитных механизмов.

Одним из направлений работы является разработка автоматизированного метода подбора RoP-гаджетов для построения эксплойта. В процессе атаки необходимо найти в памяти программы подходящие последовательности инструкций, которые можно комбинировать для выполнения нужных действий. Планируется создание инструмента, который будет анализировать исполняемые файлы, извлекать потенциальные гаджеты и формировать из них возможные RoP-цепочки.

Разрабатываемая программа также будет использоваться для оценки степени защищенности различных приложений перед RoP-атаками. Она позволит анализировать бинарные файлы на предмет наличия подходящих гаджетов, выявлять потенциально уязвимые участки кода и оценивать сложность построения RoP-цепочек.

ЛИТЕРАТУРА

1. Лубкин И.А. Метрики защищенности приложений при использовании средств противодействия уязвимостям, основанным на возвратно-ориентированном программировании // Доклады ТУСУР. – 2021. – Т. 24, № 4. – С. 46–51.

2. Вишняков А.В. Классификация RoP-гаджетов // Труды ИСП РАН. – 2016. – Т. 28, вып. 6. – С. 27–36.

3. Гущин Н.А. Возвратно-ориентированное программирование в 64-битных архитектурах: магистерская диссертация [Электронный ресурс]. – Режим доступа: https://elib.spbstu.ru/dl/2/8639.pdf/info, по паролю из интернет (дата обращения: 11.03.2025).

УДК 004.912

СОВРЕМЕННОЕ ПОЛОЖЕНИЕ ИССЛЕДОВАНИЙ В ОБЛАСТИ ОПРЕДЕЛЕНИЯ ИСКУССТВЕННО СГЕНЕРИРОВАННОГО ИСХОДНОГО КОДА

А.П. Патышев, С.Г. Букина, студенты каф. БИС

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

Проект ГПО БИС-2501. Безопасность исходного кода

г. Томск, ТУСУР, anton2005pat@mail.ru

Рассматривается современное состояние исследований в области детекции искусственно сгенерированного исходного кода, включая статистические методы, методы машинного обучения, глубокие нейронные сети, анализ стилистических и семантических аномалий. Обозначены основные вызовы исследований по данной научной тематике. Также обсуждаются перспективы развития технологий детекции, включая использование метаобучения, интеграцию статического и динамического анализа, а также разработку легковесных моделей для повышения доступности технологий.

Ключевые слова: исходный код, языки программирования, языковые модели, детекция кода, информационная безопасность, машинное обучение.

Современные достижения в области искусственного интеллекта (ИИ) привели к прогрессу в генерации исходного кода. Большие языковые модели демонстрируют способность создавать исходный код, трудно отличимый от написанного человеком. Эти технологии находят применение в широком спектре задач. Согласно отчету McKinsey [1], треть компаний используют генеративный ИИ для выполнения бизнес-функций. Наряду с преимуществами, искусственная генерация кода создает ряд угроз – создание вредоносного или небезопасного кода, интеграция такого кода в цепочки поставки ПО, что может привести к внедрению уязвимостей. Кроме того, использование сгенери-

рованного кода может привести к снижению качества разработки, увеличению технического долга и затрат на поддержку ПО. В связи с этим разработка методов определения искусственно сгенерированного кода становится значимой задачей для обеспечения информационной безопасности, и качества ПО.

Основные подходы к детекции искусственно сгенерированного кода. Современные исследования можно разделить на ряд ключевых подходов. Статистические методы основаны на анализе распределения токенов, *n*-грамм и других характеристик кода. В работе [2] показано, что для выявления сгенерированного кода применим анализ энтропии кода и распределения вероятностей токенов. Однако такие методы часто оказываются недостаточно точными при работе с кодом, сгененрированным современными моделями, способными имитировать статистические характеристики человеческого кода. Также для решения данной научной проблемы применяются классические методы машинного обучения.

В работе [3] был использован случайный лес, достигший точности около 80% на задаче бинарной классификации. Но такие методы могут быть уязвимы к изменениям в генеративных моделях, которые быстро эволюционируют. Глубокие нейронные сети, модели трансформерной архитектуры демонстрируют наилучшие результаты. Например, модель UniXcoder показала среднюю точность 77,4% в выявлении кода [4].

В работе [5] были использованы двунаправленные трансформеры для анализа семантической связности кода, что позволило достичь значения F1-score 95,2%. Одним из перспективных направлений является адаптация методов, разработанных для детекции искусственно сгенерированных текстов. В работе [6] исследована возможность использования модели BERT, изначально разработанной для текстов. Результаты показали, что прямое применение текстовых детекторов к коду оказывается менее эффективным со средним значением F1-score 82,1%, что указывает на необходимость использования специализированных подходов. Стилистический анализ также играет важную роль.

В работе [7] был предложен подход, основанный на анализе стилистических характеристик, таких как длина имен переменных, использование комментариев и форматирование кода. Этот метод показал среднюю точность 70,86% на задаче бинарной классификации кода, однако его эффективность снижается при анализе кода, сгенерированного моделями, которые были специально обучены на данных с разнообразными стилями.

Обзор проблем в детекции. Несмотря на прогресс в исследованиях по данной тематике, существует ряд проблем, которые затрудняют разработку универсальных и надежных методов.

Постоянное совершенствование генеративных моделей влечет за собой изменение признаков сгенерированного исходного кода, что создает проблему для детекторов, обученных на данных от устаревших моделей. В работе [8] показано, что детекторы, обученные на коде модели GPT-3.5, демонстрируют снижение точности при анализе кода GPT-4. Для решения проблемы предлагается разработка адаптивных моделей, способных подстраиваться под новые генеративные модели.

Большинство детекторов демонстрируют высокую точность при анализе кода известных моделей, но эффективность снижается при анализе кода неизвестных моделей. Различные генеративные модели могут иметь разные стили генерации, что затрудняет выделение универсальных признаков. В работе [9] было предложено использовать метаобучение для повышения обобщающей способности детекторов, однако подход требует значительных вычислительных ресурсов и больших объемов данных.

Анализ семантической связности и логической корректности кода остается одной из наиболее сложных задач в детекции. В работе [10] был предложен подход, основанный на динамическом анализе кода, позволяющий выявлять аномалии, однако метод требует значительных вычислительных ресурсов и не всегда применим в реальных условиях.

Многие современные детекторы, особенно основанные на глубоких нейронных сетях и графовых моделях, требуют значительных вычислительных ресурсов. Это ограничивает их применимость в реальных условиях. Для решения проблемы требуется разработка более эффективных моделей, обеспечивающих высокую точность при меньших затратах ресурсов.

Таким образом, в статье проанализированы ключевые подходы к детекции и вызовы при решении данной научной проблемы. Перспективы дальнейших исследований включают разработку моделей, способных эффективно работать с кодом, сгенерированным неизвестными моделями. Возможными решениями являются использование метаобучения и трансферного обучения, разработка методов с минимизацией вычислительных затрат. Исследования в области определения искусственно сгенерированного кода находятся на ранней стадии развития, но уже демонстрируют значительный потенциал. Успешное решение существующих проблем и реализация предложенных направлений исследований позволят повысить безопасность и качество программного обеспечения.

ЛИТЕРАТУРА

1. McKinsey & Company. The state of AI in 2023: Generative AI’s breakout year. – 2023.

2. Bielik P. PHOG: Probabilistic model for code / P. Bielik, V. Raychev, M. Vechev // Proceedings of the 33rd International Conference on Machine Learning (ICML). – 2016. – P. 2933–2942.

3. GraphCodeBERT: Pre-training code representations with data flow / D. Guo, Ren, S. Lu et al. // International Conference on Learning Represen S.tations (ICLR). – 2021.

4. UniXcoder: Unified cross-modal pre-training for code representation / Z. Yang, Z. Dai, Y. Yang et al. // arXiv preprint arXiv:2203.03850. – 2022.

5. BERT: Pre-training of deep bidirectional transformers for language understanding / J. Devlin, M.W. Chang, K. Lee, K. Toutanova // Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL). – 2019. – P. 4171–4186.

6. Allamanis M. Learning to represent programs with graphs / M. Allamanis, M. Brockschmidt, M. Khademi // International Conference on Learning Representations (ICLR). – 2018.

7. Nguyen A.T. Graph-based statistical language model for code / A.T. Nguyen, T.N. Nguyen // Proceedings of the 37th International Conference on Software Engineering (ICSE). – 2015. – P. 858–868.

8. Code Llama: Open foundation models for code / B. Roziere, J. Gehring, F. Gloeckle et al. // arXiv preprint arXiv:2308.12950. – 2023.

9. Language models are few-shot learners / T.B. Brown, B. Mann, N. Ryder et al. // Advances in Neural Information Processing Systems (NeurIPS). – 2020. – P. 1877–1901.

10. Dynamic analysis of generated code for security vetting / J. Li, X. Wang, Y. Lin et al. // Proceedings of the 2023 IEEE Symposium on Security and Privacy (S&P). – 2023. – P. 1234–1249.

УДК 004.056

ЗАЩИТА ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ДЛЯ ПОДГОТОВКИ ДОКУМЕНТОВ ДЛЯ ПРОХОЖДЕНИЯ ВСЕХ ВИДОВ ПРАКТИК

А.В. Яремчук, В.А. Долгополов, студенты каф. БИС;
В.А. Терещенко, студент каф. ЭБ
Научный руководитель С.В. Глухарева, ст. преп. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)
Проект ГПО КИБЭВС-2101. Автоматизированная система для подготовки документов для прохождения всех видов практик
г. Томск, ТУСУР, nastaaremcuk627@gmail.com, varvaratereshenko@gmail.com, vladimir-dolgopolov@mail.ru

Рассматриваются вопросы обеспечения безопасности данных в автоматизированной системе (АИС), предназначенной для подготовки документов, необходимых студентам для прохождения всех ти-

пов практик. Анализируются потенциальные угрозы и уязвимости, которые могут привезти к несанкционированному доступу к информации. Приводятся рекомендации по обеспечению безопасности.
Ключевые слова: защита данных, персональные данные, автоматизированная система, практика, конфиденциальность, целостность, доступность, безопасность, риски информационной безопасности, угрозы, уязвимости.

Обеспечение надежной защиты информации является важной задачей для организаций, особенно тех, которые обрабатывают персональные данные. Это особенно актуально для образовательных учреждений, которые используют автоматизированные системы для управления процессом подготовки документации для прохождения студентами всех видов практик. Утечка данных или нарушения безопасности в таких системах может привести к серьезным последствиям, что подчеркивает необходимость разработки и внедрения эффективных мер защиты.

Одной из основных задач является автоматизация процесса формирования пакета документов для прохождения стажировки, включая заявление на прохождение практики, которая содержит следующую информацию:

1. Данные студента: ФИО студента, академическая группа, направление подготовки.
2. Сведения об учебном заведении: ФИО руководителя практики, тип и вид практики, срок её прохождения.
3. Сведения о предприятии: название организации, адрес, почтовый индекс.

Понимание рисков и потенциального ущерба – первый шаг к созданию надежной системы защиты. Необходимо четко различать понятия риска и ущерба в сфере информационной безопасности. Риск – это вероятность реализации угрозы, использующей уязвимость системы, что приводит к негативным последствиям [1]. Ущерб, в свою очередь, представляет собой оценку этих негативных последствий [2].

Разработка АИС для подготовки документов к практике сопряжена с определенными рисками и угрозами:

1. Угрозы аутентификации и авторизации:

– брутфорс атаки на учетные записи пользователей.

2. Угрозы сансов:

– риск кражи сессии при отсутствии ротации сессионных токенов;

– угрозы, связанные с session fixation.

3. Сетевые угрозы:

– DDoS атаки.

4. Угрозы данных:

– возможны NoSQL-инъекции в Redis;

– риск XSS атак при отображении пользовательских данных.

5. Утечки данных:

– нет шифрования данных в Redis;

– потенциальные утечки через журналы.

6. Инфраструктурные риски:

– отсутствие аутентификации для Redis;

– Redis доступен по умолчанию на локальном хосте.

7. Отказоустойчивость:

– нет механизма репликации данных;

– отсутствует механизм graceful shutdown.

8. Проблемы мониторинга и аудита.

9. Ограниченное логирование: фиксируется только подозрительная деятельность; нет аудита действий пользователей и мониторинга состояния системы.

10. Проблемы конфигурации:

– отсутствие: механизма обновления конфигурации без перезапуска; валидации конфигурационных параметров.

11. Риски разработки:

– нет механизма версионирования API.

Для минимизации этих рисков требуется внедрение мер безопасности.

К мерам безопасности, которые можно применять в АИС для подготовки документов для прохождения практики, относятся:

1. Защита от HTTP Flood:

– ограничение частоты запросов (Rate Limiting) – предотвращает перегрузку сервера из-за большого числа запросов;

– ограничение количества попыток входа – защищает от перебора паролей;

– блокировка IP-адресов при выявлении подозрительной активности – реагирует на аномальное поведение;

– использование Redis для хранения счетчиков и блокировок – обеспечивает быстрое и эффективное управление блокировками.

2. Защита от Slowloris:

– настройка таймаутов соединений – освобождает ресурсы сервера при неактивных соединениях;

– ограничение количества одновременных соединений – предотвращает исчерпание ресурсов сервера множеством соединений.

3. Общие механизмы безопасности:

– защита от XSS через CSP заголовки – предотвращает внедрение вредоносного кода;

– защита от CSRF через SameSite cookie – обеспечивает безопасность от межсайтовых атак;

– защита от кликджекинга через X-Frame-Options – предотвращает обманные клики;

– принудительное использование HTTPS – шифрует трафик для защиты от перехвата;

– безопасные заголовки сессии – усиливает безопасность пользовательских сессий;

– защита от MIME-снифинга – предотвращает ошибочное распознавание файлов браузером.

4. Дополнительные меры:

– мониторинг подозрительной активности – позволяет своевременно выявлять аномалии;

– логирование событий безопасности – обеспечивает возможность анализа инцидентов;

– автоматическая блокировка IP-адресов – обеспечивает быструю реакцию на угрозы;

– защита от брутфорс-атак – предотвращает перебор паролей.

Обеспечение безопасности данных в автоматизированной системе для подготовки документации по всем видам практик – важная задача. Внедрение предложенных организационных и технических мер позволит минимизировать риски утечки информации, нарушения целостности и доступности данных, а также гарантировать конфиденциальность и безопасность персональных данных студентов и других пользователей.

ЛИТЕРАТУРА

1. Анализ и управление рисками в информационных системах [Электронный ресурс]. – Режим доступа: https://intuit.ru/studies/courses/962/387/lecture/8990 (дата обращения: 27.02.2025).

2. Что такое информационная безопасность [Электронный ресурс]. – Режим доступа: https://www.reg.ru/blog/chto-takoe-informacionnaya-bezopasnost/?ysclid=m82p5db40130761667 (дата обращения: 27.02.2025).

3. ISO/IEC 27001:2022 [Электронный ресурс]. – Режим доступа: https://www.iso.org/ru/standard/27001, свободный (дата обращения: 27.02.2025).

4. Федеральный закон от 27.07.2006 № 159-ФЗ. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Справочная правовая система КонсультантПлюс: https://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 27.02.2025).

УДК 004.056

РИСКИ И СПОСОБЫ ЗАЩИТЫ ОТ DDOS-АТАК В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ДЛЯ ПОДГОТОВКИ ДОКУМЕНТОВ ДЛЯ ПРОХОЖДЕНИЯ ВСЕХ ВИДОВ ПРАКТИК

Е.Н. Нимаева, студентка каф. БИС;
Н.В. Филатов, А.А. Ермолов, студенты каф. КИБЭВС
Научный руководитель С.В. Глухарева, ст. преп. каф. КИБЭВС
г. Томск, ТУСУР, katya.nimayeva@internet.ru, vip.bam444@mail.ru, d1vze@mail.ru

Проект ГПО КИБЭВС-2101. Автоматизированная система для подготовки документов для прохождения всех видов практик

Представлен анализ рисков DDoS-атак на автоматизированную систему для подготовки документов для прохождения всех видов практик. Рассмотрены основные методы защиты, направленные на обеспечение стабильной работы системы.

Ключевые слова: DDoS-атака, автоматизированная система, информационная безопасность, защита от атак, киберугрозы.

С развитием цифровых технологий и широким внедрением автоматизированных систем значительно возросли риски кибератак, в частности DDoS-атак. Автоматизированная информационная система для подготовки документов для прохождения всех видов практик играет важную роль в образовательных процессах. Ее стабильная работа влияет на эффективность документооборота. DDoS-атаки представляют серьёзную угрозу для таких систем, так как они могут остановить работу сервиса, нарушить его доступность и привести к потере важных данных. В связи с этим актуальной задачей становится изучение методов защиты автоматизированных систем от подобных угроз.

DDoS-атака представляет собой распределённую атаку, направленную на создание отказа в обслуживании различных интернет-сервисов [1]. DDoS-атаки могут различаться по механизму воздействия на систему:

Сетевые атаки – направлены на исчерпание пропускной способности сети.

Прикладные атаки – нацелены на перегрузку серверных ресурсов.

Комбинированные атаки – объединяют несколько методов для максимального эффекта.

Наиболее распространёнными видами атак являются:

1. UDP Flood – атака, основанная на массовой отправке пакетов UDP на случайные порты сервера, вызывая перегрузку системы.

2. SYN Flood – атака, при которой злоумышленник отправляет множество SYN-запросов без завершения установки соединения, истощая ресурсы сервера.

3. HTTP Flood – атака, при которой сервер перегружается множеством HTTP-запросов.

4. Slowloris – злоумышленник открывает большое количество соединений с сервером без ответа, расходуя ресурсы.

5. DNS Amplification – отправка поддельных DNS-запросов с подменённым IP-адресом жертвы, получая усиленные ответы [3].

Последствия DDoS-атак:

– нарушение работоспособности системы и её недоступность для пользователей;

– финансовые убытки, связанные с простоем системы и необходимостью восстановления инфраструктуры;

– ухудшение репутации организации и снижение доверия пользователей;

– возможные утечки данных при комбинированных атаках.

В первой половине 2024 г. наблюдается значительный рост числа DDoS-атак на российские организации. Зафиксировано 355 тыс. атак, что на 16% больше, чем за весь 2023 г. Основные тенденции включают увеличение кратковременных, но интенсивных атак, а также рост мультивекторных атак, включающих несколько типов атак одновременно. Особенно пострадали отрасли ИТ, госсектор, телекоммуникации и энергетика. Это подчеркивает необходимость усовершенствования методов защиты для обеспечения стабильности работы автоматизированных систем и критической инфраструктуры [4].

В автоматизированной информационной системе для подготовки документов для прохождения всех видов практик были реализованы следующие меры защиты:

1. Защита от SYN Flood – применение механизма SYN Cookies, который позволяет минимизировать нагрузку на сервер, исключая необходимость выделения ресурсов до полного установления соединения.

2. Защита от HTTP Flood – ограничение количества запросов с одного IP-адреса (rate limiting), анализ заголовков запросов, блокировка подозрительной активности.

3. Защита от Slowloris – настройка таймаутов соединений и ограничение количества одновременных соединений.

4. Применение кэширования – использование серверного кэширования для снижения нагрузки на серверные ресурсы.

5. Анализ аномалий – мониторинг трафика и автоматическое выявление подозрительных действий.

Дополнительно эффективными мерами могут стать:

– использование балансировщиков нагрузки для перераспределения трафика;

– применение географической фильтрации трафика;

– интеграция с сервисами защиты от DDoS, такими как Cloudflare, Imperva;

– использование специализированных решений по анализу сетевого трафика и его фильтрации.

Надёжная защита автоматизированной системы от DDoS-атак требует комплексного подхода, включающего не только технические решения, но и постоянный мониторинг работы системы. Реализация таких механизмов, как SYN Cookies, ограничение частоты запросов и применение технологий кэширования позволяют снизить нагрузку на серверные ресурсы и повысить устойчивость системы к атакам.

Однако методы атак постоянно совершенствуются, что требует регулярного обновления средств защиты и адаптации к новым угрозам. Перспективным направлением является использование технологий машинного обучения и искусственного интеллекта, которые позволяют анализировать сетевой трафик в реальном времени и автоматически выявлять аномальную активность.

Комплексный подход к кибербезопасности включает не только технические меры, но и регулярный аудит, анализ сетевого трафика и разработку стратегий быстрого реагирования на инциденты. Это позволяет не только минимизировать последствия атак, но и повысить общую устойчивость системы к возможным киберугрозам.

ЛИТЕРАТУРА

1. Анализ актуальных типов DDoS-атак и методов защиты от них [Электронный ресурс]. – Режим доступа: https://izv.etu.ru/assets/files/izv-etu-1-20161-7-14.pdf, свободный (дата обращения: 1.02.2024).

2. Применение статистических методов для прогнозирования UPD-Flood атак. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/primenenie-statisticheskih-metodov-dlya-prognozirovaniya-udp-flood-atak/viewer (дата обращения: 01.03.2025).

3. Самые популярные виды DDoS [Электронный ресурс]. – Режим доступа: https://servicepipe.ru/blog/what-is-ddos (дата обращения: 04.02.2025).

4. Отчет о DDoS-атаках на онлайн-ресурсы российских компаний в I полугодии 2024 года [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/analytics/reports/4677/ (дата обращения: 15.03.2025).

УДК 004.514.6

КИБЕРБЕЗОПАСНОСТЬ В OPC UA: МЕХАНИЗМЫ ЗАЩИТЫ ДАННЫХ В ПРОМЫШЛЕННЫХ СЕТЯХ

М.Д. Поскрёбышев, В.С. Зайнулин, М.А. Гавриленко

Научный руководитель В.М. Дмитриев, д.т.н., проф. каф. КСУП

г. Томск, ТУСУР, midtower@mail.ru, vuasheslav93@gmail.com, Misha007494@mail.ru

В условиях цифровой трансформации промышленности (Industrie 4.0) и роста числа кибератак на критически важную инфраструктуру обеспечение безопасности данных становится ключевой задачей. Статья посвящена анализу встроенных механизмов кибербезопасности протокола OPC UA, разработанного для устранения уязвимостей устаревших промышленных стандартов, таких как Modbus и Profibus. Рассматриваются основные угрозы для промышленных сетей, включая атаки типа «человек посередине» (MITM), подмену данных и DoS-атаки, а также демонстрируется, как OPC UA обеспечивает защиту за счет сквозного шифрования данных с использованием TLS и алгоритмов AES, строгой аутентификации устройств на основе сертификатов X.509, ролевой модели доступа и цифровых подписей для гарантии целостности информации.

Ключевые слова: OPC UA, промышленные сети, тип передачи, SCADA-системы.

Промышленные системы, такие как SCADA, PLC и MES, традиционно полагались на протоколы без встроенной защиты (Modbus, Profibus). Это делало их уязвимыми для атак, как в случае со Stuxnet (2010), где вредоносный код нарушил работу иранских ядерных объектов. С переходом к облачным решениям и IIoT потребовался протокол, обеспечивающий безопасность на всех уровнях. OPC UA (Unified Architecture), разработанный OPC Foundation, стал стандартом для безопасной передачи данных в Industrie 4.0 благодаря своей архитектуре, ориентированной на кибербезопасность.

Основные риски включают:

1) перехват данных (MITM-атаки), например, мониторинг параметров производства конкурентами;

2) подмену команд (spoofing), ведущую к остановке конвейера или повреждению оборудования;

3) DoS-атаки, нарушающие работу систем управления;

4) эксплуатацию уязвимостей legacy-протоколов, таких как отсутствие шифрования в Modbus TCP.

Эти угрозы актуальны для энергетики, транспорта и умных фабрик, где утечка данных или сбой системы могут привести к катастрофическим последствиям.

OPC UA использует сертификаты X.509 для взаимной аутентификации клиентов и серверов. Каждое устройство в сети имеет уникальный сертификат, подписанный доверенным центром (CA). Ролевая модель доступа ограничивает права пользователей: например, оператор может только читать данные, а инженер – вносить изменения в конфигурацию.

Шифрование данных.

1) Transport Layer Security (TLS): защищает канал связи, предотвращая MITM-атаки. Режимы шифрования (AES-256, RSA-2048) соответствуют стандартам NIST;

2) Message Security Mode: шифрует отдельные сообщения, что актуально для систем с высокой задержкой.

Каждое сообщение подписывается цифровой подписью (ECDSA), гарантируя, что данные не были изменены.

OPC UA поддерживает журналирование событий (логи аутентификации, попыток доступа), что помогает выявлять аномалии и расследовать инциденты. Сравнение возможностей протокола OPC UA с другими представлено в таблице.

Сравнение возможностей протоколов

Параметр	OPC UA	Modbus/Profibus
Шифрование	TLS + Message Security	Отсутствует
Аутентификация	X.509 + OAuth2	Логин/пароль (опционально)
Целостность	Цифровые подписи	Контрольные суммы
Совместимость	Кроссплатформенность	Ограничена оборудованием

OPC UA устанавливает новый стандарт безопасности для промышленных сетей, устраняя ключевые недостатки legacy-протоколов. Несмотря на сложности внедрения, его механизмы защиты (шифрование, X.509, аудит) делают его незаменимым инструментом для цифровой трансформации предприятий. Дальнейшее развитие стандарта, включая интеграцию с TSN и AI, укрепит его позиции как основы Industrie 4.0.

ЛИТЕРАТУРА

1. Overview of the .NET Framework [Электронный ресурс]. – Режим доступа: URL: https://msdn.microsoft.com/en-us/library/zw4w595w.aspx (дата обращения: 12.03.2025).

2. OPC Foundation home page [Электронный ресурс]. – Режим доступа: URL: https://opcfoundation.org (дата обращения: 12.03.2025).

3. .NET Programming with C++/CLI (Visual C++) [Электронный ресурс]. – Режим доступа: URL: https://msdn.microsoft.com/enus/library/68td296t.aspx (дата обращения: 17.03.2025).

4. Unified Architecture. Part 1: Overview and Concepts [Электронный ресурс]. – Режим доступа: URL: https://opcfoundation.org/developertools/specifications-unified-architecture/part-1-overview-and-concepts (дата обращения: 15.03.2025).

5. Unified Architecture. Part 9: Alarms and Conditions [Электронный ресурс]. – Режим доступа: URL: https://opcfoundation.org/developertools/specifications-unified-architecture/part-9-alarms-and-conditions (дата обращения: 15.03.2025).

6. Фаулер М. UML Основы. – СПб.: Символ, 2005. – 184 с.

УДК 004.056.53

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОНТЕЙНЕРОВ

Н.Д. Кириков, оператор роты (научной)

Научный руководитель А.А. Шевченко, с.н.с.
третьего научно-исследовательского отдела
научно-исследовательского центра
г. Санкт-Петербург, Военная орденов Жукова и Ленина
Краснознаменная академия связи им. Маршала Советского Союза
С.М. Буденного МО РФ, taleofmorfey@gmail.com

Представлен обзор различных технологий, применяемых для обеспечения безопасности контейнеров. Приводятся примеры уязвимостей, с помощью которых возможно совершить атаку на конвейеризированные приложения.

Ключевые слова: контейнеры, сервисы, безопасность приложений.

Существует много векторов атак на контейнеры, однако большинство из них сводятся к неправильной конфигурации при развертывании приложения или же к использованию устаревших механизмов безопасности.

Определение контейнера. Контейнеры представляют собой, как правило, один процесс (за исключением lxc-контейнеров), в котором происходит виртуализация на уровне операционной системы, при этом в виртуализированной операционной системе происходит запуск одного сервиса или приложения, после завершения работы приложения контейнер завершает свою работу.

Атаки на контейнеры. Существует множество атак на контейнеры, среди которых наиболее известными являются:

1. Монтирование файловой системы. Данный метод может быть реализован при использовании shell-раннера для развертывания приложений, в таком случае пользователи контейнера с правом использования «docker» команд фактически эквивалентны пользователям с root-правами.

Например, при запуске контейнера с привилегией SYS_ADMIN:

– docker run -it --cap-drop=ALL --cap-add=SYS_ADMIN --security-opt apparmor=unconfined --device=/dev/:/ ubuntu bash.

Возможно выполнить следующие команды и получить root доступ к хостовой файловой системе:

– mount /dev/<DEVICE-FILE> /mnt;

– ls /mnt.

2. Использование смонтированного docker.sock. Docker daemon [1] – процесс, который управляет контейнерами на хосте и слушает Docker API запросы через Docker socket, монтирование Docker socket в контейнер позволяет общаться с Docker daemon изнутри контейнера. Однако наличие доступа к docker.socket означает возможность использования chroot к хостовой системе (рис. 1).

```
root@5c940b4546d8:/# docker run -it --privileged -v /:/host/ ubuntu bash -c "chroot /host/"
# ls
bin  boot  builds  dev  etc  home  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  r
oot  run  sbin  snap  sources.list  srv  swap.img  sys  tmp  usr  var
# cd /home
# ls
gitlab-runner  neroot  odoo  secret
# whoami
/bin/sh: 4: upwhoami: not found
# whoami
root
# ■
```

Рис. 1. Пример реализации атаки выхода за изоляцию контейнера

3. Добавление уязвимого kernel-модуля. Linux контейнеры делят между собой одну kernel OS, но они изолированы между собой в их процессах от остальной системы, однако контейнер с включенным SYS_MODULE может загружать и удалять kernel-модули в хостовой системе. Таким образом, можно реализовать внутри контейнера такой модуль, который при внедрении в основную систему предоставлял бы контроль над хостом любому, кто подключается к его сервису.

Технологии защиты контейнеров. Так как контейнеры представляют собой процессы [2], то для их защиты применяются те же методы, что и для процессов (рис. 2):

– пространства имен (namespaces): необходимы для изоляции части файловой системы, в контейнерах используются для изоляции процессов от других контейнеров и от хостовой файловой системы с помощью пространства имен PID;

– привилегии (capabilities) – позволяют предоставить программам доступ к определённым возможностям, которые обычно есть только у суперпользователя, позволяя избежать запуска программ от имени root;

– контрольные группы (cgroups) – позволяют объединять процессы в отдельные группы и предоставлять доступ к контроллерам, ограничивающим доступ к ресурсам, например, контроллер «memory» ограничивает доступ к оперативной памяти;

– Apparmor/SELinux – средства защиты, регламентирующие политики безопасности, определяющие, какие приложения к каким ресурсам и с какими привилегиями будут иметь доступ. В случае Apparmor используется ролевая модель разграничения доступа, а в случае SELinux используется мандатная модель разграничения доступа;

– Seccomp – средство защиты, работающее на уровне ядра Linux и позволяющее ограничить доступ приложений к системным вызовам.

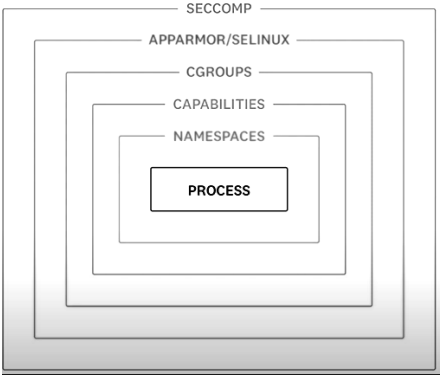

Рис. 2. Технологии для обеспечении безопасности процессов в Linux

Векторы атак, связанные с монтированием файловой системы и уязвимого «docker.sock», часто используются, чтобы выйти за изоляцию docker:dind-раннеров [3]. Для защиты от подобных атак можно отказаться от использования раннеров docker in docker в пользу kaniko или buildpacks. В случае невозможности отказа от dind нужно запретить запуск раннера в привилегированном режиме. Например, при развёртывании приложения в Kubernetees [4] в описании yaml pod'a можно установить security-context-параметры Privileged и allowPrivilegeEscalation в False (рис. 3), что не позволит процессу получить привилегий больше, чем у его родительского процесса.

Для защиты от вектора атаки добавления уязвимого kernel-модуля необходимо ограничивать с помощью AppArmor привилегии пользователя контейнера.

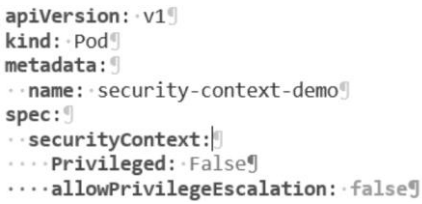

Рис. 3. Описание привилегий для pod в Kubernetes

Заключение. Таким образом, для обеспечения безопасности контейнеров не рекомендуется:

– использовать shell runner;

– использовать docker dind runner;

– запускать контейнеры в привилегированном режиме;

– запускать контейнеры без профиля AppArmor;

– предоставлять доступ к привилегиям SYS_ADMIN, SYS_PTRACE, SYS_MODULE, DAC_READ_SEARCH, DAC_READ_SEARCH, DAC_OVERRIDE.

ЛИТЕРАТУРА

1. Docker daemon configuration overview [Электронный ресурс]. – Режим доступа: https://docs.docker.com/engine/daemon, свободный (дата обращения: 29.02.2025).

2. Datadog Security labs [Электронный ресурс]. – Режим доступа: https://securitylabs.datadoghq.com/articles/container-security-fundamentals-part-1, свободный (дата обращения: 27.02.2025).

3. GitLab Runner [Электронный ресурс]. – Режим доступа: https://docs.gitlab.com/runner, свободный (дата обращения: 29.02.2025).

4. Kubernetes documentation [Электронный ресурс]. – Режим доступа: https://kubernetes.io/docs/home/, свободный (дата обращения: 27.02.2025).

УДК 004.056

МОДЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ КОМПОНЕНТОВ АППАРАТНОГО УРОВНЯ НА ОСНОВЕ МЕТАГРАФА

Н.А. Коровкин, Д.А. Коровкин, студенты каф. КИБЭВС

г. Томск, ТУСУР, korovkin2003@bk.ru

Рассмотрена проблема моделирования информационных систем на уровне аппаратных компонентов с использованием метаграфового подхода в контексте обеспечения информационной безопасности. Смоделирован метаграф на уровне компонентов аппаратного уровня, приведено математическое описание модели.

Ключевые слова: механизмы защиты, оценка защищенности, теория графов, аппаратные компоненты, математический аппарат.

Задача обеспечения информационной безопасности современных информационных систем является актуальной как для предприятий государственного сектора, так и для частных компаний. Однако единого и структурированного подхода для решения данной задачи в настоящее время создано не было. Вместе с тем, существуют отдельные приказы надзорных органов в сфере информационной безопасности, устанавливающие требования о защите информации в различного вида информационных системах.

Наиболее структурированным правовым актом с точки зрения методики определения мер защиты является приказ ФСТЭК № 17 от 11 февраля 2013 г. [1]. Тем не менее у данных требований есть существенный недостаток – отсутствие необходимости моделирования информационной системы перед определением актуального списка мер защиты – при анализе безопасности системы большинство подходов предполагают рассмотрение каждого ее элемента отдельно от всей системы. Несмотря на то, что такой подход может помочь в обеспечении информационной безопасности, это не исключает вероятности возникновения угроз безопасности в ситуациях взаимодействия между отдельными компонентами системы [2], именно поэтому необходима модель информационной системы для исследования связей её компонентов. В качестве математического аппарата, рассматривающего вопросы защиты информации, достаточно часто применяются положения: теории вероятностей, теории графов, автоматов и сетей Петри, имитационного моделирования, теории игр и конфликтов, теории нечетких множеств и т.д. [3].

Воспользуемся теорией графов, а именно метаграфовой моделью как разновидностью графовых структур для моделирования абстрактной информационной системы. В работе [4] для данной задачи используется атрибутивный метаграф, это наиболее удачный вариант, поскольку позволяет описать программные компоненты и все возможные связи между ними. Однако для того чтобы спроектированная модель учитывала специфику взаимодействия элементов с наибольшей точностью, необходимо разделить компоненты системы на программный и аппаратный уровни. В данной статье информационная система представлена в виде метаграфа с компонентами аппаратного уровня (рис. 1).

Как и в статье [5], метаграф был поделён на три уровня, где верхний уровень – локальные сети, на втором уровне расположены рабочие станции, нижний уровень представляет собой множество компонентов рабочих станций. Для завершения формализации модели было выполнено математическое описание данной модели:

метаграф MG = (P3, MP1, MP2, E3, ME1, ME2 , ME3),

где MG – метаграф информационной системы;

P3={p1,1,1 , p1,2,2 ,…, pj,f,k} – множество вершин, уровень «Компоненты PC»;

MP1={mp1,1 , mp1,2 ,…, mpj,k} – множество метавершин, уровень «Локальная сеть в рамках глобальной сети»;

MP2 ={mp2,1 , mp2,2 ,…, mpj,k} – множество метавершин, уровень «Компьютер в рамках локальной сети»;

E3={e1,1,1 , e1,2,2,…, ei,f,k, eri,k} – множество рёбер, уровень «Компоненты PC»;

ME1 ={me1,1 , me1,2 ,…, mei,k} – множество метарёбер, уровень «Локальная сеть в рамках глобальной сети»;

ME2 ={me2,1 , me2,2 ,…, mei,k} – множество метарёбер, уровень «Компьютер в рамках локальной сети»;

ME3 ={me3,1 , me3,2 ,…, mei,k} – множество метарёбер, уровень «Компоненты PC», где k – номер экземпляра на уровнях j и i, соответственно. j, i ∈ {1; 3}, где 1 – локальная сеть в рамках глобальной сети, 2 – компьютер в рамках локальной сети, 3 – компоненты PC. f – обозначение конкретной операционной системы, eri,k – ребро, представленное виртуальной связью: k, f ∈ {1; +∞}.

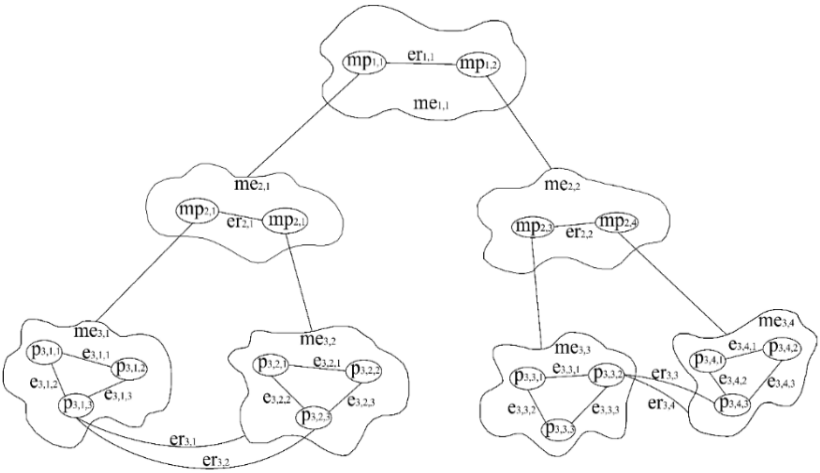

Рис. 1. Метаграф компонентов аппаратного уровня

В результате была разработана модель информационной системы на уровне аппаратных компонентов с использованием метаграфового подхода, представленная в виде атрибутивного трёхуровневого мета-

графа, также было выполнено математическое описание модели, что позволило формально описать структуру и взаимосвязи системы. Данный метод моделирования информационной системы является эффективным, поскольку позволяет учитывать неограниченное число элементов и связей, что даёт возможность масштабировать систему без риска не учесть все её возможные уязвимости.

ЛИТЕРАТУРА

1. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России от 11.02.2013 № 17 [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n17?ysclid=m86adee8kk972988494 (дата обращения: 06.03.2025).

2. 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. – P. 283–290.

3. Прокушев Я.Е. Моделирование процессов проектирования систем защиты информации в государственных информационных системах / Я.Е. Прокушев, С.В. Пономаренко, С.А. Пономаренко // Computational Nanotechnology. – 2021. – Т. 8, № 1. – С. 26–37. DOI: 10.33693/2313-223X-2021-8-1-26-37.

4. Novokhrestov A. Model of Threats to Computer Network Software / A. Novokhrestov, A. Konev, A. Shelupanov // Symmetry. – 2019. – Vol. 11, Is. 12. – 13 p.

5. Коровкин Н.А. Моделирование угроз безопасности системы пересылки и получения электронных сообщений / Н.А. Коровкин, Д.А. Коровкин // Электронные средства и системы управления: матер. докладов междунар. науч.-практ. конф. – 2023. – № 1-2. – С. 133–135.

УДК 004.912

ОБФУСКАЦИЯ КАК МЕТОД ЗАЩИТЫ ИСХОДНОГО КОДА

П.Е. Плотников, студент каф. БИС

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

Проект ГПО БИС-2501. Безопасность исходного кода

г. Томск, ТУСУР, petr05022005@gmail.com

Рассматривается актуальный вопрос защиты программного обеспечения от несанкционированного использования, копирования и модификации. Основное внимание уделено методу обфускации, который позволяет затруднить анализ и понимание исходного кода, сохраняя его функциональность. Описаны ключевые методы обфускации, такие как разбиение выражений, изменение имен переменных, методов и полей, а также добавление недостижимого кода. Отмечены проблемы, связанные с обфускацией, включая воз-

можность обратного инжиниринга, снижение производительности и теоретические ограничения метода. Несмотря на эти недостатки, обфускация остается эффективным инструментом защиты исходного кода, что подчеркивает необходимость дальнейшего развития и совершенствования методов обфускации для повышения их надежности и универсальности.
Ключевые слова: обфускация, обратный инжиниринг, исходный код, декомпиляция, безопасность кода, шифрование, анализ кода, методы обфускации.

Обфускация – приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции [7].

Можно выделить следующие **методы обфускации** [1]:

Разбиение выражения на несколько выражений. Этот метод заключается в изменении стандартного вычисления путем разбиения его на несколько отдельных выражений.

Изменение имен переменных. Обфускация достигается путем замены имен переменных на бессмысленные или сложные конструкции, например, сочетание похожих символов или использование терминов из других областей.

Смешивание однотипных полей. В этом методе переменные схожего типа объединяются в один массив или переменные подмешиваются в уже существующие структуры данных.

Переименование имен полей. Поля классов получают новые имена, что усложняет анализ программы.

Переименование имен методов. Аналогично переменным и полям методы могут быть переименованы. Более того, можно изменить их сигнатуры, добавляя мусорные аргументы, которые не используются.

Изменение имени пакета. Пакеты переименовываются по аналогии с классами.

Добавление недостижимого кода. Этот метод заключается в добавлении фрагментов кода, которые никогда не выполняются.

Проблемы и перспективы. Хотя обфускация и затрудняет обратный инжиниринг, она не делает его невозможным. Как пример, приложение, которое проверяет, аутентифицирован ли пользователь, написанное на C#, после обфускации и декомпиляции кода обратно можно заметить, что большая часть кода была переименована. Однако строки, содержащие текстовые сообщения (уведомления об успешном входе или неверных учетных данных), не были изменены. Это создает потенциальную угрозу, позволяя провести обратный инжиниринг.

Поскольку анализ текстовых сообщений позволяет восстановить логику работы исходного кода [2].

Также обфускация кода может оказывать негативное влияние на производительность итогового продукта. Это связано с тем, что в процессе обфускации оригинальные команды могут заменяться на большее количество команд. Это увеличивает количество выполняемых инструкций, что в конечном итоге приводит к увеличению времени выполнения программы.

Третий и главный минус – это невозможность обфускации в ее классическом понимании. Идеальная обфускация должна превращать программу в виртуальный черный ящик. Но было доказано, что обфускация не может достичь такого результата [3]. Авторы строят семейство функций, которые невозможно обфусцировать, что демонстрирует, что существует свойство π, которое можно эффективно вычислить, имея доступ к исходному коду программы, но невозможно вычислить с оракульным доступом к программе.

В настоящее время существует ряд решений для обфускации, но большинство из них являются либо платными, причем имеют высокую стоимость, сложные в использовании и не являются универсальными, либо бесплатными, но являются малоэффективными [5]. Также существующие методы обфускации не позволяют достичь полной защиты исходного кода, оставляя возможность опытным злоумышленникам проводить обратный инжиниринг.

Несмотря на существующие недостатки, обфускация показывает высокую эффективность при защите исходного кода от несанкционированного воздействия. Это подтверждает ее важность как одного из методов обеспечения безопасности исходного кода. Но учитывая тот факт, что недостатки оказывают значительное влияние на эффективность самой обфускации, необходимо дальнейшее изучение и развитие новых методов обфускации.

ЛИТЕРАТУРА

1. Алгоритмы и методы защиты программного кода на базе обфускации / А.В. Красов, И.П. Зуев, П.В. Карельский и др. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/algoritmy-i-metody-zaschity-programmnogo-koda-na-baze-obfuskatsii/viewer, свободный (дата обращения: 14.02.2025).

2. Don’t rely on obfuscation [Электронный ресурс]. – Режим доступа: https://www.codeproject.com/Articles/23794/Don-t-rely-on-obfuscation, свободный (дата обращения: 14.02.2025).

3. On the (im) possibility of obfuscating programs / B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang [Электронный ресурс]. – Режим доступа: https://www.iacr.org/archive/crypto2001/21390001.pdf, свободный (дата обращения: 17.02.2025).

4. Reverse engineering [Электронный ресурс]. – Режим доступа: https://www.techtarget.com/searchsoftwarequality/definition/reverse-engineering#:~:text=Reverse%2Dengineering%20is%20the%20act,duplicate%20or%20enhance%20the%20object, свободный (дата обращения: 19.02.2025).

5. Градский Д.Ю. Алгоритмы обфускации программного кода на языках скриптового программирования [Электронный ресурс]. – Режим доступа: https://elib.pnzgu.ru/files/eb/doc/MIExqoevWhxW.pdf, свободный (дата обращения: 23.02.2025).

6. What is Obfuscation? [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/what-is-obfuscation/, свободный (дата обращения: 23.02.2025).

7. Драгунцова И.С. Сравнительный анализ защиты информации методами криптографии, стенографии и обфускации // Молодой ученый. – 2022. – № 14 (409). – С. 9–11.

УДК 004.056.53

ОБЗОР МЕТОДОВ АНАЛИЗА КАНАЛОВ ЭНЕРГОПОТРЕБЛЕНИЯ

Е.Ю. Похила, студент каф. БИС

Научный руководитель М.М. Немирович-Данченко,
проф. каф. КИБЭВС, д.ф.-м.н.
г. Томск, ТУСУР, lisapokhila@mail.ru

Существуют инвазивные и побочные каналы утечки информации. Побочные каналы, в частности каналы энергопотребления, представляют большую опасность из-за сложности их предотвращения и выявления. В статье представлено описание методов анализа каналов энергопотребления.

Ключевые слова: информационная безопасность, атаки по каналам энергопотребления, простой анализ мощности, дифференциальный анализ мощности, корреляционный анализ мощности, шаблонные атаки, взаимный информационный анализ, оценка утечки тестового вектора.

Информационная безопасность критически важна. Исследование угроз необходимо для выявления уязвимостей и разработки эффективных мер защиты. Важно помнить, что уровень злоумышленников постоянно растет.

Современные устройства работают от электричества, что создает возможность утечки информации по каналам энергопотребления. Измеряя параметры этих каналов, можно выяснить информацию о выполняемых операциях.

Атаки по сторонним каналам делятся на активные и пассивные [1]. Атаки по каналам энергопотребления относятся ко второму виду.

Идея атаки заключается в том, что логические схемы потребляют разное количество энергии в зависимости от входных данных. Наблюдая за изменениями, можно понять, какие блоки активны, и получить информацию о данных.

Методы анализа каналов энергопотребления:

1. Простой анализ мощности (SPA) – это прямая интерпретация кривых энергопотребления. Например, анализируется сигнал микроконтроллера при шифровании AES в режиме ECB. Записывается сигнал потребления энергии, разбивается на фрагменты, соответствующие тактам процессора. Анализ показывает зависимость значения шифруемого байта и уровня потребляемой мощности. SPA позволяет узнать потребление энергии, время выполнения операций, особенности аппаратного обеспечения и, в некоторых случаях, восстановить ключ шифрования [2, 3].

2. Дифференциальный анализ мощности (DPA) использует статистические методы для выявления скрытых зависимостей. Например, для каждого блока данных записывается несколько измерений потребления энергии. Измерения группируются по значениям первого байта ключа, вычисляется среднее значение для каждой группы. По различиям в среднем потреблении энергии определяется правильное значение байта ключа. DPA позволяет получить значение секретного ключа шифрования, узнать особенности аппаратного обеспечения и используемые алгоритмы.

3. Шаблонные атаки (TA) – это атаки по заранее известным шаблонам. Например, анализируются данные об энергопотреблении предприятия за период. Извлекаются ключевые признаки (среднее значение, пиковые значения, кривые). Анализируются данные за прошлые периоды для выявления шаблонов. Текущие данные сравниваются с шаблонами. Отклонения указывают на неисправности, взлом, саботаж. TA позволяет прогнозировать энергопотребление, обнаруживать сбои, неисправности и угрозы безопасности [4].

4. Корреляционный анализ мощности (CPA) использует статистические методы для обнаружения связи между параметрами. Собираются данные, очищаются от шумов, выбираются метрики, вычисляются коэффициенты корреляции, строится график зависимостей. CPA позволяет определить атаки по резкому увеличению энергопотребления.

5. Взаимный анализ информации (MIA) определяет, насколько сильно потребление энергии криптографического устройства зависит от секретных данных. Например, для AES данные делятся на наборы, соответствующие частям ключа. Вычисляется взаимная информация между значением байта ключа и потреблением энергии. Высокое зна-

чение указывает на высокую вероятность правильного значения. MIA позволяет восстановить ключ частично или полностью [5].

6. Оценка утечки тестового вектора (TVLA) количественно измеряет утечку информации. Сравниваются реализации криптографических алгоритмов. Выбирается модель утечки, оцениваются параметры на основе данных энергопотребления. Вычисляется метрика утечки (вероятность утечки, информация о утечке). Результаты сравниваются с пороговым значением. TVLA не пытается восстановить ключ, а измеряет количество утечки.

ЛИТЕРАТУРА

1. Данилов И. Применение асинхронных схем для повышения защиты от атак по сторонним каналам / И. Данилов, П. Долотов // Безопасность информационных технологий. – 2022. – № 29 (2). – С. 112–127.

2. Standaert F. Introduction to Side-Channel Attacks // Secure Integrated Circuits and Systems. – 2010. – P. 27–42.

3. Randolph M. Power side-channel attack analysis: A review of 20 years of study for the layman / M. Randolph, W. Diehl // Cryptography. – 2020. – № 4 (2). – P. 15.

4. Won Y.-S. Key Schedule against Template Attack-Based Simple Power Analysis on a Single Target / Y.-S. Won, B.-Y. Sim, J.-Y. Park // Applied Sciences. – 2020. – № 10 (11). – P. 3804.

5. Schorn E. Machine Learning 104: Breaking AES With Power Side-Channels // Cryptography Services Practice, NCC Group. – 2023 [Электронный ресурс]. – URL: https://nccgroup.github.io/ataraxy/ml104/NCCGroup_ML104_blog.html (дата обращения: 15.02.2025).

УДК 004.94

СРАВНЕНИЕ ПОДХОДОВ К РАЗРАБОТКЕ НАДСТРОЕК ДЛЯ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ MODEL STUDIO CS

А.О. Сапунов, аспирант каф. КИБЭВС,
ТИМ-мастер «ТомскНИПИнефть»
Научный руководитель М.М. Немирович-Данченко,
д.ф.-м.н., проф. каф. КИБЭВС
г. Томск, ТУСУР, АО «ТомскНИПИнефть», sanovta@yandex.ru

Проводится сравнение подходов к разработке надстроек для комплексной системы информационного моделирования Model Studio CS при помощи COM API и NRX API.

Ключевые слова: надстройка, COM API, NRX API, информационное моделирование, Model Studio CS, MS.

Современное проектирование уже нельзя представить без использования информационных технологий и цифровых решений. Одним из таких решений является Model Studio CS (далее «MS»)– комплексная система для CAD-платформ, таких как AutoCAD и nanoCAD, которая состоит из множества модулей, каждый из которых отвечает за то или иное направление проектирования [1].

Так, например, MS «Трубопроводы» отвечает за проектирование трубопроводных систем всех типов, MS «Генплан» предназначен для создания генерального плана проекта, а MS «Молниезащита» предназначен для проектирования молниезащиты, заземления и расчета зон молниезащиты. Всего таких модулей в настоящий момент 16.

Каждый из модулей сделан под свою конкретную область в проектировании объектов строительства и имеет внушительный перечень возможностей и функционала. Однако в каждой организации, использующей такое ПО, всегда найдется место для уникальных задач, креативных идей, а также специфики и особенностей специалистов. Именно для таких случаев существует SDK MS (набор средств для разработки надстроек под платформу MS) [2].

Разработчики MS (СиСофт Девелопмент) предлагают два подхода к разработке надстроек: COM API и NRX API. Сравнение этих подходов может помочь будущим исследователям или специалистам определиться с тем, какой подход использовать лично им.

Разработка надстроек при помощи COM API. Первый подход представляет собой разработку надстроек при помощи программной платформы .NET на языке программирования C#. В SDK MS отсутствуют библиотеки COM API, т.к. все объекты COM здесь являются объектами типа dynamic (тип данных, обеспечивающий динамическую типизацию данных) [3]. Вместо библиотек пользователям предоставляется «Справочник COM» – документ, который можно использовать в качестве пособия по разработке надстроек для MS (документ состоит из более чем 90 страниц формата А4). В нем подробно описываются все классы, перечисления, интерфейсы, а также отношения между ними. Пример схемы отношений между объектами из справочника COM представлен на рис. 1.

Разработка надстроек при помощи NRX API. Следующий подход основывается на большом перечне подготовленных библиотек, написанных на языке программирования C++. В данном случае подход отличается от предыдущего – SDK MS содержит свыше тысячи различных файлов-заголовков (.h) и библиотек (далее просто библиотек) под любые задачи специалистов, однако никакой документации по их использованию официально не существует. Важно отметить, что для каждого модуля MS имеется свой набор библиотек.

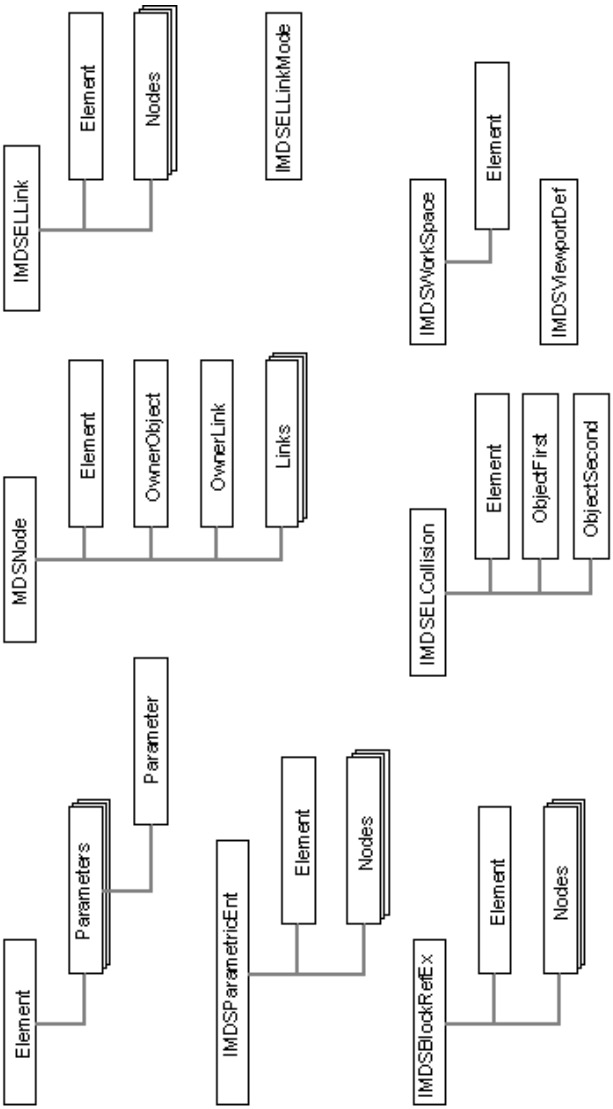

Рис. 1. Схемы отношений между объектами

Сравнение подходов к разработке надстроек. Сравнение было решено проводить по трем критериям – функциональные возможности, уровень описания функционала, а также порог вхождения для специалиста.

В первую очередь была проведена оценка функциональных возможностей. Определено, что с помощью NRX API можно повторить большую часть функций, которые имеются в MS. Также имеется возможность взаимодействовать с уже имеющимися элементами 3D-модели и создавать новые. С помощью COM API же можно лишь манипулировать существующими объектами модели, а также использовать их методы. Таким образом, было заключено, что в NRX API содержится более обширный функционал, чем в COM API.

Далее была проведена оценка уровня описания функционала. В данном случае COM API лучше описан, так как он по большей части состоит из описания объектов, с которыми предстоит работать использующим его. В NRX API, как было сказано ранее, документация отсутствует.

Далее была проведена оценка порога вхождения для специалиста. На данном этапе было определено, что для использования COM API достаточно базового знания принципов работы с платформой .NET. Все объекты API – динамические, что обязует специалиста читать «Справочник COM» и использовать то, что там написано. Для того, чтобы работать с NRX API, необходимы знания о работе с памятью, о разрядных архитектурах и в целом о том, как работать с C++ на достаточно высоком уровне, что делает порог вхождения для работы с NRX API выше, чем для COM API.

Подводя итоги, можно заключить, что на оба метода найдется свой пользователь. COM API подойдет специалистам с невысокими навыками программирования, которым необходимо решить небольшие задачи, связанные с чтением/изменением объектов 3D-модели. NRX API, в свою очередь, подойдет специалистам, занимающимся разработкой ПО, которым нужно писать новый функционал или автоматизировать объемные и сложные задачи.

ЛИТЕРАТУРА

1. Фахрутдинов А.Ю. Сравнение отечественного программного обеспечения по ТИМ-проектированию nanoCAD «инженерный BIM» и Model Studio CS / А.Ю. Фахрутдинов, Л.В. Фетисов // Наука и образование сегодня. – 2024. – № 2 (79). – С. 11–13.

2. Федухина Н.В. Сравнительный анализ российского программного обеспечения для информационного моделирования зданий и сооружений / Н.В. Федухина, Н.С. Астафьева // BIM-моделирование в задачах строительства и архитектуры. – 2023. – С. 389–394.

3. Зубов М.В. Получение типов данных в языках с динамической типизацией для статического анализа исходного кода с помощью универсального классового представления / М.В. Зубов, А.Н. Пустыгин, Е.В. Старцев // Вестник Астраханского гос. техн. ун-та. – Сер.: Управление, вычислительная техника и информатика. – 2013. – № 2. – С. 66–74.

УДК 004.056

ФУНКЦИИ ФИЛЬТРАЦИИ ТРАФИКА ПРОМЫШЛЕННОГО ПРОТОКОЛА ДЛЯ ЗАЩИТЫ АСУ ТП ОТ АТАК

И.Р. Трухманов, оператор роты (научной);
Л.В. Акопян, командир взвода роты (научной)
Научный руководитель А.А. Негурица, адъюнкт
научно-исследовательского центра
г. Санкт-Петербург, Военная орденов Жукова и Ленина
Краснознаменная академия связи им. Маршала Советского Союза
С.М. Буденного МО РФ, truhmanovigor@yandex.ru

Рассмотрены вопросы защиты автоматизированных систем управления технологическими процессами (АСУ ТП) от кибератак посредством фильтрации трафика промышленных протоколов. В условиях растущей цифровизации и подключения АСУ ТП к сети Интернет их уязвимость увеличивается, что делает необходимым применение эффективных методов защиты. Анализируются основные уязвимости промышленных протоколов, таких как отсутствие шифрования и неэффективные механизмы аутентификации. Описываются ключевые функции фильтрации трафика, включая мониторинг трафика, фильтрацию по IP-адресам, фильтрацию по протоколам и анализ поведения пользователей и устройств. Каждая функция детализируется с точки зрения технических процессов, что подчеркивает их важность для обеспечения безопасности АСУ ТП и предотвращения несанкционированного доступа.
Ключевые слова: АСУ, кибератаки, фильтрация, безопасность.

Автоматизированные системы управления технологическими процессами (АСУ ТП) играют ключевую роль в современных промышленных предприятиях. Однако с увеличением уровня цифровизации и подключенности к глобальной сети Интернет эти системы становятся уязвимыми для кибератак [1]. Для защиты АСУ ТП от угроз необходимо использовать эффективные методы фильтрации сетевого трафика, направленные на выявление и блокировку подозрительной активности. В этой статье рассматриваются функции по фильтрации трафика промышленных протоколов и их роль в обеспечении безопасности и защищенности АСУ ТП.

Промышленные протоколы и их уязвимости. Промышленные протоколы, такие как Modbus, DNP3, OPC UA и Profibus, широко используются для обмена данными между устройствами в АСУ ТП. Эти протоколы имеют свои особенности, которые могут быть использованы злоумышленниками:

1. *Отсутствие шифрования.* Многие промышленные протоколы не используют шифрование, что делает их уязвимыми для перехвата данных.

2. *Неэффективные механизмы аутентификации.* Некоторые протоколы допускают использование простых паролей или вообще не требуют аутентификации.

3. *Неполная проверка целостности.* Это может привести к модификации данных в процессе передачи.

Функции фильтрации трафика. Фильтрация трафика является важным элементом защиты АСУ ТП и включает в себя несколько ключевых функций:

1. Мониторинг трафика. Мониторинг сетевого трафика позволяет выявить аномалии и подозрительную активность. Это может быть реализовано с помощью систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS), которые анализируют пакеты данных в реальном времени.

Технический процесс:

– *сбор данных.* Установление точки мониторинга на сетевых устройствах для сбора информации о проходящем трафике;

– *анализ пакетов.* Использование инструментов анализа пакетов (например, Wireshark) для детального изучения заголовков и содержимого пакетов [3];

– *выявление аномалий.* Настройка правила для выявления аномалий, таких как неожиданные источники или назначения IP-адресов, необычные порты и частота запросов.

2. Фильтрация по IP-адресам. Фильтрация по IP-адресам позволяет ограничить доступ к АСУ ТП только для разрешенных устройств. Это помогает предотвратить несанкционированный доступ.

Технический процесс:

– *создание черных и белых списков.* Определение списка разрешенных (белый список) и запрещенных (черный список) IP-адресов;

– *настройка маршрутизаторов и брандмауэров* (Firewalle). Настройка правила фильтрации на уровне маршрутизаторов и брандмауэров, чтобы блокировать сетевой трафик от нежелательных источников.

3. Фильтрация по протоколам. Фильтрация по протоколам позволяет контролировать, какие протоколы могут использоваться в сети. Это особенно важно для защиты от уязвимостей, связанных с конкретными протоколами.

Технический процесс:

– *идентификация используемых протоколов.* Определение, используемых в сети промышленных протоколов;

– *настройка правил фильтрации.* Установление правил, которые разрешают или блокируют определенные протоколы на основе их безопасности и необходимости.

4. Анализ поведения. Анализ поведения пользователей и устройств (UEBA) позволяет выявлять подозрительные действия на основе анализа паттернов поведения [2].

Технический процесс:

– *сбор данных о поведении.* Установление системы для сбора данных о действиях пользователей и устройств в сети;

– *моделирование нормального поведения*. Создание модели нормального поведения для пользователей и устройств;

– *выявление аномалий.* Настройка системы для автоматического выявления отклонений от нормального поведения, что может указывать на потенциальные атаки или подозрительную активность.

5. Реагирование на инциденты. Фильтрация трафика должна быть частью более широкой стратегии реагирования на инциденты. Это включает в себя автоматическое блокирование подозрительных действий, и уведомление администраторов безопасности.

Технический процесс:

– *настройка автоматических реакций.* Определение действия, которые должны быть предприняты при обнаружении подозрительного трафика (например, блокировка IP-адреса);

– *уведомления.* Настройка системы уведомлений для информирования администраторов безопасности о потенциальных угрозах.

Заключение. Фильтрация трафика промышленных протоколов является критически важной мерой для защиты АСУ ТП от атак. Эффективная реализация функций мониторинга, фильтрации по IP-адресам и протоколам, анализа поведения и реагирования на инциденты позволяет значительно повысить уровень безопасности систем управления. В условиях постоянно растущих угроз важно не только внедрять эти меры, но и регулярно обновлять их в соответствии с новыми вызовами в области кибербезопасности.

ЛИТЕРАТУРА

1. Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review, свободный (дата обращения: 25.02.2025).

2. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования = Information technology. Security techniques. Information security management systems. Requirements: Национальный стандарт Российской Федерации: издание официальное: утв. и введ. Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст.: дата введ.: 01.01.2022.

3. Wireshark Foundation. Wireshark: The world’s foremost network protocol analyzer [Электронный ресурс]. – URL: https://www.wireshark.org (дата обращения: 25.02.2023).

УДК 004.056

ИЗУЧЕНИЕ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ГЕНЕРАЦИИ СЕТЕВОГО ТРАФИКА IXIA BREAKINGPOINT VE

С.А. Пашкевич, К.И. Цимбалов, аспиранты каф. КИБЭВС
Научный руководитель А.А. Конев, доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, psa@fb.tusur.ru

Рассмотрены некоторые особенности и функции программного комплекса для генерации сетевого трафика IXIA BreakingPoint VE, который позволяет проводить тестирование производительности и безопасности сетевой инфраструктуры.
Ключевые слова: IXIA BreakingPoint VE, трафик, IP-пакеты, атаки.

Современные информационные системы невозможно представить без сетевой инфраструктуры, которую необходимо постоянно тестировать и анализировать для обеспечения высокой производительности и безопасности. Одним из инструментов для решения таких задач является программный комплекс IXIA BreakingPoint VE.

IXIA BreakingPoint VE генерирует масштабируемый трафик реального мира для полного тестирования производительности и безопасности сетевой инфраструктуры. Поставляется в виде двух образов виртуальных машин (vController – виртуализированный системный контроллер, управляющий модулями vBlade и vBlade – виртуализированными нагрузочными модулями) и работает на частных облачных платформах, включая гипервизоры VMware ESXi и KVM, а также на VMware vCenter и OpenStack [1].

Данный программный комплекс включает в себя несколько различных тестовых компонентов для моделирования реальных приложений и угроз (рис. 1).

1. Application Simulator измеряет способность устройства обрабатывать различные потоки трафика прикладного уровня. Данный компонент генерирует реалистичные потоки трафика приложений и проверяет, что они правильно передаются устройством.

2. Live AppSim восстанавливает шаблоны трафика, записанные TrafficREWIND.

3. Client Simulation измеряет способность внешнего устройства обрабатывать различные потоки трафика уровня приложений на стороне клиента. Данный компонент генерирует реалистичные потоки трафика клиентских приложений и реагирует на активность внешнего сервера.

4. Session Sender измеряет способность устройства обрабатывать параллельные сеансы TCP. Данный компонент создаёт и поддерживает действительные TCP-сессии с искусственными данными.

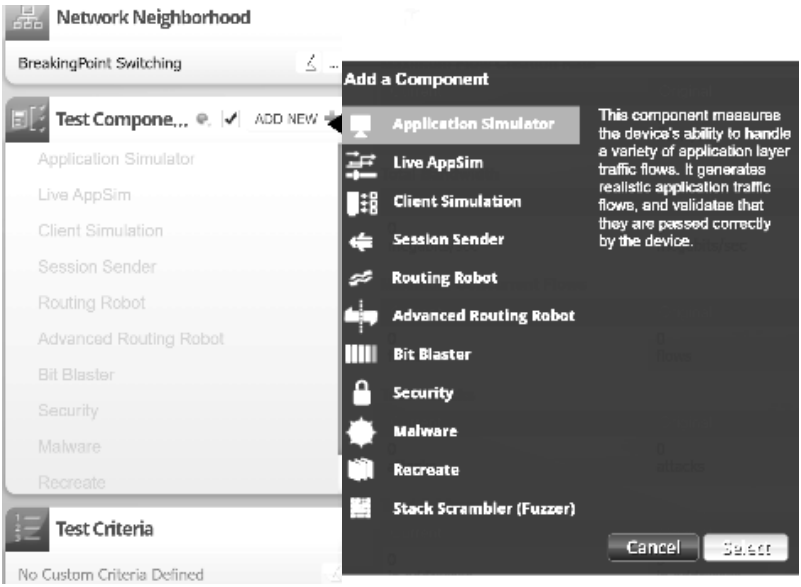

Рис. 1. Тестовые компоненты

5. Routing Robot измеряет способность устройства точно маршрутизировать IP-пакеты. Данный компонент отправляет IP-пакеты с искусственными полезными нагрузками и измеряет, достигают ли пакеты предполагаемого места назначения.

6. Advanced Routing Robot предоставляет функциональные возможности, аналогичные Session Sender и Routing Robot. Данный компонент позволяет настраивать или использовать расширенные пути сетевого окружения и синхронизировать транспорт UDP/TCP с уровнями IP.

7. Bit Blaster измеряет сырую пропускную способность устройства. Данный компонент отправляет допустимые кадры Ethernet уровня 2 с вымышленным содержимым и измеряет, достигают ли кадры своего предполагаемого назначения.

8. Компоненты Security и Malware измеряют способность устройства справляться с угрозами безопасности, отправляя на устройство живые эксплойты и проверяя, блокирует ли устройство атаки. Данные компоненты реалистично имитируют атакующего, а также ответы атакуемого хоста.

9. Recreate воссоздает захваченные шаблоны трафика.

10. Stack Scrambler (Fuzzer) измеряет способность устройства обрабатывать недействительные пакеты IP, TCP, UDP, ICMP и Ethernet.

Данный компонент отправляет недействительные IP-пакеты, созданные в результате фаззинга, и проверяет, что устройство продолжает работать.

В разделе LABS представлены готовые шаблоны. Одним из таких шаблонов является шаблон DDoS атаки, в котором можно провести гибкую настройку перед запуском (рис. 2).

Рис. 2. Шаблон DDoS-атаки

Исходя из вышесказанного можно сделать вывод о том, что программный комплекс IXIA BreakingPoint VE представляет собой мощный инструмент для тестирования производительности и безопасности. Благодаря своим функциональным возможностям, а именно моделированию реального трафика, генерации атак и тестированиб устойчивости устройств к различным угрозам, IXIA BreakingPoint VE позволяет эффективно оценивать и улучшать работу сетевой инфраструктуры.

ЛИТЕРАТУРА

1. BreakingPoint VE [Электронный ресурс]. – Режим доступа: https://www.keysight.com/us/en/products/network-security/breakingpoint-ve.html, свободный (дата обращения: 27.01.2025).

УДК 004.056

ФАЗЗИНГ: МЕТОДЫ И ПРИМЕНЕНИЕ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ

Г.Г. Варданян, студент каф. БИС

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

Проект ГПО БИС-2501. Безопасность исходного кода

г. Томск, ТУСУР, gevorg.585@list.ru

Представлен обзор современных методов фаззинга, применяемых для автоматизированного тестирования программного обеспечения. Рассмотрены основные подходы, включая слепой, мутационный, генеративный и гибридный фаззинг. Анализируются динамические и статические методы, а также применение алгоритмов машинного обучения, таких как трансформеры, генетические алгоритмы и графовые нейронные сети, для оптимизации процесса тестирования. Проведена классификация алгоритмов фаззинга, выявлены их преимущества и ограничения при поиске уязвимостей. Особое внимание уделено перспективам использования искусственного интеллекта для автоматизации тестирования и повышения эффективности обнаружения ошибок.

Ключевые слова: фаззинг, тестирование, безопасность, машинное обучение, алгоритмы, классификация, автоматизация, динамический анализ, генеративные модели.

Фаззинг – это процесс отсылки намеренно некорректных данных в исследуемый объект с целью вызвать ситуацию сбоя или ошибку. Настоящих правил фаззинга нет. Это такая технология, при которой успех измеряется исключительно результатами теста. Для любого отдельно взятого продукта количество вводимых данных может быть бесконечным. Фаззинг – это процесс предсказания, какие типы программных ошибок могут оказаться в продукте, какие именно значения ввода вызовут эти ошибки [1].

Обычно фаззинг лучше всего работает с программами, которые принимают входные данные, такие как веб-сайты, которые могут запрашивать ваше имя или возраст. Первое публичное употребление слова относится к исследовательскому проекту университета Висконсин Мэдисон [2]. С тех пор термин принят для обозначения целой методологии тестирования программного обеспечения.

В академическом мире фаззинг более всего связан с анализом граничных значений (boundary value analysis, BVA), при котором рассматривается диапазон удовлетворительных для конкретного входа значений и определяются тестовые значения, которые выходят за границы известных корректных и некорректных значений. Результаты BVA могут помочь убедиться в том, что метод исключений успешно фильтрует нежелательные значения, в то время как значения во всем

допустимом диапазоне ввести возможно. Фаззинг схож с BVA, но при фаззинге мы концентрируемся не только на граничных, но и на всех введенных значениях, которые могут вызвать непредсказуемое или небезопасное поведение тестируемого объекта.

В настоящее время существуют различные виды фаззинга, которые можно условно разделить на три основные категории: тестирование «черного ящика», «белого ящика» и «серого ящика». При использовании метода «черного ящика» тестировщик не имеет доступа к исходному коду приложения и работает только с его интерфейсом, что делает этот подход применимым даже к закрытым системам. Метод «белого ящика», напротив, предполагает детальное изучение внутренней логики программы, что позволяет нацеливаться на конкретные участки кода и выявлять сложные логические ошибки. Компромиссный вариант, известный как «серый ящик», сочетает преимущества обоих подходов: тестировщик обладает частичным знанием структуры программы, что позволяет оптимизировать процесс генерации тестовых данных без необходимости полного доступа к исходному коду.

Фаззинг нашёл широкое применение в области информационной безопасности. Он используется для выявления таких критических уязвимостей, как ошибки переполнения буфера, некорректное обращение с памятью и другие проблемы, способные привести к компрометации системы. В рамках аудитов безопасности этот метод позволяет не только обнаружить существующие проблемы, но и оценить общую устойчивость программного продукта к несанкционированным воздействиям. Благодаря фаззингу компании получают возможность оперативно реагировать на выявленные дефекты и предотвращать потенциальные атаки злоумышленников, что особенно важно в условиях постоянно растущих киберугроз.

Методы и алгоритмы фаззинга. Методы фаззинга можно условно разделить на несколько категорий, каждая из которых имеет свои особенности и применяется в зависимости от специфики тестируемых приложений. Основные методы фаззинга выглядят следующим образом: *слепой фаззинг* – метод, генерирующий случайные входные данные без учета структуры программы, отличается простотой и высокой скоростью, но имеет низкую вероятность выявления сложных участков кода, что может привести к пропуску критических ошибок.

Мутационный фаззинг основан на модификации корректных входных данных с помощью алгоритмов, изменяющих байты или структуру тестовых примеров, что позволяет целенаправленно исследовать уязвимости и повышает вероятность обнаружения скрытых ошибок.

Генеративный фаззинг создает входные данные с использованием моделей, учитывающих синтаксические и семантические особенности систем, что повышает эффективность обнаружения сложных ошибок благодаря нейронным сетям, хотя требует предварительного обучения на больших наборах данных.

Гибридные методы объединяют элементы статического и динамического анализа, адаптивно корректируя стратегию генерации данных; примером является coverage-guided фаззинг, использующий информацию о покрытии кода для направления тестирования, что способствует выявлению редких, но критически важных ошибок и повышает общую эффективность тестирования.

Проблемы и перспективы. Несмотря на существенные достижения, метод фаззинга сталкивается с рядом нерешённых проблем. Одной из основных задач остаётся создание качественных и репрезентативных наборов данных для обучения генеративных моделей, способных учитывать все особенности тестируемых систем [4].

Высокая вычислительная сложность и требовательность к ресурсам также остаются важными ограничениями при применении продвинутых методов фаззинга в реальных условиях. Перспективы развития данной области связаны с интеграцией фаззинга с методами статического анализа и динамического трассирования, что позволит более полно охватывать все возможные пути выполнения программ. Активное использование методов машинного обучения для адаптации алгоритмов к специфике тестируемых систем открывает новые возможности для повышения эффективности обнаружения уязвимостей и сокращения времени тестирования [3].

Будущее фаззинга связано с интеграцией новых технологий, таких как машинное обучение и искусственный интеллект, что позволит ещё более эффективно генерировать тестовые данные и анализировать поведение программ. Современные разработки направлены на адаптацию методик для тестирования распределённых систем и облачных сервисов, где традиционные подходы оказываются менее эффективными [9].

Таким образом, фаззинг остаётся важным и актуальным инструментом в арсенале специалистов по обеспечению безопасности программного обеспечения [6]. Он позволяет обнаруживать скрытые уязвимости, повышать надёжность приложений и снижать риск эксплуатации критических ошибок злоумышленниками. Постоянное развитие методов и инструментов фаззинга, а также их интеграция в процессы разработки помогают поддерживать высокий уровень защиты данных в условиях современной цифровой экономики. Несмотря на существующие ограничения, фаззинг демонстрирует свою эффективность

как метод автоматизированного тестирования, позволяющий своевременно выявлять и устранять ошибки, что делает его неотъемлемой частью современных подходов к обеспечению кибербезопасности [5].

ЛИТЕРАТУРА

1. Sutton M. Fuzzing: Brute Force Vulnerability Discovery / M. Sutton, A. Greene, P. Amini. – Publisher: Pearson Education, 2007. – 576 p.
2. Мишечкин М.В. Обзор различных средств фаззинга [Электронный ресурс]. – Режим доступа: https://moluch.ru/archive/186/47575/ (дата обращения: 01.03.2025).
3. Что такое фаззинг? Обзор нечеткого тестирования [Электронный ресурс]. – Режим доступа: https://wiki.merionet.ru/articles/cto-takoe-fazzing-opredelenie-necetkogo-testirovaniia-s-primerami (дата обращения: 02.03.2025).
4. Фаззинг для поиска уязвимостей: адаптация методов [Электронный ресурс]. – Режим доступа: https://ptresearch.media/articles/adaptiruem-fazzing-dlya-poiska-uyazvimostej (дата обращения: 05.03.2025).
5. Воробьев Е. Г. Технические средства и методы защиты информации / Е. Г. Воробьев, Т. В. Альшанская.
6. Лозовецкий В. В. Методы и средства защиты информации / В. В. Лозовецкий, Е. Г. Комаров; под ред. В.В. Лазовецкого. – 2-е изд., стер. – СПб.: Лань, 2025 – 224 с. [Электронный ресурс]. – Режим доступа: https://reader.lanbook.com/book/457268?demoKey=d8fc985aa4c244686ec659fd013cbe85#2 (дата обращения: 04.03.2025).
7. Fuzzing Testing Handbook [Электронный ресурс]. – Режим доступа: https://trailofbits.github.io/testing-handbook-preview/pr-preview/pr-33/docs/fuzzing/ (дата обращения: 01.03.2025).
8. Fuzzing for Software Security / M. Sutton, A. Greene, P. Amini et al.
9. DeMott J. Fuzzing Against the Machine / J. DeMott, M. Miller, C. Miller.
10. Fuzzing [Электронный ресурс]. – Режим доступа: https://www.sciencedirect.com/topics/computer-science/fuzzing#:~:text=Fuzzing%20is%20a%20process%20invulnerabilities%20such%20as%20buffer%20overflows (дата обращения: 05.03.2025).

УДК 004.424

ТОПОЛОГИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ «ЗВЕЗДА»

К.Д. Юркина, курсант

Научный руководитель А.В. Лубенцов, проф. каф. ОРЭ, к.геогр.н., доцент

г. Воронеж, Россия, Воронежский институт ФСИН России

yurkina_karina_05@mail.ru, lubensov@mail.ru

Рассматривается создание локальной вычислительной сети с помощью топологии «звезда». Приведены режимы функционирования,

разновидности данной топологии компьютерной сети, а также преимущества и недостатки.
Ключевые слова: топология, звезда, ЛВС, локальная сеть.

Топология – это пространственное расположение компьютерных сетей и метод соединения элементов линиями связи. Она определяет структуру связей между устройствами, возможности расширения сети, а также влияет на оборудование и методы управления обменом.

Существуют два основных типа топологий: физическая и логическая. К основным физическим относятся следующие три базовые топологии сети:

1) шина (bus);
2) кольцо (ring);
3) звезда (star).

Топология «звезда» является наиболее распространенной как для проводных, так и для беспроводных сетей. В ней все устройства подключены кабелем (витой парой) к центральному компьютеру или хабу (hub), который управляет обменом данными. Это создает большую нагрузку на центральный узел, что может ограничивать его функциональность.

Преимущества топологии «звезда» включают отсутствие конфликтов в работе сети и простоту управления. Однако недостатками являются высокие затраты на кабель, так как все устройства подключены к центральной точке, и уязвимость всей сети при выходе из строя центрального компонента. В случае поломки одного устройства или кабеля остальные устройства продолжают функционировать.

Анализ моделирования ЛВС. Сеть может работать в полудуплексном или дуплексном режиме в зависимости от поколения коммутатора:

• Беспроводные сети WiFi функционируют только в полудуплексном режиме, подключаясь к узлам поочередно.

• Сети с пассивными или активными концентраторами работают по принципу шины, где коммутатор передает пакеты всем узлам. Клиентские устройства не отражают пакеты, а только отправляют уведомления о получении. Такие сети быстрее шины благодаря лучшему качеству передачи.

• Сети со свитчами обеспечивают высокую скорость и возможность работы в режиме Full Duplex. Свитч создает временные таблицы соответствия портов и адресов, что позволяет направлять пакеты только к конкретным получателям, избегая коллизий и ускоряя передачу данных. Управляемые свитчи могут разделять сеть на изолированные подсети для управления доступом пользователей.

На рис. 1 представлен вид ЛВС с комбинированным режимом работы.

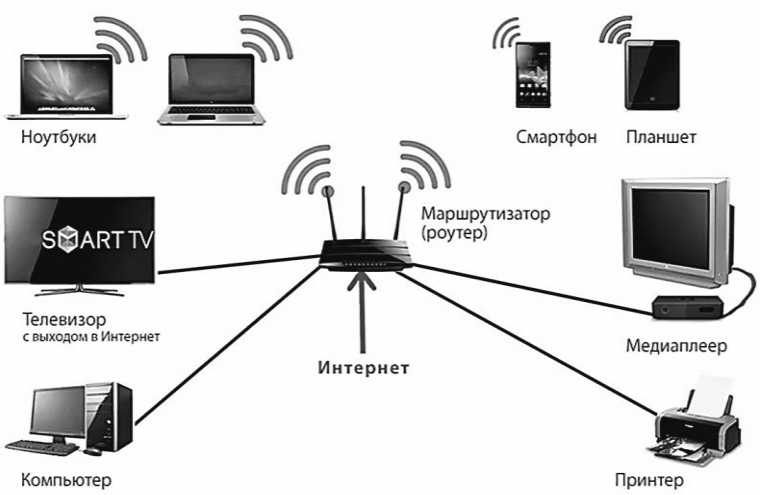

Рис. 1. Подключение оконечных устройств по топологии «звезда»

Топология «звезда» подходит для небольших офисных сетей, где достаточно подключить коммутатор и абонентов. Однако провайдеру может быть выгоднее использовать кольцевую топологию для подключения конечных пользователей, так как она обеспечивает защиту от обрывов проводов и отключения питания.

Помимо имеющихся топологий существуют также их гибриды, которые способны минимизировать недостатки основных видов и добавить некоторые преимущества. Далее представлены гибридные топологии для «звезды».

1. «Звезда-шина». Это комбинация топологий «шина» и «звезда», где несколько сетей «звезда» соединены магистральной линейной шиной. Данный вид создания локальной сети прост в реализации и имеет ряд преимуществ. В этой конфигурации выход из строя одного компьютера не влияет на остальную сеть, но сбой концентратора остановит все подключенные к нему устройства. На главный коммутатор лежит основная нагрузка и от него зависит подключение всех устройств к сети Интернет. Для увеличения надежности данной схемы следует приобрести мощный резервный коммутатор, на который можно будет в случае необходимости заменить главный сетевой коммутатор. Также необходимо иметь заранее сохраненную конфигурацию для того, чтобы уменьшить время замены.

2. «Звезда-кольцо». Данная топология напоминает «-везду-шину», так как компьютеры подключены к главному сетевому коммутатору, через который осуществляется выход в сеть Интернет. В данной схеме используется намного большее количество кабеля, но и надежность выше. При выходе из строя главного коммутатора локальная сеть продолжит свое функционирование без доступа в интернет. Однако можно переподключить оптоволоконный кабель, по которому происходит подключение к интернету, в другой коммутатор, тем самым можно полностью восстановить работоспособность ЛВС.

Недостатки топологии «звезда» зависят от центрального узла. Она используется в сетях с кабелем «витая пара» UTP 3-й и 5-й категории и коммутатором в качестве главного устройства. Существуют разные сетевые компоновки, но основными являются три топологии. Важно учитывать их преимущества и недостатки для выбора подходящей.

Выбор топологии зависит от конкретных потребностей сети, бюджета и требований к надежности. Топология «звезда» часто выбирается для небольших и средних офисных сетей благодаря своей простоте и удобству в управлении.

ЛИТЕРАТУРА

1. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей. – М.: Питер, Русская редакция, 2007.

2. Байер Доминик. Microsoft ASP .NET. Обеспечение безопасности. – М.: Питер, Русская Архитектура вычислительных сетей / Э.Я. Якубайтис-Статистика, 1980. Редакция, 2008.

УДК 004.056

РАЗРАБОТКА МОДУЛЕЙ ДЛЯ КИБЕРПОЛИГОНА НА БАЗЕ PYTHON КАК СРЕДСТВО АВТОМАТИЗАЦИИ ТЕСТИРОВАНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

И.С. Гущин, старший оператор роты (научной);
Д.В. Макаренко, адъюнкт научно-исследовательского центра
Научный руководитель В.А. Липатников, с.н.с. научно-исследовательского центра
г. Санкт-Петербург, Военная орденов Жукова и Ленина Краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного МО РФ, gushilya@gmail.com

Рассматривается разработка модулей для киберполигона на базе Python, предназначенных для автоматизации тестирования сетевой безопасности. Основное внимание уделяется созданию скриптов

для имитации атак, таким как сканирование сети и подбор паролей, а также интеграции с системами обнаружения вторжений (IDS) – Snort и Suricata. В работе формулируются цель и задачи исследования, приводится схема этапов реализации, описывается методика решения поставленной задачи и делается вывод, непосредственно вытекающий из выполненного анализа.
Ключевые слова: киберполигон, автоматизация тестирования, киберугрозы, мониторинг трафика.

Современные информационные системы постоянно подвергаются новым кибератакам, поэтому своевременное тестирование и анализ эффективности систем защиты остаются крайне важными. Однако в существующих исследованиях основное внимание уделяется либо методам мониторинга, либо базовому моделированию атак, в то время как интеграция с системами обнаружения вторжений (IDS) и анализ логов остаются недостаточно проработанными. Наше исследование направлено на комплексное решение этой проблемы, что делает его актуальным для современных условий, где требуется не только имитация атак, но и детальный анализ реакции IDS с целью оптимизации мер защиты.

Целью исследования является разработка модулей для автоматизации тестирования сетевой безопасности на базе Python. Для достижения поставленной цели решаются следующие задачи:

1. Разработать скрипты для автоматизированного сканирования сети с использованием библиотек socket и asyncio для выявления активных сервисов и открытых портов.

2. Создать модуль для перебора паролей (например, для SSH) с помощью библиотеки paramiko, что позволит оценить стойкость учетных данных.

3. Обеспечить интеграцию созданных модулей с системами обнаружения вторжений (IDS), такими как Snort и Suricata, посредством автоматизированного анализа логов.

Архитектура киберполигона. Киберполигон представляет собой виртуальную сеть, состоящую из нескольких компонентов. На одной стороне находится атакующая платформа, где запускаются Python-скрипты, выполняющие сканирование сети и подбор паролей. На другой стороне располагаются целевые сервисы, имитирующие реальные узлы корпоративной инфраструктуры (например, SSH-серверы или веб-сервисы). Третий компонент – системы обнаружения вторжений (IDS) Snort и Suricata – осуществляют мониторинг трафика и фиксируют подозрительную активность. Система логирования анализирует полученные данные, сопоставляет их с атаками и позволяет оперативно корректировать параметры защиты [1].

Создание скриптов имитации атак. Скрипты на Python позволяют автоматизировать различные сценарии атак, что делает процесс тестирования сетевой безопасности более эффективным и гибким. Одним из ключевых этапов является сканирование сети, которое можно выполнять с использованием библиотеки socket для работы с соединениями или asyncio для асинхронного взаимодействия с множеством узлов одновременно. Такой подход позволяет получать информацию о доступных сервисах, открытых портах и возможных точках входа [2].

Для подбора учетных данных в SSH-сервисах широко применяется библиотека paramiko, позволяющая осуществлять попытки аутентификации по заранее подготовленным спискам паролей. Этот метод помогает проверить стойкость паролей пользователей и оценить эффективность механизмов защиты, таких как блокировка IP-адресов после нескольких неудачных попыток входа. В зависимости от целей тестирования можно варьировать частоту и интенсивность запросов, изменяя скорость перебора паролей или моделируя атаки с различными временными интервалами. Это позволяет проверить реакцию систем обнаружения вторжений (IDS) в условиях реального сетевого трафика.

Сбор и анализ логов работы атакующих скриптов являются неотъемлемыми этапами тестирования. Они помогают не только оценить эффективность самой атаки, но и определить, какие действия были зафиксированы системами безопасности. Логи можно сопоставлять с журналами Snort и Suricata, чтобы выяснить, какие сигнатуры сработали, какие атаки остались незамеченными и как IDS классифицировала трафик.

Дополнительно анализ логов IDS помогает понять, насколько адекватно система реагирует на угрозы и какие её настройки требуют доработки. Например, если система слишком чувствительна и блокирует легитимный трафик, её параметры можно скорректировать, чтобы снизить уровень ложных срабатываний. Напротив, если атаки остаются незамеченными, необходимо доработать правила детектирования или обновить базу сигнатур. Таким образом, автоматизированное тестирование на основе Python позволяет не только выявлять уязвимости, но и оптимизировать защитные меры, повышая общую устойчивость сети к потенциальным атакам.

Интеграция с системами обнаружения вторжений. Snort и Suricata анализируют сетевой трафик, выявляя угрозы по сигнатурам. Snort использует сигнатурный анализ, а Suricata дополнительно поддерживает многопоточность и анализ пакетов. Логи IDS можно пар-

сить с помощью Python, извлекая данные о сработавших правилах и сравнивая их с параметрами тестов [3].

Использование JSON-логов Suricata позволяет в реальном времени анализировать атаки. Python-скрипты могут автоматически обрабатывать эти данные, формировать отчёты и помогать в настройке новых правил IDS [4].

Реагирование на инциденты. Для получения наиболее полной картины безопасности необходимо продумать серию разнообразных сценариев. Один из базовых сценариев – это простое сканирование с разной интенсивностью, которое позволяет увидеть, насколько быстро IDS реагирует на известные паттерны порт-скана. Другой сценарий может включать словарный перебор паролей к SSH или FTP, чтобы выяснить, на каком этапе система безопасности распознает угрозу. Можно также комбинировать несколько типов атак: проводить сканирование, перебор паролей и параллельно отправлять вредоносные пакеты, чтобы проверить способность IDS справляться с нагрузкой и не давать большого числа ложных срабатываний.

Заключение. Проведённое исследование демонстрирует, что комплексная автоматизация тестирования сетевой безопасности с использованием Python позволяет не только имитировать различные сценарии атак, но и проводить детальный анализ реакции систем обнаружения вторжений. Разработанные модули, объединённые в рамках киберполигона, обеспечивают последовательное выполнение этапов – от сканирования сети и подбора паролей до интеграции с IDS и анализа логов. Вывод, вытекающий из поставленной задачи, заключается в том, что внедрение данной системы автоматизированного тестирования позволяет оперативно выявлять уязвимости и корректировать настройки защитных систем, что является ключевым фактором для повышения безопасности современных информационных систем.

ЛИТЕРАТУРА

1. Степанов В.Ф. Информационная безопасность: теория и практика. – М.: Академический проект, 2019.

2. Лутц М. Изучаем Python. – М.: Диалектика, 2013.

3. Snort – система обнаружения вторжений: установка и настройка [Электонный ресурс]. – URL: https://habr.com/ru/post/128800/ (дата обращения: 27.02.2025).

4. Suricata – современная IDS/IPS: обзор возможностей и настройка. [Электонный ресурс]. – URL: https://habr.com/ru/post/461234/ (дата обращения: 27.02.2025).

УДК 004.056

УСТОЙЧИВОСТЬ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ С УЧЕТОМ РЕШЕНИЙ, ИСПОЛЬЗУЕМЫХ ДЛЯ ЗАЩИТЫ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ ОТ АТАКИ «СКАНИРОВАНИЕ СЕТИ»

Д.В. Макаренко, адъюнкт;
Я.Г. Солдатенко, старший оператор роты научной
Научный руководитель В.А. Липатников, д.т.н., проф., с.н.с.
г. Санкт-Петербург, Военная орденов Жукова и Ленина Краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного МО РФ, sokoltyp@gmail.com, nsdivdeni@yandex.ru

Описывается атака «сканирование сети». Данная атака относится к подготовительному этапу при выполнении вредоносного воздействия на сети передачи данных. Для построения системы защиты первоначально разбираются все возможные сценарии действий нарушителей, что наглядно отображено в данной статье. Проведен первоначальный анализ атаки с построением математической модели. По итогам построенной модели с учетом средств защиты составлена система дифференциальных уравнений с последующим ее решением. Построены графы, отображающие динамику повышения вероятности на успешную реализацию атаки в зависимости от времени, потраченного на реализацию одного этапа.
Ключевые слова: сети передачи данных, атаки на сети передачи данных, сканирование сети.

Атака сканирования сети (network scanning) – это процесс исследования сети с целью сбора информации о её структуре, активных устройствах, открытых портах, операционных системах (ОС) и других характеристиках. Это один из первых этапов, который злоумышленники используют для подготовки к более серьёзным атакам, таким как эксплуатация уязвимостей или несанкционированный доступ к сети передачи данных (СПД) [2, 3].

В качестве основных этапов атаки были выбраны следующие:

– обнаружение активных хостов;

– сканирование портов и определение служб, работающих на этих портах, у обнаруженных объектов;

– определение типа ОС, установленных на объектах сети.

Построена дискретная система одноканального многофазового массового обслуживания с ожиданием.

Модель атаки «сканирование сети» представлена в виде графа, состоящего из конечного числа возможных состояний и переходов системы из одного состояния в другое [1]. Ввиду маловероятного воз-

никновения очереди данную модель можно представить в виде схемы на рис. 1.

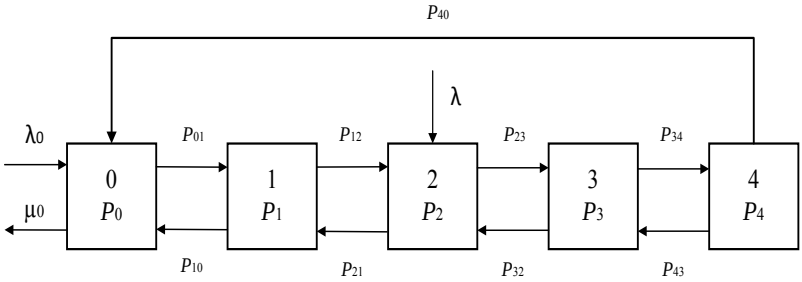

Рис. 1. Модель атаки «сканирование сети»

На данной схеме представлены следующие этапы:

1. P_0 – ожидание запроса на атаку.
2. P_1 – обнаружение объектов сети.
3. P_2 – сканирование портов.
4. P_3 – определение типа ОС.
5. P_4 – конец атаки и возвращение к этапу.

Исходя из данной модели, можно определить разницу с ранее построенной. Следующим шагом была написана система дифференциальных уравнений для расчета вероятности реализации атаки.

Система будет состоять из 5 уравнений, где выходящий вектор представлен со знаком (–), а входящий – со знаком (+) [1].

Вероятность того, что за время Δt не поступит ни одной задачи на вторжение, равна $e^{-\lambda_0 \Delta t} \approx 1-\lambda_0 \Delta t$, а вероятность того, что за время Δt система проведёт кибервторжение, равна $\mu_0 \Delta t$, вероятность того, что за время Δt не поступит ни одной задачи и система не освободится, равна $e^{-\lambda_0 \Delta t} \cdot e^{-\mu_0 \Delta t} \approx 1-(\lambda_0+\mu_0)\Delta t$.

Вероятности нахождения системы в определённых состояниях можно определить по некоторым значениям временных параметров.

Вероятность P_4 можно принять за вероятность воздействия, если считать, что после реализации одного воздействия система сразу же приступает к реализации другого, т.е. система должна эффективно работать и в состоянии штатной работы (P_0). Таким образом, вероятность воздействия $K_B = P_0 + P_4$ примет вид

$$P_B = \frac{1+\alpha}{1+\alpha \cdot \left(1+E+\dfrac{(\beta_3+\lambda)\mu_0}{\beta_2\beta_3}+\dfrac{\mu_0}{\beta_3}\right)}.$$

При тестировании программы Nmap были сделаны замеры времени, которое необходимо для реализации этапов атак. Итог замеров представлен в таблице. Далее, подставляя полученные значения, были построены графики каждого этапа.

Временные параемтры событий

Событие	Описание	Параметр	Значение
P_1	Выполнение команды ping	$\beta_1 = \frac{1}{t_1}$	1,2 с 1,5 с 1,8 с
P_2	Сканирование портов	$\beta_2 = \frac{1}{t_2}$	2,5 с 2,7 с 2,9 с
P_3	Обнаружение ОС	$\beta_2 = \frac{1}{t_3}$	0,8 с 1 с 1,2 с

Построен график функции для наглядного визуального отображения динамики развития атаки «сканирование сети», изображенный на рис. 2.

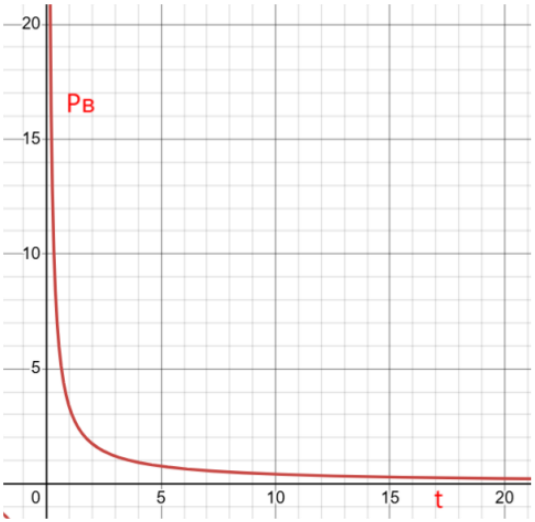

Рис. 2. Динамика развития атак

На рис. 2 изображена динамика изменения вероятности в зависимости от времени перехода между этапами.

Заключение. Данная модель атаки позволяет наглядно изучить все основные этапы атаки «сканирование сети», что позволяет, под-

ставляя значения временных параметров интенсивности переходов между этапами, определить вероятность реализации атаки на СПД. Данная модель помогает более точно выстраивать защиту СПД и позволяет выбирать наиболее подходящие средства защиты.

ЛИТЕРАТУРА

1. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя / В.А. Липатников, А.А. Шевченко, В.С. Косолапов, Д.С. Сокол // Информационно-управляющие системы. – 2022. – № 1 (116). – С. 54– 67.

2. Бегаев А.Н. Тестирование на проникновение / А.Н. Бегаев, С.Н. Бегаев, В.А. Федотов. – СПб.: Университет ИТМО, 2018. – 45 с.

3. Ожиганова М.И. Повышение уровня информационной защищенности корпоративной компьютерной сети за счет разработанных модулей сканирования сетевых ресурсов / М.И. Ожиганова, А.В. Колесников, А.Ю. Колодяжная // Перспективы развития информационных технологий. – 2015.

4. Актуальные проблемы инфотелекоммуникаций в науке и образовании: матер. конф. – СПб.: СПбГУТ им. М.А. Бонч-Бруевича, 2023. – Т. 3. – 915 с.

5. Липатников В.А. Способ обнаружения и классификации многоэтапной атаки на основе долгой краткосрочной памяти / В.А. Липатников, А.А. Ломанов // Технологии. Инновации. Связь: сборник матер. науч.-практ. конф. – СПб.: Военная академия связи им. Маршала Советского Союза С.М. Буденного, 2022. – С. 104–108.

6. Задбоев В.А. Способ защиты информационной сети с использованием метода определения местоположения злоумышленника / В.А. Задбоев, В.А. Липатников, К.В. Мелехов // Технологии. Инновации. Связь: сборник матер. науч.-практ. конф. – СПб.: Военная академия связи им. Маршала Советского Союза С.М. Буденного, 2023. – С. 138–143.

ПОДСЕКЦИЯ 4.2

ЦИФРОВЫЕ СИСТЕМЫ РАДИОСВЯЗИ И СРЕДСТВА ИХ ЗАЩИТЫ

*Председатель – **Голиков А.М.**, доцент каф. РТС, к.т.н., с.н.с.;*
*зам. председателя – **Громов В.А.**, доцент каф. РТС, к.т.н.*

УДК 621.396.946

ПРОЕКТИРОВАНИЕ ВЫСОКОСКОРОСТНОЙ СИСТЕМЫ СВЯЗИ НА БАЗЕ СОЗВЕЗДИЙ КОСМИЧЕСКИХ АППАРАТОВ

А.А. Майков, М.В. Изупов, А.Е. Томских, Е.В. Черкасская, Г.Б. Герман, студенты каф. РТС

Научный руководитель А.М. Голиков, к.т.н., с.н.с., доцент каф. РТС
г. Томск, ТУСУР, rts2_golikov@mail.ru

Описаны проектные разработки высокоскоростных систем связи, перспективных методов построения патч-антенных систем для создания локальных систем связи с пространственно-временным кодированием MIMO.

Ключевые слова: многоуровневые методы цифровой модуляции DVB-S2X, патч-антенные системы (LDPC), пространственно-временное кодирование MIMO.

При выполнении заданий проекта разработана высокоскоростная система связи для созвездий космических аппаратов (КА), которая включает ряд прорывных технологий, например, многоуровневые методы цифровой модуляции DVB-S2X (32APSK) и DVB-S2X (64APSK, 128APSK, 256APSK), быстродействующие и высокоэффективные методы помехоустойчивого кодирования (LDPC), перспективные методы построения патч-антенных систем с пространственно-временным кодированием MIMO. Высокоскоростная система связи построена на базе новой системы широкополосной связи DVB-S2X и предназначена для создания локальных систем связи в удаленных районах или в зоне чрезвычайных ситуаций.

Многоуровневые модуляции DVB-S2X [1], обеспечивают передачу потокового видео 4K (рис. 1–4).

Зависимости BER от SNR для каждого метода модуляции представлены на рис. 5. Графики зависимостей позволяют оценить необходимые SNR для достижения минимальной битовой ошибки.

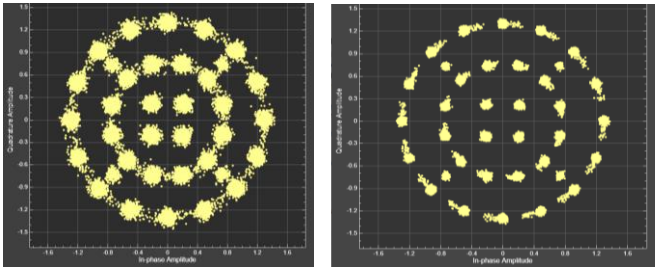

Рис. 1. Созвездие 32APSK 9/10 для разных SNR (25 и 35 дБ)

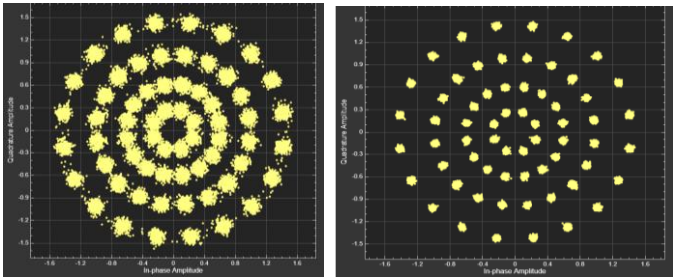

Рис. 2. Созвездие 64APSK 7/9 для разных SNR (25 и 38 дБ)

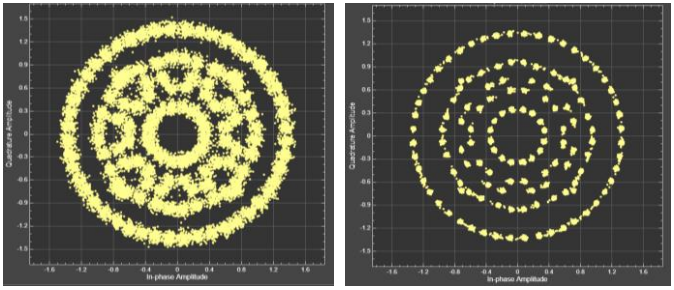

Рис. 3. Созвездие 128APSK 135/180 для разных SNR (25 и 40 дБ)

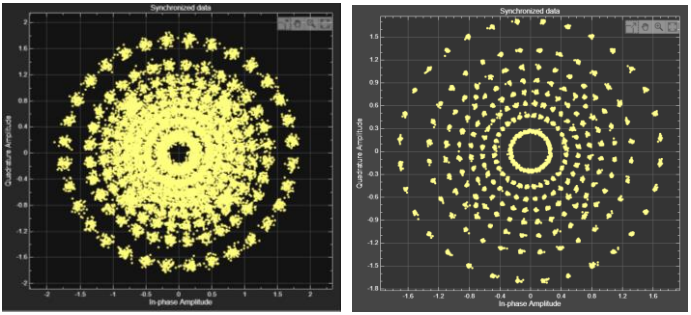

Рис. 4. Созвездие 256APSK 116/180 для разных SNR (25 и 40 дБ)

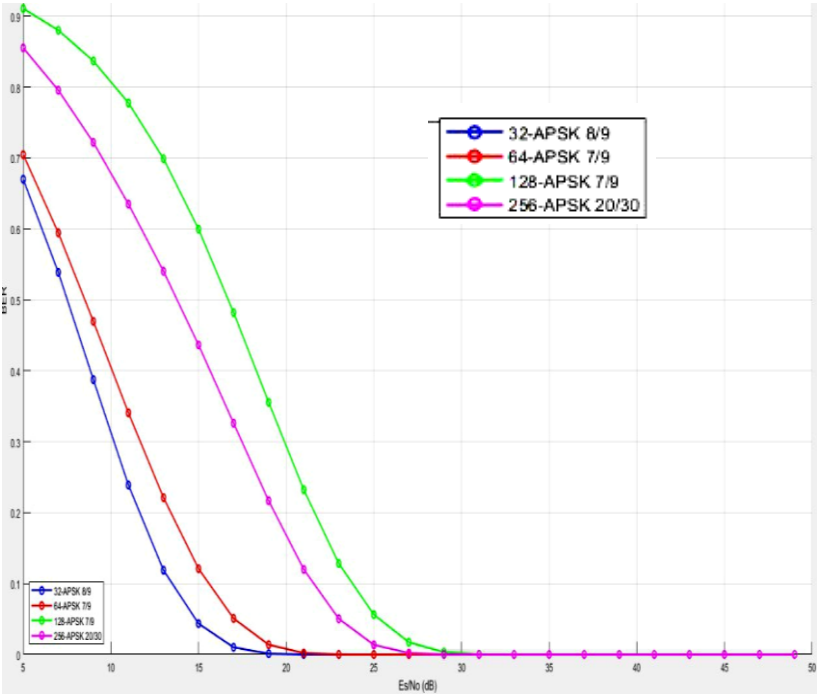

Рис. 5. Зависимость BER от SNR для различных уровней модуляции

В проекте разработаны 3D-модели двухполяризационных патч-антенн, позволяющих создать технологию пространственно-временного кодирования и увеличить скорость передачи данных в 4 раза.

Таким образом, предложены перспективные методы для создания высокоскоростной системы связи на базе созвездий космических аппаратов.

ЛИТЕРАТУРА

1. Голиков А.М. Системы цифровой радиосвязи: учеб. – М.: Ай Пи Ар Медиа, 2022. – 340 с. [Электронный ресурс]. – URL: https://doi.org/10.23682/117865 (дата обращения: 8.03.2024).

УДК 621.376.6

ПРЕЦИЗИОННАЯ СИСТЕМА ПОЗИЦИОНИРОВАНИЯ НА БАЗЕ СОЗВЕЗДИЙ БПЛА

М.А. Кызласов, М.Е. Ильясов, Е.Д. Морозов, студенты каф. РТС
Научный руководитель А.М. Голиков, к.т.н., с.н.с., доцент каф. РТС
г. Томск, ТУСУР, rts2_golikov@mail.ru

Выполнено проектирование прецизионной системы позиционирования на базе созвездий беспилотных летательных аппаратов (БПЛА). Разработанная система использует высокоскоростные Mesh-сети, дифференциальные методы навигации (RTK, PPP), а также методы частотного доступа FDMA/CDMA для достижения высокой точности позиционирования автономных объектов. В рамках исследования проведены моделирование работы системы, анализ её эффективности и перспектив внедрения.

Ключевые слова: прецизионное позиционирование, созвездие БПЛА, Mesh-сети, Real Time Kinematic (RTK), Point-to-Point Protocol (PPP), Frequency-division multiple access (FDMA), Code Division Multiple Access (CDMA), навигационные системы, беспилотные технологии.

Современные задачи точного позиционирования требуют разработки новых технологий, обеспечивающих сантиметровую точность в реальном времени. В связи с этим особую актуальность приобретают инновационные методы, способные обеспечить надежную и высокоточную навигацию даже в условиях сложных рельефов и возможных помех.

Прецизионные системы позиционирования необходимы в различных областях, таких как геодезия, сельское хозяйство, военные и спасательные операции, управление автономными транспортными средствами, мониторинг инфраструктуры, а также в сферах, связанных с безопасностью и разведкой. Традиционные спутниковые системы, такие как GNSS, GPS и ГЛОНАСС, не всегда обеспечивают требуемую точность, особенно в сложных условиях, включая городскую застройку, густые лесные массивы, тоннели, подземные сооружения и промышленные зоны с сильными радиочастотными помехами. Развитие созвездий БПЛА позволяет компенсировать недостатки глобальных систем навигации, обеспечивая точное определение координат объектов даже в условиях сложного рельефа, динамических помех и нестабильности сигналов.

Разработанная система основывается на применении высокоскоростных Mesh-сетей (IEEE 802.11s), обеспечивающих надежную связь между БПЛА, что позволяет обмениваться данными без центрального узла. Это делает систему масштабируемой и адаптивной к различным

условиям работы, а также позволяет наращивать количество взаимодействующих аппаратов без существенного снижения эффективности системы. Дифференциальные системы навигации, такие как RTK и PPP, значительно повышают точность позиционирования с 1–5 м до 2 см за счёт передачи корректировок от базовых станций. Эффективность передачи данных обеспечивается методами многоканального доступа (FDMA, CDMA), что позволяет снизить помехи, улучшить синхронизацию сигналов, повысить устойчивость системы к внешним воздействиям, а также уменьшить вероятность сбоев и потерь информации.

Для повышения точности также применяются псевдошумовые последовательности (m-последовательности), улучшающие фазовую обработку сигналов, уменьшающие уровень ошибок позиционирования и повышающие надежность передачи данных даже в условиях сложной радиочастотной обстановки.

В рамках исследования проведено детальное сравнение различных технологий навигации для беспилотных летательных аппаратов. Анализируются преимущества и недостатки традиционных спутниковых систем GNSS по сравнению с системами позиционирования на основе БПЛА.

Проведенное моделирование в MatLab продемонстрировало, что точность позиционирования достигает 2 см при использовании RTK и Mesh-сетей с высокой пропускной способностью.

Разработанная система позиционирования на базе созвездий БПЛА является перспективной альтернативой спутниковым GNSS-системам, обеспечивая повышенную точность, автономность и адаптивность к различным условиям эксплуатации. Применение Mesh-сетей, современных алгоритмов обработки сигналов и коррекции ошибок позволяет существенно улучшить характеристики системы по сравнению с традиционными методами навигации. Будущие исследования могут быть направлены на интеграцию искусственного интеллекта для адаптивного управления роем БПЛА, оптимизацию маршрутов передачи данных и разработку более энергоэффективных алгоритмов обработки навигационных сигналов.

ЛИТЕРАТУРА

1. Аппаратура высокоточного позиционирования по сигналам глобальных навигационных спутниковых систем: приемники-потребители навигационной информации / А.Д. Борискин, А.В. Вейцель, В.А. Вейцель, М.И. Жодзишский, Д.С. Милютин; под ред. М.И. Жодзишского. – М.: Изд-во МАИ-ПРИНТ, 2010. – 292 с.

УДК 629.786.2

ПРЕЦИЗИОННАЯ СИСТЕМА ПОЗИЦИОНИРОВАНИЯ НА БАЗЕ СОЗВЕЗДИЙ КА

Н.В. Муковников, студент каф. РТС

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

г. Томск, ТУСУР, rts2_golikov@mail.ru

Работа посвящена проектированию прецизионной системы позиционирования на базе созвездий кубсатов. Описываются основные компоненты системы, включая высокоскоростные Mesh-сети передачи данных и дифференциальные системы навигации. Анализируются методы и алгоритмы, используемые для достижения высокой точности позиционирования, а также представлены результаты системного анализа.

Ключевые слова: кубсат, прецизионное позиционирование, Mesh-сети, дифференциальная навигация, MIMO, DVB-S2.

Современные требования к точности позиционирования в различных областях, таких как навигация, геодезия и мониторинг окружающей среды, стимулируют разработку новых технологий. Одним из перспективных направлений является использование созвездий космических аппаратов кубсат для создания прецизионных систем позиционирования.

Кубсат – это тип миниатюрных спутников, разработанных для использования в космических исследованиях и различных приложениях. Они стандартизированы по размеру и форме, что позволяет значительно снизить затраты на их производство и запуск. Обычно имеют форму куба с размером стороны 10 см (1U). Могут быть объединены в более крупные модули, например, 2U, 3U и т.д.

Проектируемая система прецизионного позиционирования на базе кубсатов включает следующие ключевые компоненты:

1. Созвездие кубсатов: группа малых спутников, обеспечивающих глобальное покрытие и передачу данных через высокоскоростные Mesh-сети.

2. Наземные станции: антенны и приемники, предназначенные для получения сигналов от спутников и передачи данных на центральный сервер.

3. Центральный сервер обработки данных: выполняет расчет координат и корректировку данных.

4. Антенная система MIMO 4×4: обеспечивает высокую пропускную способность и надежность связи.

5. Линия связи: реализуется на базе стандарта DVB-S2 для передачи данных на наземные станции.

Планируется производить позиционирование наземных обьектов по аналогии с системой ГЛОНАСС, но с более высокой точностью за счет использования новых технологий.

Современные системы позиционирования построены на комплексном использовании передовых технологических решений. Для обеспечения высокой точности определения местоположения применяются специальные псевдослучайные сигналы, среди которых особое место занимают m-последовательности, а также коды Голда и Уолша. Эти сигналы позволяют эффективно бороться с помехами и значительно повышают точность позиционирования.

В дополнение к этому системы используют различные методы множественного доступа к частотному спектру, такие как FDMA и CDMA, что обеспечивает их оптимальное распределение и эффективное использование доступных радиочастотных ресурсов. Особую роль в повышении точности позиционирования играют дифференциальные навигационные системы. Они корректируют данные с помощью группировки спутников кубсат, что позволяет достичь максимальной точности определения местоположения.

В ходе проектирования и исследований были разработаны алгоритмы программного обеспечения для построения прецизионной системы позиционирования. Проведен системный анализ достигнутых технических характеристик, который показал соответствие системы заданным требованиям. Разработанная система позиционирования на базе созвездий КА является перспективной альтернативой спутниковым GNSS-системам, обеспечивая повышенную точность, автономность и адаптивность к различным условиям эксплуатации. Применение Mesh-сетей, современных алгоритмов обработки сигналов и коррекции ошибок позволяет существенно улучшить характеристики системы по сравнению с традиционными методами навигации. Будущие исследования могут быть направлены на интеграцию искусственного интеллекта для адаптивного управления роем КА.

ЛИТЕРАТУРА

1. Аппаратура высокоточного позиционирования по сигналам глобальных навигационных спутниковых систем: приемники-потребители навигационной информации / А.Д. Борискин, А.В. Вейцель, В.А. Вейцель, М.И. Жодзишский, Д.С. Милютин; под ред. М.И. Жодзишского. – М.: Изд-во МАИ-ПРИНТ, 2010. – 292 с.

УДК 621.376.6

ВЫСОКОТОЧНАЯ СИСТЕМА МОНИТОРИНГА С НЕЙРОСЕТЕВОЙ ОБРАБОТКОЙ НА БАЗЕ СОЗВЕЗДИЙ КОСМИЧЕСКИХ АППАРАТОВ

А.В. Зяблицев, Е.Д. Морозов, М.Е. Ильясов, М.А. Кызласов, студенты каф. РТС

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

г. Томск, ТУСУР, rts2_golikov@mail.ru

Работа посвящена разработке высокоточной системы мониторинга с нейросетевой обработкой на базе созвездий космических аппаратов, что представляет собой новый виток развития в области систем мониторинга и их точности. Был предложен алгоритм на основе нейронных сетей по увеличению точности. Проведено моделирование. Показана эффективность использования нейросетевой обработки в системах мониторинга.

Ключевые слова: машинное обучение, нейронная сеть, обработка информации, мониторинг, космический аппарат.

Нейронная сеть YOLO представляет собой двухуровневую нейронную сеть преимущественно со сверточными слоями. Она способна обрабатывать все регионы изображения за один раз. Она имеет лучшие значения по соотношению скорости и точности. Ее структура представлена на рис. 1.

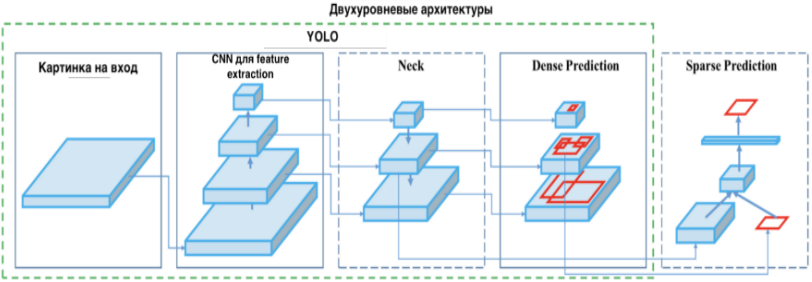

Рис. 1. Структура нейронной сети YOLO

На данных момент существует 8 разных версий нейронной сети YOLO, каждая из которых еще подразделяется на несколько в зависимости от ее размера. Для исследования получаемых метрик в данной работе будем пользоваться самыми популярными версиями 5, 8 и 11, а также различными размерами, такими как n и s. Необязательно использовать самую большую модель, так как это будет очень ресурсозатратно, и важно подобрать оптимальные модели под конкретные

задачи, чтобы не было избыточности, но и не было недостатка точности распознавания.

По мере обучения будут получены следующие метрики:

- P (Precision) – точность обнаруженных объектов, показывающая, сколько обнаружений было верным;
- R (Recall) – способность модели идентифицировать все экземпляры объектов на изображениях;
- mAP50 – средняя точность модели при пороге в 0,5;
- mAP50-95 – среднее значение точности модели, рассчитанное при различных значениях порога от 0,5 до 0,95, дает понимание о работе модели при разных уровнях сложности обнаружения.

Также каждая из получаемых метрик получена как для всех классов, так и отдельно для каждого, что может показать, какие объекты модель способна определить с большей точностью, а с какими у нее возникают трудности.

Проведено исследование точности распознавания объектов в зависимости от модели (таблица).

Сравнительная таблица нейронных сетей YOLO по всем классам

Версия	Precision	Recall	mAP50	mAP50-95
YOLOv5n	0,899	0,874	0,957	0,754
YOLOv5s	0,856	0,875	0,94	0,743
YOLOv8n	0,809	0,85	0,872	0,651
YOLOv8s	0,734	0,83	0,894	0,671
YOLOv11n	0,887	0,939	0,947	0,729
YOLOv11s	0,915	0,913	0,954	0,765

Данное исследование позволяет сделать обоснованные выводы о том, какие версии нейронной сети YOLO будут наиболее эффективными для задачи мониторинга, а также как повысить точность системы, прибегая к нейросетевой обработке.

ЛИТЕРАТУРА

1. Голиков А.М. Системы цифровой радиосвязи: учеб. – М.: Ай Пи Ар Медиа, 2022. – 340 с. [Электронный ресурс]. – URL: https://doi.org/10.23682/117865 (дата обращения: 03.03.2025).

УДК 621.376.6

РАЗРАБОТКА СИСТЕМЫ ОБРАБОТКИ СИГНАЛОВ МНОГОСПУТНИКОВОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ «МАРАФОН IOT» НА БАЗЕ LORAWAN

В.В. Борисова, студентка каф. РТС

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

г. Томск, ТУСУР, rts2_golikov@mail.ru

Мы разрабатываем систему обработки данных для спутниковой сети «Марафон IoT», чтобы IoT-устройства могли передавать данные по всему миру через спутники LoRaWAN. Наша система должна быть очень эффективной, потому что у спутников ограниченная «ширина канала» (пропускная способность), связь с ними осуществляется на большом расстоянии, а IoT-устройства должны долго работать от батарейки.

Ключевые слова: LoRaWAN, Марафон IoT.

Марафон IoT – разрабатываемая многоспутниковая система связи, предназначенная для сбора и передачи телеметрической информации в диапазонах ISM и S. Низкоорбитальная группировка (264 спутника на высоте 750 км) обеспечит глобальное покрытие и поддержку широкого спектра приложений: от мониторинга окружающей среды и оптимизации сельского хозяйства (мониторинг параметров почвы и воздуха) до приёма сигналов автоматического зависимого наблюдения-вещания (АЗН-В) с воздушных судов, что способствует повышению безопасности полётов. Внешний вид КА представлен на рис. 1.

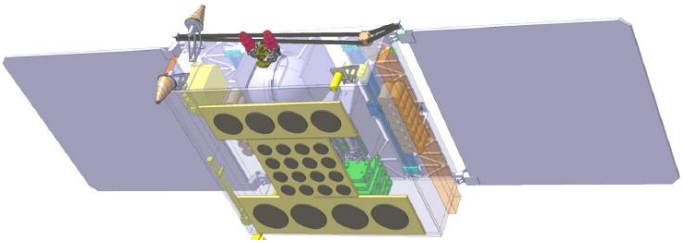

Рис. 1. Внешний вид КА «Марафон IoT»

«Марафон IoT» задуман как универсальный ресурс для организации сервисов передачи данных, что позволит создавать многочисленные приложения для конечных пользователей, в том числе в сочетании с другими информационными системами.

Разработка многоспутниковой системы находится на стадии проектирования, включающей подготовку технического предложения и эскизного проекта.

Планируемые характеристики системы «Марафон-IoT»

Тип орбиты	Круговая
Количество аппаратов в орбитальной группировке	264 (в том числе 12 резервных аппаратов)
Высота орбиты, км	750
Количество орбитальных плоскостей	12
Наклонение орбитальных плоскостей	87,2º
Продолжительность витка	5984,76 с
Максимальная продолжительность тени	35 мин
Срок активного существования космического аппарата, лет	4–5 (с доведением до 7)
Стоимость серийного космического аппарата на заводе-изготовителе	Не более 35 млн руб.

ЛИТЕРАТУРА

1. Голиков А.М. Бортовые радиоэлектронные системы связи космических аппаратов: учеб. пособие для студентов инженерно-технических специальностей. – Томск: ТУСУР, 2024. – 111 с. [Электронный ресурс]. – URL: https://edu.tusur.ru/publications/10874 (дата обращения: 12.03.2025).

УДК 621.396.946

ПРОЕКТИРОВАНИЕ ВЫСОКОСКОРОСТНОЙ СИСТЕМЫ МЕЖСПУТНИКОВОЙ СВЯЗИ НА БАЗЕ НОВОГО СТАНДАРТА DVB-S2X ДЛЯ ГРУППЫ КОСМИЧЕСКИХ АППАРАТОВ

М.Е. Ильясов, Е.Д. Морозов, А.В. Зяблицев,
М.А. Кызласов, студенты каф. РТС
Научный руководитель А.М. Голиков, к.т.н., с.н.с., доцент каф. РТС
г. Томск, ТУСУР

Описана реализация математической модели системы DVB-S2X 256APSK, включающая: генерацию, кодирование и модуляцию данных, симуляцию через прохождения данных через канал с шумами, демодуляцию и декодирование на приемной стороне.
Ключевые слова: межспутниковая линия связи, DVB-S2x, LDPC, BCH, бюджет радиолинии, APSK, MatLab, Simulink.

DVB-S2X – это расширение стандарта DVB-S2, предложенное в 2014 г., предназначенное для улучшения эффективности использования спутниковых каналов. Основные улучшения DVB-S2X включают:

1. Новые уровни модуляций и кодирования: 64APSK, 128APSK, 256APSK.

2. Модуляцию для низкого отношения сигнал/шум. Для этого используется BPSK.

3. Усовершенствованную коррекцию ошибок. DVB-S2X продолжает использовать LDPC и BCH. Кодовая скорость может варьировать от 1/4 до 9/10 в зависимости от требований к надежности и пропускной способности.

4. Гибкие коэффициенты ската фильтров: 0.05, 0.10, 0.15. Это позволит сократить избыточную полосу частот и увеличить эффективность использования спектра [1].

Структура LDPS. В стандарте DVB-S2 используют внешнее и внутреннее кодирования. Во втором поколении уже использовались коды Боуза–Чоудхури–Хоквингема (БЧХ) для внешнего, а для внутренней – коды с малой плотностью проверкой на четность (LDPC) – это линейные блочные коды, где проверочные символы добавляются в конце информационного сообщения. LDPC-коды (Low-Density Parity-Check, коды с малой плотностью проверок) – это мощные помехоустойчивые коды, использующие редкие проверочные матрицы для обнаружения и исправления ошибок. В стандарте DVB-S2 проверочная матрица LDPC организована в виде блочного диагонального формата, что позволяет эффективно обрабатывать кадры длиной 64 800 бит (нормальный кадр) или 16 200 бит (короткий кадр) (рис. 1) [3].

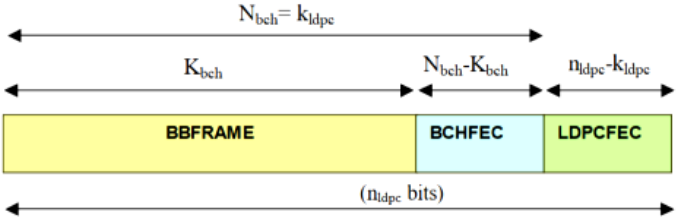

Рис. 1. Структура кадра для длины 64 800 бит

Модель стандарта DVB-S2X. Для моделирования работы стандарта DVB-S2X разработана модель Matlab Simulink (рис. 2). Обеспечивает эмуляцию процесса передачи данных, включая этапы кодирования, модуляции, передачи через канал с шумом и декодирования на приемной стороне.

Разработанная модель позволяет работать с использованием всех доступных кодировок для 256APSK. Модель включает следующие ключевые компоненты:

1. Генерацию данных: используется блок Bernoulli Binary Generator для формирования случайной последовательности данных, представляющей информационный поток.

2. Кодирование данных: блок BCH Encoder выполняет внешнее кодирование BCH для исправления остаточных ошибок; блок LDPC Encoder производит внутреннее кодирование с использованием LDPC, что обеспечивает высокую помехоустойчивость.

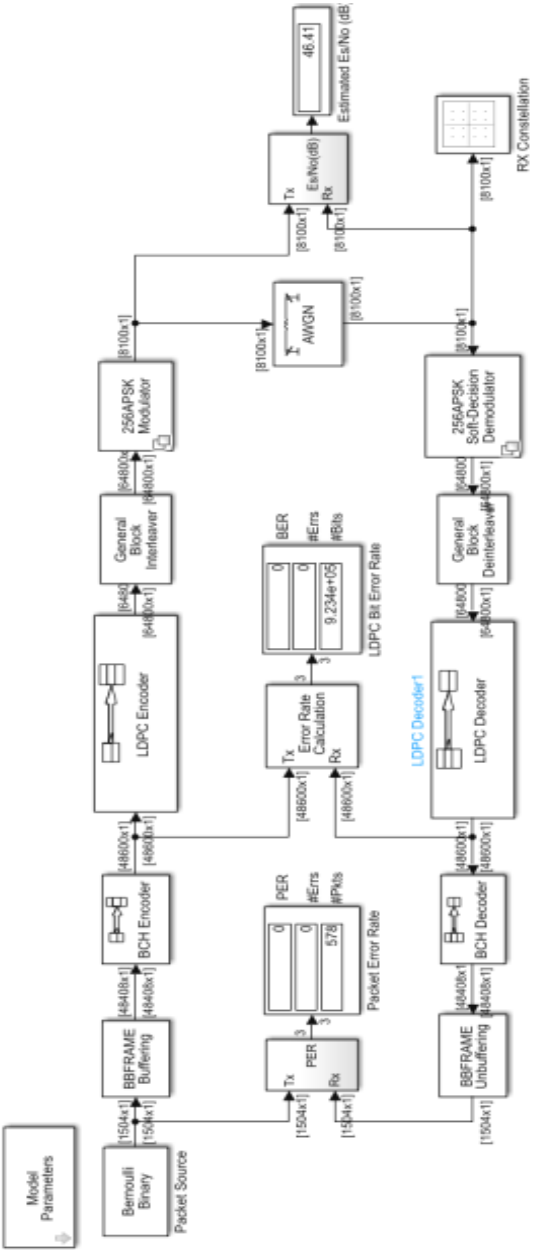

Рис. 2. Модель DVB-S2x

3. Модуляцию сигнала: блок Modulator поддерживает модуляции 256APSK. Для стандартов DVB-S2X реализована поддержка модуляции 256APSK с различными коэффициентами кодирования.

4. Канал передачи: симулируется аддитивный белый гауссов шум (AWGN) с возможностью настройки уровня SNR для оценки производительности системы.

5. Демодуляцию и декодирование: в приемной части происходит обратная демодуляция, LDPC-декодирование и BCH-декодирование для восстановления исходных данных.

На рис. 3 представлен блок параметров системы.

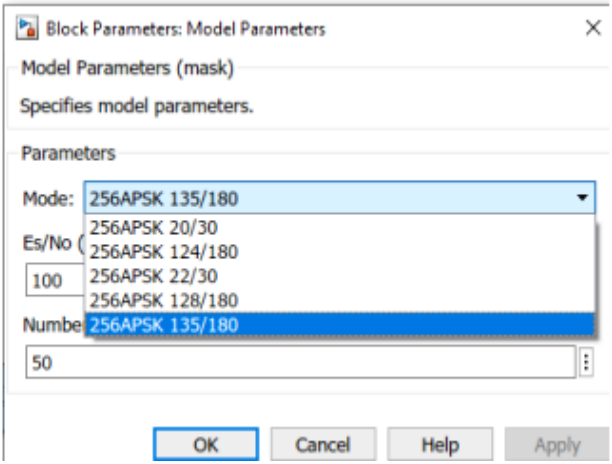

Рис. 3. Блок параметров модели

ЛИТЕРАТУРА

1. Камнев В.Е. Спутниковые сети связи: учеб. пособие. – 2-е изд., доп. / В.Е. Камнев, В.В. Черкасов, Г.В. Чечин. – М.: ООО «Военный парад», 2010. – 608 с.

2. Системы спутниковой связи с эллиптическими орбитами, разнесением ветвей и адаптивной обработкой / Е.Ф. Камнев, А.И. Аболиц, А.А. Акимов, А.С. Белов, В.Ю. Бобков, М.И. Пелехатый. – М.: Глобсатком, 2009. – 724 с.

3. Richardson T. Modern Coding Theory / T. Richardson, R.L. Urbanke. – New York: Cambridge University Press, 2008. – 586 p.

4. Asadi A. A Survey on Device-to-Device Communication in Cellular Networks / A. Asadi, Q. Wang, V. Mancuso // IEEE Communications Surveys & Tutorials. – 2014. –18 p.

5. 5G – не только скорость // Connect WIT. – 2017. – № 1-2.

6. Кргузов Р.Ю. Предложения в концепцию создания перспективной НССС / Р.Ю. Кргузов, В.В. Голоков, А.В. Черноусов. – Железногорск, 2024. – 614 с.

7. Регламент радиосвязи: статьи. – Женева, 2020. – 442 с.
8. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. – 2-е изд., испр. / Пер. с англ. – М.: Вильямс, 2017. – 1100 с.

УДК 621.396.946

ПАТЧ-АНТЕННАЯ СИСТЕМА MIMO ДЛЯ КОСМИЧЕСКОГО АППАРАТА

Е.Д. Морозов, М.Е. Ильясов, А.В. Зяблицев, М.А. Кызласов, студенты каф. РТС

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

г. Томск, ТУСУР

Описана реализация математической модели патч-антенны в двухполяризационном исполнении. Приведены 3D-модель антенны, а также частотные характеристики коэффициентов передачи и отражения.

Ключевые слова: коэффициент отражения, патч-антенна, двухполяризационная антенна, MIMO.

MIMO – это технология, которая применяется в беспроводной связи с использованием нескольких передающих и приёмных антенн. Передатчик и приёмник оборудованы несколькими антеннами, которые могут передавать или принимать несколько потоков данных в один момент времени.

За счёт использования нескольких антенн одновременно технология MIMO позволяет увеличить скорость передачи данных и пропускную способность системы. Также передача данных становится более надежной, так как уменьшается влияние помех и интерференции.

Технология MIMO за счет наличия нескольких путей распространения сигнала позволяет бороться с многолучевостью и повышать производительность беспроводной связи. Многолучевость возникает, когда радиосигналы приходят к приемнику через разные пути, отражаясь от препятствий, зданий, поверхностей и других объектов [1, 2].

Функциональная схема антенной системы MIMO. Применение технологий MIMO позволяет обеспечить пердачу данных с более высокими сокоростями между передатчиком и приемником посредством увеличения пространственного временного, частотного кодирования и (или) формирования лучей. Повышение скорости передачи обеспечивается при применении мультиплексирования, например пространственного. Схематично система MIMO изображена на рис. 1.

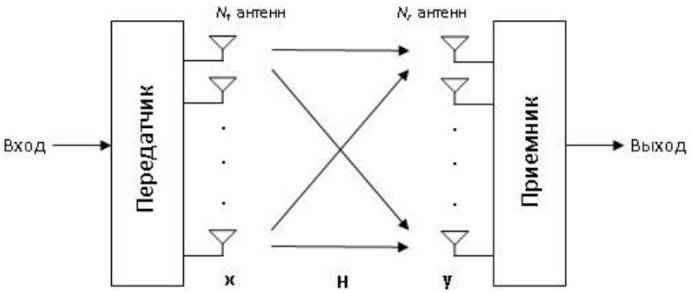

Рис. 1. Структура системы MIMO

Применение иного вида разделения каналов, например использование двухполяризационных антенн, позволяет увеличить скорость передачи данных. Применение двухполяризационных антенн позволяет формировать любой вид поляризации в зависимости от способа их подключения.

Разработка модели двухполяризационной антенны. На рис. 2 представлена 3D-модель двухполяризационной патч-антенны с изображением объёмной диаграммы направленности.

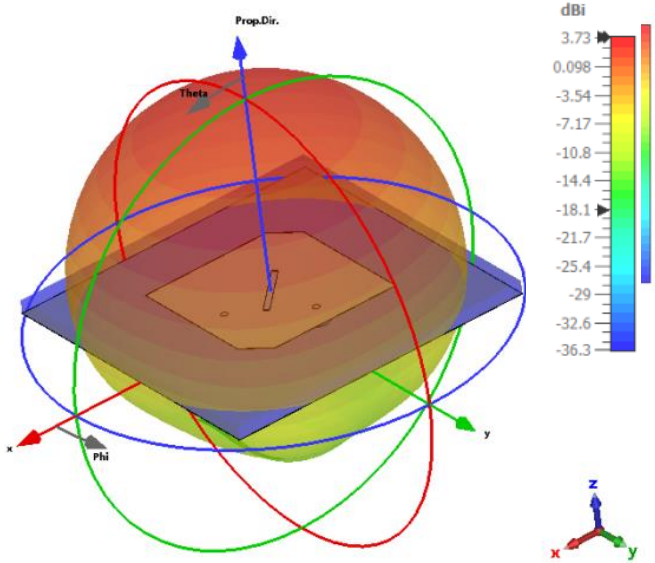

Рис. 2. Объёмное изображение двухполяризационной патч-антенны

На рис. 3 изображены частотные характеристики параметров S11 и S21 соответственно.

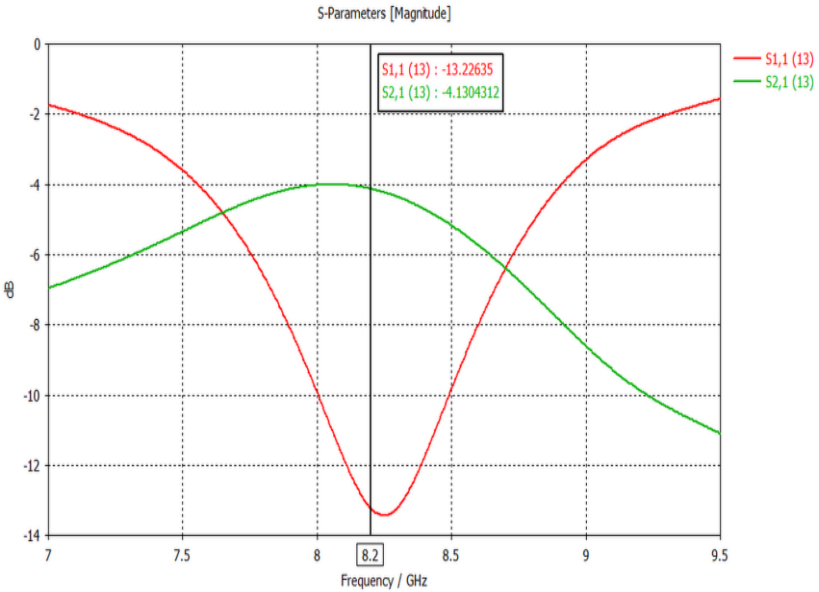

Рис. 3. S-параметры двухполяризационной антенны

По полученным графикам можно сделать вывод, что S-параметры двухполяризационной патч-антенны имеют аналогичные значения, как у патч-антенны с линейной поляризацией [3], однако главным её преимуществом является зависимость выходной поляризации от разности фаз сигналов на входе антенны, что позволяет увеличить скорость передачи данных в системе MIMO.

ЛИТЕРАТУРА

1. Передатчик X-диапазона SXC-XTX-0. [Электронный ресурс]. – Режим доступа: https://sputnix.ru/ru/platformyi/cubesat-platformy/sxc6-adc-as-tff (дата обращения: 10.03.2025).

2. Ермолаев В.Т. Пространственная обработка сигналов MIMO – в системах сотовой связи: учеб. пособие / В.Т. Ермолаев, А.Г. Флаксман, А.В. Елохин, И.С. Сорокин. – Нижний Новгород: Нижегородский гос. ун-т, 2020. – 134 с.

3. Cubesat X-band Transmitter, datasheet [Электронный ресурс]. – Режим доступа: https://www.trade.glavkosmos.com/ru/catalog/spacecraft/telecommandand-telemetry-system/receivers-transmitters/X-band-transmitter-for-Cubesat/ (дата обращения: 23.12.2024).

УДК 621.376

ИССЛЕДОВАНИЕ МЕТОДОВ СВЕРХРАЗРЕШЕНИЯ

В.И. Мошногорский, студент каф. РТС

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

г. Томск, ТУСУР, rts2_golikov@mail.ru

Исследовано несколько перспективных алгоритмов сверхразрешения. Приводится исследование эффективности методов измерения угловых координат со сверхразрешением в зависимости от различного соотношения сигнал/шум на входе приёмника и конфигурации антенной решетки.

Ключевые слова: метод Root MUSIC, сверхразрешение, метод Кейптолна, метод Бартлетта, метод теплового шума.

Исследуемые алгоритмы – это алгоритмы сверхразрешения [1], они должны показывать предел разрешения больший, чем рэлеевский предел. На рис. 1–3 представлены результаты с использованием алгоритмов при максимальном сближении источников сигналов для их разрешения.

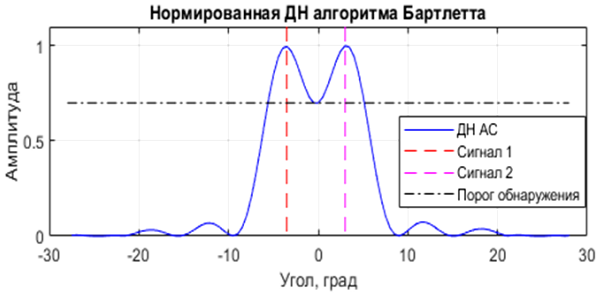

Рис. 1. Нормированная ДН алгоритма Бартлетта
на пределе углового разрешения

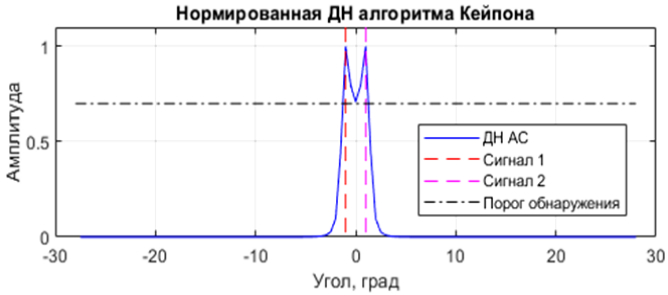

Рис. 2. Нормированная ДН алгоритма Кейпона
на пределе углового разрешения

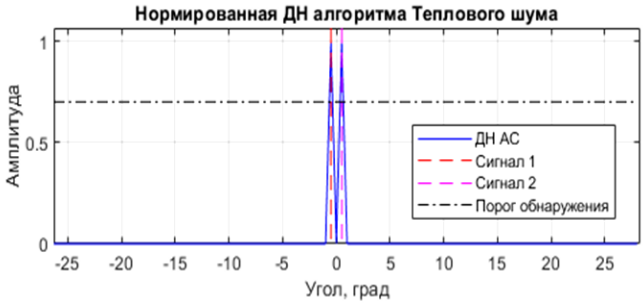

Рис. 3. Нормированная ДН алгоритма теплового шума на пределе углового разрешения

По итогам исследования наименее эффективным оказался метод Бартлетта, так как он показал наихудший предел углового разрешения источников сигналов. Наиболее эффективные оказались методы Кейпона и теплового шума, так как они показали наименьшие пределы углового разрешения источников сигналов.

ЛИТЕРАТУРА

1. Ильчук А.Р. Угловое сверхразрешение в бортовых радиолокационных системах воздушного базирования / А.Р. Ильчук, Ю.Д. Каргашин, В.И. Меркулов, В.С. Чернов // Журнал радиоэлектроники (электронный журнал). – Институт радиотехники и радиоэлектроники РАН. – 2021. – № 12. – 40 с. https://driorg/10.30898/1684-1719.12.3.

УДК 621.376.6

СИСТЕМА ПРОСТРАНСТВЕННО-ВРЕМЕННОГО КОДИРОВАНИЯ MIMO ДЛЯ КОСМИЧЕСКИХ АППАРАТОВ

Д.Н. Мишин, М.В. Изупов, студенты каф. РТС

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

г. Томск, ТУСУР, rts2_golikov@mail.ru

Разрабатывается система пространственно-временного кодирования MIMO для космических аппаратов, что представляет собой значительный шаг вперед в области улучшения связи и передачи данных в космосе. Предложены алгоритмы, основанные на технологии MIMO, для повышения эффективности и надежности передачи данных. Проведено моделирование и проанализирована производительность системы. Показана эффективность использования MIMO в космических коммуникациях.

Ключевые слова: MIMO, пространственно-временное кодирование, космическая связь, передача данных, космический аппарат.

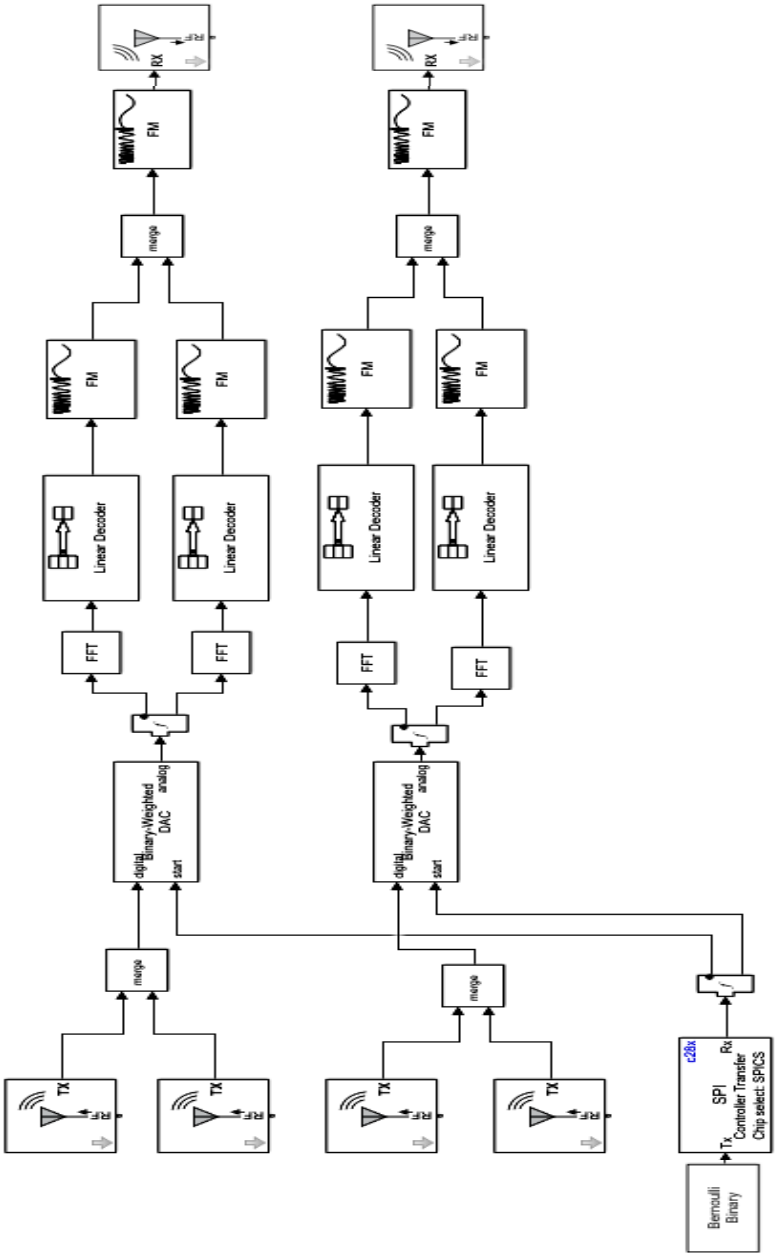

Рис. 1. Simulink-модель приёмника с использованием технологии

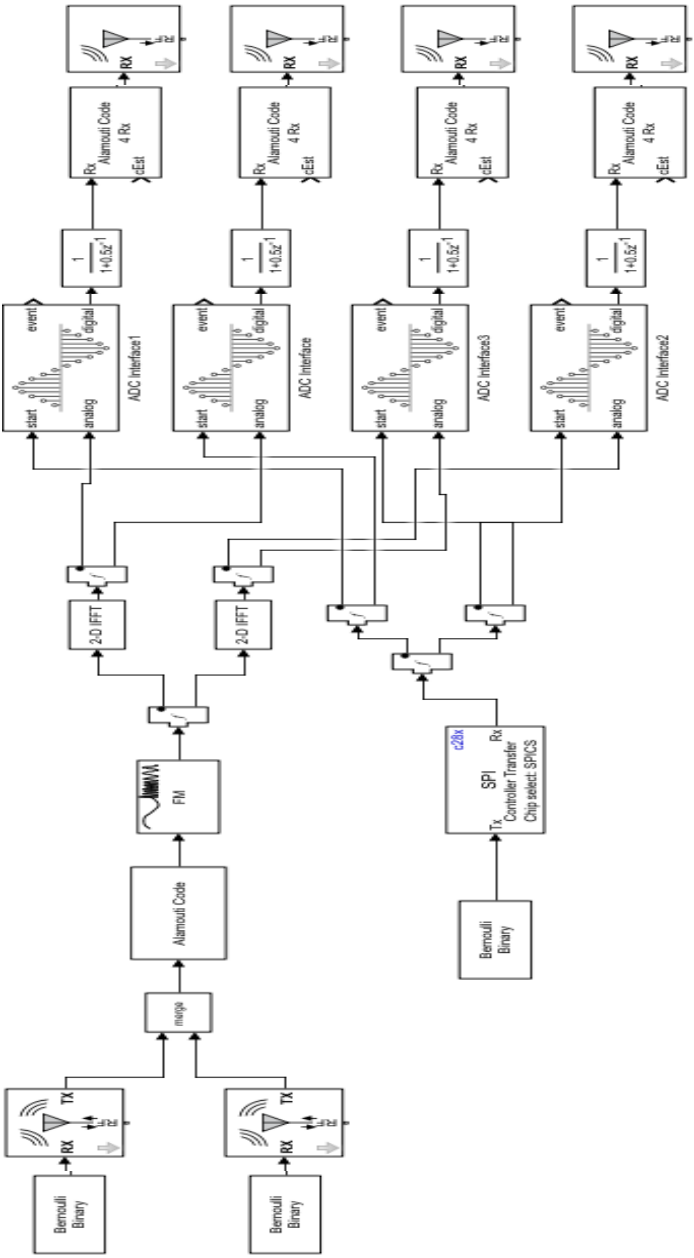

Рис. 2. Simulink модель передатчика с использованием технологии

Технология MIMO (Multiple Input Multiple Output) позволяет использовать несколько антенн на передатчике и приемнике для улучшения качества связи. Это достигается за счет пространственного разделения сигналов и временного кодирования. Модель приемника системы MIMO представлена на рис. 1.

Существует несколько различных схем пространственно-временного кодирования, каждая из которых имеет свои преимущества и недостатки. В данной работе рассматриваются наиболее эффективные схемы, такие как Alamouti и Space-Time Block Codes (STBC). Важно выбрать оптимальную схему для конкретных условий эксплуатации, чтобы обеспечить наилучшее соотношение между производительностью и ресурсоемкостью.

Модель передатчика системы MIMO представлена на рис. 2.

По мере моделирования были получены следующие метрики:

- BER (Bit Error Rate) – вероятность ошибки на бит, показывающая, сколько битов было передано с ошибками.
- PER (Packet Error Rate) – вероятность ошибки на пакет, показывающая, сколько пакетов данных было передано с ошибками.
- Спектральная эффективность – показатель, характеризующий эффективность использования частотного спектра.
- Пропускная способность – максимальная скорость передачи данных в системе.

Проведено исследование производительности системы MIMO в зависимости от различных схем кодирования.

Данное исследование позволяет сделать обоснованные выводы о том, какие схемы пространственно-временного кодирования MIMO будут наиболее эффективными для космических коммуникаций, а также как повысить надежность и производительность системы передачи данных.

ЛИТЕРАТУРА

1. Голиков А.М. Системы цифровой радиосвязи: учеб. – М.: Ай Пи Ар Медиа, 2022. – 340 с. [Электронный ресурс]. – URL: https://doi.org/10.23682/117865 (дата обращения: 03.03.2025).

УДК 621.396.946

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПАТЧ-АНТЕННОЙ СИСТЕМЫ MIMO ДЛЯ КОСМИЧЕСКИХ АППАРАТОВ

Д.В. Иванов, студент каф. РТС

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

г. Томск, ТУСУР

Описана реализация математической модели патч-антенны в двухполяризационном исполнении. Приведены 3D-модель антенны, а также частотные характеристики коэффициентов передачи и отражения.

Ключевые слова: коэффициент отражения, патч-антенна, двухполяризационная антенна, MIMO 4×4.

Технология MIMO применяется в беспроводной связи с и пользованием нескольких передающих и приёмных антенн, которые могут передавать или принимать несколько потоков данных в один момент времени. MIMO позволяет увеличить скорость передачи данных и пропускную способность системы за счёт использования нескольких антенн одновременно. Передача данных становится более надежной, так как уменьшается влияние интерференции и помех.

Разработаны модели двухполяризационной антенны**.** На рис. 1 представлена 3D-модель двухполяризационной патч-антенны

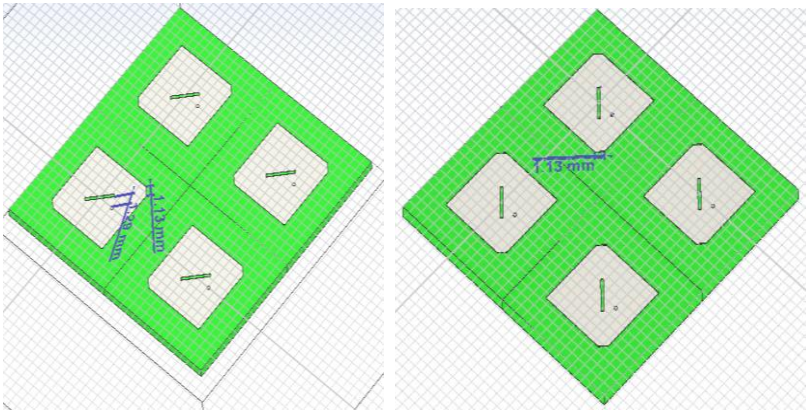

Рис. 1. Патч-антенна 4×4 для правой и левой круговой поляризации

На рис. 2 изображена частотная характеристика патч-антенной системы. Видно, что полосы частот более 500 МГц.

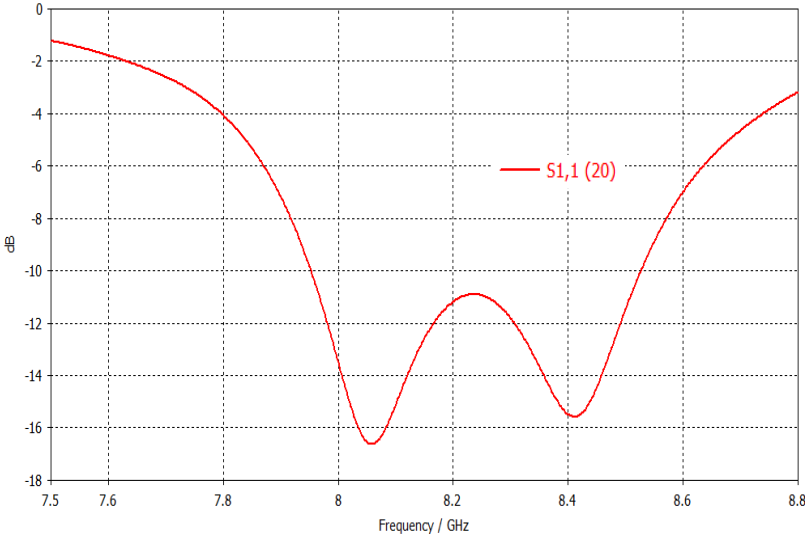

Рис. 2. S-параметры двухполяризационной антенны

По полученным графикам можно сделать вывод, что S-параметры двухполяризационной патч-антенны имеют аналогичные значения, что у патч-антенны с линейной поляризацией [1–3], однако главным её преимуществом является зависимость выходной поляризации от разности фаз сигналов на входе антенны, что позволяет увеличить скорость передачи данных в системе MIMO.

ЛИТЕРАТУРА

1. Передатчик X-диапазона SXC-XTX-0 [Электронный ресурс]. – Режим доступа: https://sputnix.ru/ru/platformyi/cubesat-platformy/sxc6-adc-as-tff (дата обращения: 10.03.2025).

2. Ермолаев В.Т. Пространственная обработка сигналов MIMO в системах сотовой связи: учеб. пособие / В.Т. Ермолаев, А.Г. Флаксман, А.В. Елохин, И.С. Сорокин. – Нижний Новгород: Нижегород. гос. ун-т, 2020. – 134 с.

3. Cubesat X-band Transmitter, datasheet [Электронный ресурс]. – Режим доступа:https://www.trade.glavkosmos.com/ru/catalog/spacecraft/telecommandand-telemetry-system/receivers-transmitters/X-band-transmitter-for-Cubesat/ (дата обращения: 23.12.2024).

УДК 621.396.623

АЛГОРИТМ ОПРЕДЕЛЕНИЯ НАПРАВЛЕНИЯ ПОМЕХИ С ИСПОЛЬЗОВАНИЕМ АДАПТИВНОЙ АНТЕННОЙ РЕШЕТКИ И ПЛИС

К.Н. Следевский, оператор роты (научной);
Ю.А. Кудрявцева, младший научный сотрудник НИЦ;
П.Н. Федоров, с.н.с. НИО-4 НИЦ, к.т.н.
г. Санкт-Петербург, Военная орденов Жукова и Ленина Краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного МО РФ, sledevskiykn@mail.ru

Рассматривается алгоритм определения направления помехи для адаптивной антенной решетки (ААР) с использованием программируемой логической интегральной схемы (ПЛИС). Представленный алгоритм позволяет вычислять вектор весовых коэффициентов для формирования диаграммы направленности антенной решетки, что способствует эффективному подавлению направленных помех. Для реализации предложенного метода используется сочетание языков Verilog и C++, что позволяет оптимизировать быстродействие системы. Применение данного подхода повышает точность и скорость обработки входных сигналов, обеспечивая более надежную работу адаптивных антенных систем в условиях радиоэлектронного противодействия.

Ключевые слова: адаптивная антенная решетка, ПЛИС, направленная помеха, диаграмма направленности.

С каждым годом с учетом увеличения количества беспилотных летательных аппаратов (БПЛА) повышается потребность в их бесперебойной связи с оператором. Одной из главных причин, которые влияют на качество принятого сигнала, является наличие помех, сформированных средствами радиоэлектронной борьбы (РЭБ). Для подавления помех и выделения полезного сигнала, предлагается использовать описанный в данной статье алгоритм, который будет являться основой работы адаптивной антенной решетки.

В основе проекционного алгоритма обработки сигналов предполагается использовать выражение, которое необходимо для расчета вектора весовых коэффициентов на k+1 шаге:

$$Y_k = \mathbf{X}_k + \mathbf{W}_k \;\; \mathbf{W}_{k+1} = \mathbf{W}_k + \mu \cdot P_{y(k)}((\mathbf{X}_k - \mathbf{W}_k) \cdot Y_k), \qquad (1)$$

где $\mathbf{X}_k$ – вектор входных сигналов на входах антенного элемента (АЭ); $P_y(k)$ – проектор; $Y_k = \mathbf{X}_k + \mathbf{W}_k$ – сигнал на выходе общего сумматора ААР; μ – коэффициент усиления инвертирующих усилителей; $\mathbf{W}_k$ – вектор весовых коэффициентов.

Полученные весовые коэффициенты позволяют сформировать требуемую диаграмму направленности антенной решетки. Для вычисления данных коэффициентов необходимо знать набег разности фаз сигналов между АЭ относительно главного, у которого данный коэффициент будет принят за единицу. Для четырехэлементной антенной решетки вектор принимаемого сигнала будет иметь вид следующей матрицы:

$$\mathbf{V}_C = [1;\ e^{jfc}; e^{2jfc}; e^{3jfc}]. \qquad (2)$$

Знание фазы полезного сигнала позволит определить направление его прихода. Подобным же вектором можно описать и направление прихода помехи для формирования ДН, которая позволит её подавить.

Фаза сигнала, приходящего на АЭ, может быть определена благодаря использованию амплитудных и фазовых датчиков, которые позволят сформировать вектор сигналов, представленный в формуле (2). После чего сигнал поступает на умножители, в которых к полученному сигналу добавляется весовой коэффициент. В первой итерации данные коэффициенты для всех линий для простоты решения примем равными единице. После блока умножения сигналы суммируются и поступают на вход приемника, а также на процессор для вычисления отношения сигнал/помеха/шум (ОСПШ). Данный алгоритм представлена на рис. 1.

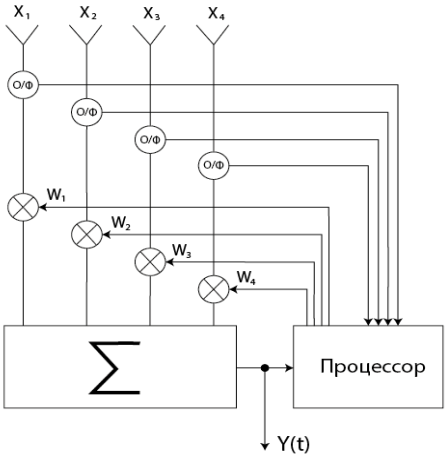

Рис. 1. Схема работы ААР

Исходя из особенностей построения программ для ПЛИС, часть алгоритма будет реализована с использованием языка описания архи-

тектуры Verilog, а часть – с использованием привычного языка программирования – C++. Для получения максимального быстродействия и отклика процессорной части ПЛИС определитель фазы и сумматор необходимо реализовать на языке Verilog, когда как добавление весового коэффициента, которое не требует такого быстродействия, реализуется на C++.

Данный алгоритм с учетом реализации некоторых блоков при помощи языка описания аппаратуры на ПЛИС позволит увеличить скорость обработки входного сигнала до практически мгновенных значений, а также получать диаграмму направленности антенной решетки, приближенную к идеальным значениям.

ЛИТЕРАТУРА

1. Харрис Д.М. Цифровая схемотехника и архитектура компьютера / Д.М. Харрис, С.Л. Харрис. – М.: ДМК-Пресс, 2018. – 221 с.

УДК 621.396

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФИЛЬТРОВ С КОНЕЧНОЙ ИМПУЛЬСНОЙ ХАРАКТЕРИСТИКОЙ ДЛЯ ПОДАВЛЕНИЯ ПОМЕХ

О.А. Рожкова, курсант

Научный руководитель А.В. Лубенцов, проф. каф. ОРЭ, к.геогр.н., доцент

г. Воронеж, ВИ ФСИН России, lubensov@mail.ru, alesya300704gmail.com

Приводится сравнительная характеристика различных типов фильтров с конечной импульсной характеристикой. Выделяются главные отличительные черты, преимущества и недостатки. В результате анализа делаются выводы по применимости каждого типа фильтров.

Ключевые слова: цифровая обработка сигналов, цифровой фильтр, фильтр с конечной импульсной характеристикой, КИХ-фильтр.

В век цифровизации активно используется цифровая обработка сигналов (ЦОС). ЦОС представляет собой область электроники, исследующей вопрос представления аналогового сигнала в дискретной форме. Одна из основных проблем данной сферы – это влияние нежелательных искажений на полезный сигнал. В результате воздействия помех снижаются качество и точность сигнала. Необходимо использовать эффективные меры противодействия искажениям. При правильном использовании данных мер повышается достоверность результатов, улучшается качество сигнала, повышается надежность систем, а также упрощается последующая обработка.

Сравнительный анализ фильтров. В качестве мер подавления помех цифровых сигналов широкое распространение получили фильтры с конечной импульсной характеристикой (КИХ-фильтры).

Целью нашего исследования является проведение структурного анализа различных типов КИХ-фильтров для подавления помех, определение их эффективности, преимуществ и недостатков.

Н.Б. Лиджиева выделяет 2 метода проектирования КИХ-фильтров: метод «взвешивания» и метод частотной выборки [1]. Рассмотрим каждый из них.

Метод «взвешивания», или метод «временных окон» стал одним из самых часто используемых методов синтеза фильтров с конечной импульсной характеристикой. Основанный на усечении бесконечно длинной импульсной характеристики, метод позволяет получить конечную последовательность отсчетов, представляющую импульсную характеристику фильтра.

Метод взвешивания для проектирования КИХ-фильтра включает три этапа:

1) определение желаемой комплексной частотной характеристики;

2) обратное дискретное преобразование Фурье (ОДПФ) для получения бесконечной импульсной характеристики;

3) применение функции окна для усечения импульсной характеристики и получения конечной импульсной характеристики с заданными характеристиками частотной области.

Кратко назовем преимущества и недостатки данного метода.

Преимущества: алгоритмическая простота; различные оконные функции (например, прямоугольное окно, окно Ханна, окно Блэкмана) предлагают компромисс между шириной переходной полосы и уровнем боковых лепестков; линейная фазовая характеристика.

Недостатки: не минимизирует ширину переходной полосы и уровень боковых лепестков, а лишь приближает к идеальной частотной характеристике; точность приближения ограничена формой выбранного окна (риск возникновения гиббсовских колебаний); зависимость от длины фильтра: чем уже переходная полоса, тем длиннее фильтр (увеличиваются вычислительная сложность и задержка); ограничен формой переходной полосы, задаваемой выбранной оконной функцией.

Области применения КИХ-фильтров, разработанных методом взвешивания, включают те объекты, где требуется не слишком высокая точность, а важна скорость проектирования и простота реализации. Данный метод редко используется для проектирования высококачественных фильтров с узкими переходными полосами и строгими требованиями к подавлению боковых лепестков.

Метод частотной выборки, или метод частотного отклика, а также метод идеального частотного отклика, заключается в прямом задании требуемого частотного отклика в дискретных точках частоты и использовании ОДПФ для получения частотной характеристики, полученной путем дискретизации по частоте заданной частотной характеристики.

А.С. Глинченко отмечает, что точность приближения определяется количеством и значениями выборок частотной характеристики в переходной зоне, а более плавная аппроксимируемая функция достигается за счет увеличения числа выборок с соответствующим выбором их значений [2].

Отличительной чертой рассматриваемых фильтров является использование итеративных алгоритмов оптимизации (например, алгоритм Парка–Макклеллана). Благодаря данному преимуществу происходит поиск оптимальных коэффициентов. В результате снижается отклонение от заданной частотной характеристики и увеличивается точность приближения.

Метод частотного отклика используется преимущественно в областях, требующих высокой точности, однако требует больших вычислительных ресурсов за счет более высокого порядка в сравнении с предыдущим методом.

Заключение. В результате системного анализа мы пришли к выводу, что КИХ-фильтры, основанные на методах «взвешивания» и частотной выборки, – фильтры, которые способны справиться с поставленной задачей – подавление помех цифрового сигнала. Однако имеют свои достоинства и недостатки. Кратко можно обозначить, что метод «взвешивания» – это более простой и быстрый способ подавления помех, однако менее точный и менее контролируемый по сравнению с методом частотной выборки. Метод частотной выборки является хоть и более точным, но требует больших вычислительных затрат. Следовательно, выбор конкретного метода построения фильтра с конечной импульсной характеристикой зависит от компромисса между необходимой точностью и имеющимися вычислительными ресурсами.

ЛИТЕРАТУРА

1. Лиджиева Н.Б. Методика проектирования цифровых КИХ-фильтров средствами пакета MathCad // Вестник МГУП. – 2011. – № 11. – URL: https://cyberleninka.ru/article/n/metodika-proektirovaniya-tsifrovyh-kih-filtrov-sredstvami-paketa-mathcad (дата обращения: 03.03.2025).

2. Глинченко А.С. Цифровая обработка сигналов. Версия 1.0: курс лекций. – Красноярск: ИПК СФУ, 2008 [Электронный ресурс]. – URL: http://optic.cs.nstu.ru/files/Lit/Image/u_lectures.pdf (дата обращения: 03.03.2025).

3. Лубенцов А.В. Модель трансформации и оптимизации видеопотока как составной части комплексной системы безопасности // Промышленные АСУ и контроллеры: Информационная безопасность. – 2023. – № 1. – С. 34–41.

4. Лубенцов А.В. Системный анализ модели описания радиотехнических сигналов сплайнами в закрытых информационных сетях комплексных систем безопасности // Правовая информатика. – 2024. – № 2. – С. 72–81.

УДК 621.396.96

ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ ОБЪЕКТА С ПОМОЩЬЮ ТЕХНОЛОГИИ SDR

М.Ю. Самков, старший оператор роты (научной);
Ю.А. Кудрявцева, м.н.с.; П.В. Воробьев, м.н.с.
Научный руководитель Д.Ф. Ткачев, к.т.н., нач. науч.-исслед. отд.
г. Санкт-Петербург, Военная орденов Жукова и Ленина
Краснознаменная академия связи им. Маршала Советского Союза
С.М. Буденного МО РФ, samkov.misha@mail.ru

Изучены вопросы защиты автоматизированных систем управления технологическими процессами (АСУ ТП) от кибератак посредством фильтрации трафика промышленных протоколов. В условиях растущей цифровизации и подключения АСУ ТП к сети Интернет, их уязвимость увеличивается, что делает необходимым применение эффективных методов защиты. Рассматриваются основные уязвимости промышленных протоколов, таких как отсутствие шифрования и неэффективные механизмы аутентификации. Описываются ключевые функции фильтрации трафика, включая мониторинг трафика, фильтрацию по IP-адресам, фильтрацию по протоколам и анализ поведения пользователей и устройств. Каждая функция детализируется с точки зрения технических процессов, что подчеркивает их важность для обеспечения безопасности АСУ ТП и предотвращения несанкционированного доступа.

Ключевые слова: АСУ, кибератаки, фильтрация, безопасность.

Программно-определяемое радио (SDR) изменило подход к обработке радиосигналов, сделав технологии, ранее доступные только военным или крупным корпорациям, доступными для энтузиастов и инженеров [1]. Одной из ключевых задач, решаемых с помощью SDR, является локализация объектов – от поиска дронов до обнаружения источников помех. Рассматриваются методы определения местоположения, такие как время прихода сигнала (ToA), триангуляция и разность времени прихода (TDoA), а также показана их реализация на практике с использованием бюджетного SDR-оборудования.

Основы технологии SDR. SDR (Software-Defined Radio) – это радиосистема, где традиционные аппаратные компоненты (фильтры, модуляторы) заменены программными алгоритмами. Устройства вроде RTL-SDR HackRF и USRP позволяют принимать и анализировать сигналы в диапазоне от 24 МГц до 6 ГГц, что делает их идеальными для экспериментов [1].

Преимущества SDR для локализации:

1. Гибкость: перенастройка частоты и параметров сигнала через ПО.
2. Доступность: низкая стоимость оборудования.
3. Широкий охват: работа с Wi-Fi, ADS-B, LoRa и другими протоколами.

Методы локализации. Существует несколько методов локализации, некоторые из них представлены ниже:

1. Время прихода сигнала (ToA). Расстояние до объекта вычисляется по формуле $d = c \times t$, где c – скорость света (3×10^8 м/с), t – время задержки между отправкой и приёмом сигнала.

Если радиомаяк передаёт сигнал с меткой времени $t_{\text{отправки}}$, приёмник фиксирует $t_{\text{приёма}}$. Разница $t = t_{\text{приёма}} - t_{\text{отправки}}$ позволяет вычислить расстояние d [2].

2. Триангуляция. Местоположение объекта определяется как точка пересечения направлений, измеренных из двух или более точек с известными координатами [3].

Для приёмников с координатами (x_1, y_1) и (x_2, y_2), направляющих сигнал под углами Q_1 и Q_2, необходимо решить следующую систему:

$$\begin{cases} x = x_1 + d_1 \times \cos(Q_1), \\ y = y_1 + d_1 \times \sin(Q_1), \\ x = x_2 + d_2 \cdot \cos(Q_2), \\ y = y_2 + d_2 \cdot \sin(Q_2), \end{cases}$$

где d_1, d_2 – расстояния, вычисленные через ToA или RSSI (мощность сигнала).

3. Разность времени прихода (TDoA). Несколько синхронизированных приёмников фиксируют сигнал. Разница во времени прихода (Δt) позволяет вычислить координаты через гиперболические уравнения

$$\Delta t_{ij} = \frac{d_i - d_j}{c},$$

где где d_i, d_j – расстояния от объекта до i-го и j-го приёмников.

Практическая реализация: поиск источника сигнала. Для поиска сигнала необходимо разместить два SDR в точках с известными координатами (например, на расстоянии 100 м друг от друга) и синхронизировать на них время.

Далее подключаемся к SDR-устройству, настраиваем его на частоту 433 МГц (рис. 1) с частотой дискретизации 2,4 МГц, захватываем и сохраняем сигнал.

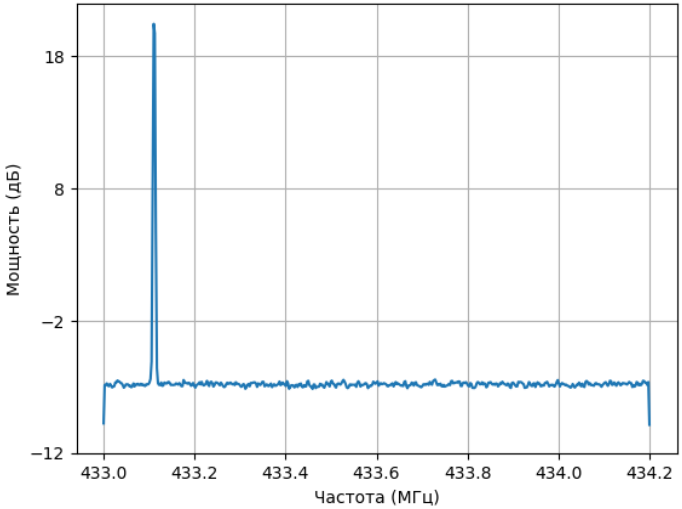

Рис. 1. Настройка SDR-устройства на частоту 433 МГц

При настройке оборудования могут возникнуть следующие проблемы:

1. Неправильная синхронизация времени.
2. Появление погрешности измерений.
3. Многолучевость.

Для решения системы уравнений триангуляции используется метод меньших квадратов. Решение системы в Python показано на рис. 2.

После строится карта с координатами источника, на которой отображаются два приемника и источник сигнала (рис. 3).

На графике показаны позиции двух приёмников (красная и синяя точки) и найденный источник сигнала (зелёная точка).

Заключение. Технология SDR позволяет реализовать сложные методы локализации, такие как TDoA, ToA и триангуляция, даже на бюджетном оборудовании. Комбинируя направленные антенны, синхронизацию и алгоритмы обработки сигналов, можно находить дроны, обнаруживать помехи или искать радиомаяки.

```python
import numpy as np

# Координаты приёмников
rx1 = (0, 0)
rx2 = (100, 0)

# Измеренные углы (в радианах)
theta1 = np.deg2rad(45)
theta2 = np.deg2rad(135)

# Решение системы
x = (-100 * np.tan(theta2)) / (np.tan(theta1) - np.tan(theta2))
y = x * np.tan(theta1)

print(f"Координаты источника: ({x}, {y})")
```

```
Координаты источника: (50.0, 50.0)
```

Рис. 2. Решение системы уравнений триангуляции в Python

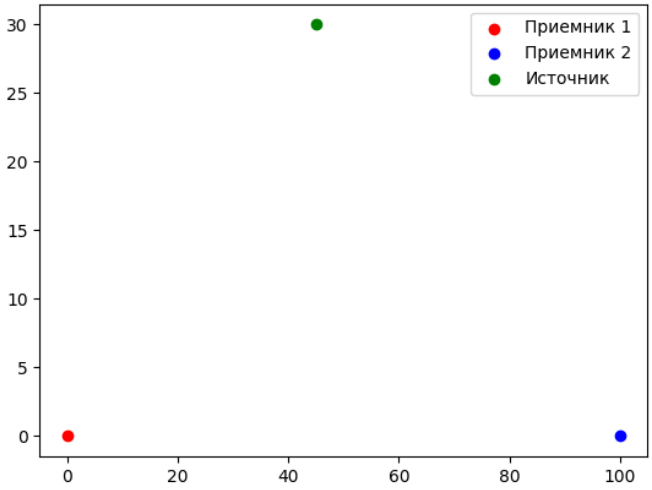

Рис. 3. Карта с координат источника

ЛИТЕРАТУРА

1. Голдберг О.Д. Программно-определяемые радиосистемы: принципы и приложения. – М.: Техносфера, 2018.

2. Калинин В.И. Локационные системы: теория и практика. – М.: Радиотехника, 2017.

3. Луценко Е.В. Алгоритмы триангуляции в радиолокации. – Киев: Наукова думка, 2016.

4. Петров А.В. RTL-SDR: Практическое руководство. – СПб.: БХВ-Петербург, 2020.

5. Григорьев А.С. Методы TDoA и ToA в локации. – СПб.: Лань, 2022.

ПОДСЕКЦИЯ 4.3

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

*Председатель – **Шелупанова П.А.**, зав. каф. ЭБ, к.э.н., доцент;*
*зам. председателя – **Колтайс А.С.**, преп. каф. ЭБ*

УДК 004.056.5

БЕЗОПАСНОСТЬ УДАЛЁННОЙ РАБОТЫ: КЛЮЧЕВЫЕ АСПЕКТЫ ЗАЩИТЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

С.П. Боброва, Р.В. Солоха, Д.В. Старосельцева, С.М. Машковская, студенты 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, bobrovaaaq@gmail.com

Описаны ключевые аспекты обеспечения информационной безопасности в условиях роста популярности удалённой работы, особенно актуального в контексте цифровой трансформации трудовых процессов. Подчёркивается необходимость комплексного подхода, сочетающего технологические решения с повышением цифровой грамотности персонала.
Ключевые слова: удалённая работа, информационная безопасность, защита данных, кибератака.

Сегодня основная часть рабочих инструментов существует в цифровом пространстве. Для обеспечения постоянного доступа к ним необходимо предотвратить риски, связанные с нарушением безопасности.

Согласно данным Forbes переход на удалённую работу в России претерпел значительные изменения в последние годы. Во время пандемии COVID-19 в 2020 г. доля дистанционных работников увеличилась с 2 до 16%.

Однако после снятия ограничений наблюдалось снижение числа удалённых сотрудников. К концу 2023 г. около 1 млн россиян, или чуть более 1% от всех занятых, продолжали работать удалённо.

В 2023 г. 6,7% вакансий в России предусматривали удалённый режим работы, что превысило уровень 2021 г., когда этот показатель

составлял 5,7%. Особенно популярна удалённая работа в сфере ИТ, где каждый восьмой сотрудник работает дистанционно [1].

Эти примеры наглядно демонстрируют, что несмотря на снижение числа удалённых сотрудников после пандемии, интерес к удалённой работе остаётся высоким, особенно в определённых отраслях.

Удаленная (дистанционная) работа – работа вне места нахождения работодателя, в том числе не на территории его подразделения. В соответствии с российским трудовым законодательством понятия «удаленная» и «дистанционная» работа равнозначны.

Компании для обеспечения непрерывного и защищенного доступа сотрудников к рабочим инструментам стали выдвигать новые требования по безопасности.

При проведении анализа безопасности удалённой работы необходимо учитывать несколько ключевых аспектов.

1. Защита данных и конфиденциальность.

Для обеспечения безопасного хранения и передачи данных работодателям и сотрудникам необходимо использовать защищённые VPN-соединения, двухфакторную аутентификацию и зашифрованные хранилища.

2. Контроль доступа и учетные записи.

Одним из рисков удалённой работы является возможность компрометации учетных записей. Использование сложных паролей, управление правами доступа и регулярное обновление учетных данных помогают минимизировать этот риск.

3. Осведомленность сотрудников.

Дистанционные сотрудники более подвержены воздействию фишинговых атак и вредоносных программ. Необходимо проводить регулярное обучение сотрудников по информационной безопасности и применять антивирусные решения. Многие кибератаки связаны с манипуляцией сотрудниками. Обучение персонала принципам цифровой гигиены и внедрение механизмов выявления мошеннических действий позволят снизить риски.

4. Безопасность рабочих устройств.

При удалённой работе часто используются личные устройства, что может привести к утечке корпоративных данных. Важно внедрять политики безопасности и использовать корпоративные инструменты управления устройствами.

5. Организация резервного копирования.

Потеря данных из-за сбоев, атак или человеческих ошибок может привести к значительным убыткам. Регулярное резервное копирование информации и использование облачных решений помогут избежать таких ситуаций [2, 3].

Таким образом, в условиях активной цифровой трансформации и роста популярности удалённой работы вопросы информационной безопасности выходят на первый план. Эффективная защита данных невозможна без комплексного подхода, включающего как технические меры – VPN, двухфакторную аутентификацию, контроль доступа и резервное копирование, так и повышение цифровой грамотности сотрудников. Компании, внедряющие политику безопасности и инвестирующие в обучение персонала, получают устойчивое преимущество в условиях современной модели труда.

ЛИТЕРАТУРА

1. Распространенность удаленной работы в России вернулась к допандемийному уровню [Электронный ресурс]. – URL: https://www.forbes.ru/biznes/520721-rasprostranennost-udalennoj-raboty-v-rossii-vernulas-k-dopandemijnomu-urovnu (дата обращения: 02.03.2025).

2. Обзор рекомендаций по безопасной удаленной работе для предприятий критической инфраструктуры и не только [Электронный ресурс]. – URL: https://ics-cert.kaspersky.ru/publications/reports/2020/04/30/secure-remote-work-for-critical-infrastructure/ (дата обращения: 01.03.2025).

3. Как получить все плюсы удаленной работы без ущерба для безопасности [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/mobile-workforce-security/28006/ (дата обращения: 01.03.2025).

УДК 336.148

БЮДЖЕТНЫЙ КОНТРОЛЬ И ЕГО ПРИМЕНЕНИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ СИСТЕМЫ ГОСУДАРСТВЕННОГО ФИНАНСОВОГО КОНТРОЛЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ю.А. Бычкова, студентка каф. ЭБ
г. Томск, ТУСУР, yuliab13@icloud.com
Научный руководитель Е.В. Курашвили, преп. каф. КИБЭВС
г. Томск, ТУСУР, mev1@fb.tusur.ru

Рассмотрены данные проведенных контрольных мероприятий органов внутреннего и внешнего финансового контроля на территории Российской Федерации в условиях цифровизации. На основе полученных данных выявлен ряд проблем, связанный с эффективностью и результативностью контрольных мероприятий.

Ключевые слова: государственный финансовый контроль, контрольные мероприятия, цифровизация, цифровые технологии, финансовые потери.

Согласно Указу Президента РФ от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на период с 2017 по 2030 годы», одной из ключевых целей стратегий информационного общества является рост эффективности государственного управления и развитие экономики страны в целом [1].

Ключевыми причинами цифровизации системы государственного финансового контроля являются: оперативность и прозрачность контрольных мероприятий, контроль совершения бюджетных операций в реальном времени, защита и надежность финансовой информации.

Основой государственного финансового контроля является контроль за использованием бюджетных средств. Внешний государственный контроль за использованием бюджетных средств осуществляет Счетная палата Российской Федерации (Счетная палата РФ). В компетенции Федерального казначейства Российской Федерации (Федеральное казначейство РФ) находится внутренний государственный финансовый контроль.

В течение последних 5 лет наблюдается активная цифровая трансформация осуществления бюджетного контроля в Российской Федерации (таблица).

Результаты контрольных мероприятий Счетной палаты РФ и Федерального казначейства РФ

Период	Проведено контрольных мероприятий, всего	Объем выявленных нарушений	Объем выявленных нарушений	Возврат в бюджет
	ед.	ед.	млрд руб.	%
Счетная палата				
2019	319	4 443	884,6	0,51
2020	334	3 698	355,2	0,46
2021	346	4 253	1 541,4	0,34
2022	338	4 447	885,6	0,96
2023	332	4 849	2 110	1,25
Федеральное казначейство				
2019	5 636	4 142	2 039,4	0,38
2020	3 165	2 126	1 044,2	0,37
2021	5 014	5 040	681,9	0,34
2022	3 096	2 289	624, 5	0,35
2023	3 936	3 438	728,9	0,7

За анализируемый период в Счетной палате РФ внедрены цифровые технологии, которые можно разделить на информационные системы взаимодействия между структурными подразделениями внутри контролирующего органа, аналитические и обрабатывающие инфор-

мацию системы – программы осуществления контрольных мероприятий, а также информационные системы сбора и визуализации данных. Процесс осуществления бюджетного контроля Федеральным казначейством РФ также претерпел цифровую трансформацию путем внедрения системы электронного бюджета, единой информационной системы в сфере закупок, государственной системы управления.

Проведен анализ осуществления Счетной палатой РФ и Федеральным казначейством РФ бюджетного контроля в условиях процесса цифровизации государственного финансового контроля страны за период с 01.01.2019 по 31.12.2023 [2, 3].

В ходе проведения за период с 01.01.2021 по 31.12.2023 анализа деятельности Счетной палаты РФ наблюдается снижение проведенных контрольных мероприятий при одновременном росте выявленных нарушений, что указывает на оперативность и прозрачность осуществления бюджетного контроля с использованием цифровых технологий. Снижение количества контрольных мероприятий и выявленных нарушений Федеральным казначейством РФ в анализируемом периоде обусловлено введением цифровых систем на основе риск-ориентированного подхода, позволяющих на этапах планирования контрольных мероприятий отсеивать организации с низким уровнем риска и тем самым снижать нагрузку на контролирующий орган и получателей бюджетных средств. Динамика контрольных мероприятий в 2020 г. по сравнению с 2019 г. указывает на наличие иных факторов, влияющих на деятельность контролирующих органов (эпидемиологическая ситуация, введение моратория на контрольные мероприятия).

Вместе с тем проведен анализ возврата бюджетных средств получателями в федеральный бюджет государства. Анализ показал, что при повсеместном введении цифровых технологий в систему государственного финансового контроля возврат в федеральный бюджет средств, использованных получателями не по целевому назначению, составил менее 1% от общей суммы потерь (рис. 1, 2). Низкий объем возвратов средств в федеральный бюджет может указывать в том числе на проблемы с низкой адаптацией получателей бюджетных средств к цифровым технологиям.

Таким образом, в современном мире цифровая трансформация системы государственного контроля является необходимым условием для повышения эффективности контроля в финансово-бюджетной сфере. Однако анализ внедрения и использования цифровых технологий в государственном финансовом контроле помимо явных преимуществ выявил ряд таких проблем, как низкий уровень межведом-

ственной интеграции и медленная адаптация к новым технологиям, что подтверждает необходимость разработки дополнительных мер для обеспечения эффективного использования цифровых технологий при осуществлении бюджетного контроля.

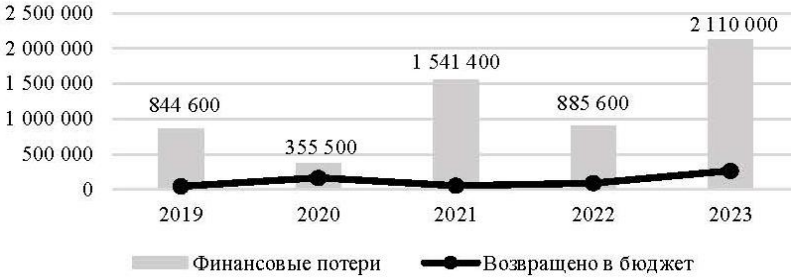

Рис. 1. Результаты проверок Счетной палатой РФ, млн руб.

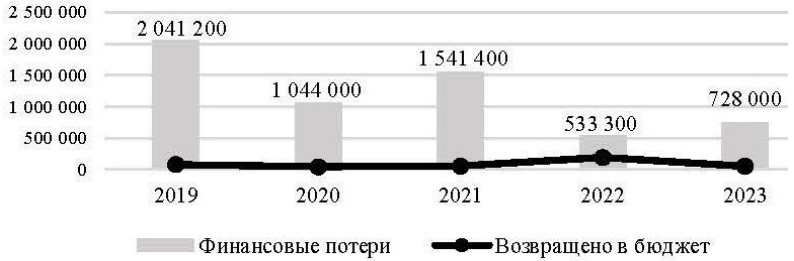

Рис. 2. Результаты проверок Федерального казначейства РФ, млрд руб.

ЛИТЕРАТУРА

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс]. – Указ Президента РФ от 09.05.2017 № 203. – Доступ из справ.-правовой системы «КонсультантПлюс».

2. Годовой отчет. Счетная палата Российской Федерации [Электронный ресурс]: Счетная палата Российской Федерации. – URL: https://ach.gov.ru/reports/ (дата обращения: 30.12.2024).

3. Доклады и отчёты [Электронный ресурс]: Информация официального сайта Федерального казначейства. – URL: https://roskazna.gov.ru/o-kaznachejstve/plany-i-otchety/o-rezultatakh-raboty-fk/?ysclid=m5b2w40vyg913982396 (дата обращения: 30.12.2024).

УДК 338.27

ОСОБЕННОСТИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ПРЕДПРИЯТИЯ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В.А. Колупаева, студентка каф. ЭБ

Научный руководитель С.В. Глухарева, ст. преп. каф. КИБЭВС

г. Томск, ТУСУР, victoriaschiriaewa@yandex.ru

Экономическая безопасность предприятий КИИ критически важна для стабильности государства и общества. В настоящее время особое внимание уделяется атомной отрасли. Исследование направлено на анализ проблем безопасности КИИ и разработку рекомендаций для их решения.

Ключевые слова: критическая информационная инфраструктура, КИИ, экономическая безопасность, кибербезопасность, организация производства.

В условиях цифровизации и глобализации экономическая безопасность предприятий КИИ становится всё более актуальной. Предприятия КИИ обеспечивают стабильность государства и общества.

Экономическая безопасность предприятия – это состояние защищенности его интересов от внешних и внутренних угроз, способных привести к существенным негативным последствиям для его финансовой стабильности, производственной деятельности, репутации и конкурентных преимуществ [1]. Ключевыми элементами экономической безопасности предприятия являются [2]:

– финансовая устойчивость: способность генерировать доход, покрывать расходы и инвестировать в развитие;

– производственная безопасность: защита от сбоев и остановок в производственном процессе;

– информационная безопасность: защита данных от несанкционированного доступа, изменений и утечек;

– кадровая безопасность: защита от недобросовестных действий, краж и некомпетентности сотрудников;

– репутационная безопасность: защита имиджа от негативных кампаний и скандалов.

Критическая информационная инфраструктура (КИИ) – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов [3]. На экономическую безопасность предприятий КИИ влияют:

– внешние факторы: геополитическая обстановка, санкции, киберугрозы, технологические изменения, конкуренция;

– внутренние факторы: уровень технической защиты, система управления рисками, компетентность персонала, финансовое состояние, корпоративная культура.

Основные угрозы и риски для КИИ:

1. Киберугрозы: атаки на информационные системы, вымогательство данных, несанкционированный доступ, сбои из-за кибератак.

2. Финансовые риски: мошенничество, недобросовестная конкуренция, санкции, инфляция, девальвация валют.

3. Технологические риски: сбои оборудования, нехватка квалифицированных кадров, развитие технологий, используемых для атак.

4. Репутационные риски: негативные информационные кампании, утечки конфиденциальной информации, скандалы, наносящие ущерб имиджу.

В контексте современных вызовов и угроз обеспечение экономической безопасности предприятий КИИ является ключевым фактором их устойчивого развития и гарантией безопасности для населения и окружающей среды. Для повышения уровня экономической безопасности предприятия КИИ необходимы следующие меры:

1. Организационные меры:

– создать единый центр безопасности для координации усилий, управления рисками и взаимодействия с внешними организациями.

2. Техническая модернизация:

– внедрить современные системы защиты: многофакторную аутентификацию, шифрование данных, обновление антивирусного ПО;

– усилить кибербезопасность через аудиты, планы предотвращения кибератак и обучение персонала;

– разработать и тестировать планы восстановления после инцидентов, создать резервные копии данных.

3. Финансовая устойчивость:

– диверсифицировать доходы через новые направления деятельности и рынки;

– оптимизировать управление финансами через бюджетирование, контроль расходов и внутренний аудит;

– сформировать резервные фонды и увеличить долю собственных средств.

4. Юридическая защита:

– обновить документы по безопасности с учетом современных угроз;

– заключить контракты о неразглашении и усилить контроль доступа к конфиденциальной информации;

– внедрить систему мониторинга легальной деятельности и создать отдел юридического обеспечения безопасности.

Таким образом, экономическая безопасность предприятий КИИ требует особого внимания из-за высокой ответственности, строгого контроля, специфических угроз и значительных финансовых затрат. Для её повышения рекомендуется создать единый центр безопасности, внедрить современные системы защиты, усилить кибербезопасность, диверсифицировать доходы, оптимизировать управление финансами, обновить документы по безопасности и усилить юридическую защиту, что обеспечит устойчивое развитие и безопасность предприятия КИИ.

ЛИТЕРАТУРА

1. Указ Президента Российской Федерации от 13.05.2017 г. № 208. О Стратегии экономической безопасности Российской Федерации на период до 2030 года: сайт – Президент России [Электронный ресурс]. – URL: https://www.kremlin.ru/acts/bank/41921 (дата обращения: 05.10.2024).

2. Линко И.В. Понятие и элементы экономической безопасности предприятий // Экономика и социум. – 2022. – № 9 (100). – Сайт: Cyberleninka. – URL: https://cyberleninka.ru/article/n/ponyatie-i-elementy-ekonomicheskoy-bezopasnosti-predpriyatiy (дата обращения: 05.10.2024).

3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. – Сайт «Консультантплюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/?ysclid=m2ml6vtlae991479963 (дата обращения: 15.10.2024).

4. Афанасьева С.В. Инновационные методы предотвращения киберугроз в целях обеспечения экономической безопасности организации / С.В. Афанасьева, Е.С. Черепанова, Н.В. Шехова // Вестник Самар. ун-та. Экономика и управление. – 2023. – Т. 14, № 2. – С. 7–16. DOI: 10.18287/2542-0461-2023-14-2-7-16. – Сайт: Elibrary [Электронный ресурс]. – URL: https://www.elibrary.ru/item.asp?id=54245552 (дата обращения: 20.10.2024).

5. Щербакова О.Р. Экономическая безопасность наукоемких предприятий // Символ науки. – 2020. – № 10. – Сайт: Cyberleninka [Электронный ресурс]. – URL: https://cyberleninka.ru/article/ n/ekonomicheskaya-bezopasnost-naukoemkih-predpriyatiy (дата обращения: 8.03.2025).

6. Ершова М.И. Методы и методики анализа экономической эффективности деятельности инжиниринговых компаний атомной энергетики: дис. … канд. экон. наук. – Нижегород. гос. техн. ун-т им. Р.Е. Алексеева, 2023. – 157 с. – Сайт: Elibrary [Электронный ресурс]. – URL: https://www.elibrary.ru/item.asp?id=74041302 (дата обращения: 8.03.2025).

УДК 65.011.56

ПРОГНОЗИРОВАНИЕ НАДЕЖНОСТИ КОНТРАГЕНТОВ НА ОСНОВЕ АНАЛИЗА ФИНАНСОВОГО СОСТОЯНИЯ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

Р.В. Солоха, Д.В. Старосельцева, С.П. Боброва, С.М. Машковская, студенты 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, zummer38@mail.ru

Рассматривается проблема оценки надежности контрагентов в современной бизнес-среде, характеризующейся повышенной неопределенностью и рисками. В статье анализируются ограничения традиционных методов оценки, основанных на анализе финансовой отчетности при выявлении скрытых рисков и прогнозировании финансовых трудностей партнеров. Предложена новая модель прогнозирования надежности контрагентов на основе анализа финансового состояния с использованием методов машинного обучения. Рассматриваются возможности использования современных технологий при оценке надежности деловых партнеров и их роли в обеспечении стабильности развития компании.

Ключевые слова: надежность контрагентов, машинное обучение, финансовый анализ, прогнозирование рисков, безопасность бизнеса.

Современная экономическая среда, характеризующаяся геополитической нестабильностью и ужесточением регуляторных требований, создает условия, при которых риски, связанные с недобросовестными или финансово неустойчивыми контрагентами, значительно увеличиваются. К началу 2025 г. количество индивидуальных предпринимателей в России превысило 4,5 млн, показав рост за три года на 23%, данный рост обусловлен развитием цифровых сервисов, увеличением доходов населения и мерами государственной поддержки, что делает необходимым более эффективное управление рисками при выборе контрагентов. И как следствие – резкое повышение индивидуальных предпринимателей может повлиять на рынок контрагентов и потребовать более тщательной проверки. Государство создает условия для большего открытия индивидуальных предпринимателей, но также ужесточает регуляторные требования [1].

В области оценки надежности контрагентов регуляторы фокусируются на исследовании кредитного рейтинга и анализе финансовой отчетности. Однако эти методы обладают значительными ограничениями: человеческий фактор приводит к субъективным ошибкам интерпретации данных, а линейные модели не учитывают малозаметные

взаимосвязи между множеством показателей, таких как долговая нагрузка, ликвидность и рентабельность. Чтобы минимизировать человеческий фактор, необходимо полностью или частично внедрить использование методов машинного обучения для прогнозирования надежности контрагентов, которые могут продемонстрировать более детальное исследование, так как машинное обучение позволяет выявлять сложные закономерности в финансовых отчетах и улучшать точность прогнозирования.

Машинное обучение предлагает более детальный подход к анализу данных, позволяя выявлять сложные закономерности и улучшать точность прогнозирования. Для реализации такой системы необходимо разработать комплексную методологическую основу, которая будет включать сбор и обработку данных, отбор значимых признаков и построение моделей машинного обучения.

В данном исследовании предлагается модель прогнозирования надежности контрагентов, основанная на анализе финансового состояния с использованием методов машинного обучения. Методология включает следующие этапы:

1. Сбор данных о финансовых показателях российских компаний. Источниками данных являются базы данных СПАРК, Ruslana.

2. Отбор финансовых показателей, влияющих на надежность контрагентов, с использованием методов статистического анализа и экспертных оценок.

3. Построение модели машинного обучения для прогнозирования надежности с учетом отобранных признаков. В качестве моделей используются алгоритмы логистической регрессии, дерева решений и случайного леса.

4. Оценка качества построенных моделей с использованием метрик точности, полноты, F1-меры и AUC-ROC [2–4].

Разработка и внедрение предложенной методологии позволит компаниям более качественно отбирать контрагентов, сократить финансовые потери от ненадежных партнеров и повысить стабильность бизнеса. Использование машинного обучения для анализа финансового состояния контрагентов позволяет обнаруживать скрытые риски и прогнозировать потенциальные проблемы, что является ключевым аспектом при анализе финансового состояния с использованием машинного обучения.

ЛИТЕРАТУРА

1. РИА Новости. Число ИП в России в начале 2025 года превысило 4,5 миллиона [Электронный ресурс]. – URL: https://ria.ru/20250306/ip-2003327978.html (дата обращения: 12.03.2025).

2. Контур.Фокус. Анализ надежности контрагентов: управление рисками и ключевые факторы выбора надежного контрагента [Электронный ре-

сурс]. – URL: https://scan-interfax.ru/blog/analiz-nadezhnosti-kontragentov-i-upravlenie-riskami-klyuchevye-faktory-vybora-nadezhnogo-kontragenta/ (дата обращения: 12.03.2025).

3. Get-Investor. Проверка контрагента. Новые инструкции и рекомендации, 2024 [Электронный ресурс]. – URL: https://get-investor.ru/proverka-kontragenta (дата обращения: 12.03.2025).

4. Pravovest-Audit. Проблемные контрагенты: что учесть на практике в 2024 году [Электронный ресурс]. – URL: https://pravovest-audit.ru/nashi-statii-nalogi-i-buhuchet/problemnye-kontragenty-chto-uchest-na-praktike-v-2024-godu/ (дата обращения: 15.02.2025).

УДК 004.89

ГОЛОСА И ЛИЦА ИЗ НИЧЕГО: КАК НЕЙРОННЫЕ СЕТИ ПРЕВРАЩАЮТ ДАННЫЕ В ОРУЖИЕ МОШЕННИКОВ

Д.В. Старосельцева, Р.В. Солоха, С.П. Боброва, С.М. Машковская, студенты 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, staroseltseva.diana@mail.ru

Рассмотрены современные технологии, такие как генеративные состязательные сети (GAN), синтез речи, deepfakes, Recurrent Neural Networks (RNN), которые активно используются в преступных целях. Проведен анализ рисков, связанных с использованием этих технологий.

Ключевые слова: нейронные сети, GAN, deepfakes, синтез речи, RNN, мошенничество, искусственный интеллект, синтетические данные.

Современные достижения в области искусственного интеллекта, в частности, развитие нейронных сетей – компьютерных систем, имитирующих работу человеческого мозга для обработки и анализа данных, привели к появлению технологий, способных генерировать синтетические данные, такие как изображения, видео и аудио, практически неотличимые от реальных. Эти технологии, изначально применявшиеся в развлекательной индустрии, стали угрозой для безопасности, поскольку мошенники используют их для обмана, манипуляции людьми и кражи личных данных. Основная сложность заключается в трудности обнаружения фальшивых изображений и голосов, что нарушает личную безопасность и конфиденциальность. Только в финансовом секторе число атак с использованием дипфейков за прошлый год выросло почти на 15%, и эксперты ожидают, что в 2025 г. количество таких атак увеличится еще в два раза. Актуальность про-

блемы возрастает на фоне увеличения случаев использования подобных технологий для мошенничества и отсутствия эффективных средств защиты [1].

Для более глубокого понимания того, как нейронные сети превращают данные в инструмент мошенничества, необходимо провести анализ (таблица).

Технологии синтетических данных и их риски

Технология	Описание	Примеры	Риск
Генеративные сети (GAN)	Класс нейронных сетей, состоящих из двух конкурирующих подмодулей: генератора и дискриминатора. Генератор создает синтетические данные, а дискриминатор пытается отличить их от реальных. В результате такого противоборства генератор учится создавать данные, которые все сложнее отличить от настоящих	Создание фальшивых изображений людей (например, водительских прав или паспортов), синтетических лиц и сцен. Используется в фальшивых видео для обмана	Утечка персональных данных, фальсификация документов, манипуляции с общественным мнением
Синтез речи	Технологии синтеза речи, такие как Tacotron и WaveNet, для создания речи, похожей на голос конкретного человека. Эти системы обучаются на больших объемах аудиоданных, что позволяет им воспроизводить интонации, акценты и другие особенности речи	Использование синтезированных голосов для звонков с целью получения конфиденциальной информации (например, через голосовые фишинг-звонки)	Мошенничество через подделку голоса, шантаж
Deepfakes	Системы, основанные на нейронных сетях, создающие фальшивые видео, где лица людей заменяются или модифицируются	Подделка видео с политическими или публичными личностями для распространения фальшивых новостей	Нарушение репутации, распространение ложной информации
Recurrent Neural Networks (RNN)	Использование рекуррентных нейронных сетей для анализа и синтеза текстов, что позволяет им имитировать стиль речи или письма человека	Мошенничество с использованием синтезированных сообщений, имитирующих стиль общения конкретных людей (например, создание поддельных электронных писем от имени руководителя компании с требованием перевода средств на мошеннический счет)	Манипуляции с личной перепиской, обман доверительных лиц

Цель анализа заключается в исследовании как механизмов работы технологий, таких как GAN, синтез речи, deepfakes и RNN, так и их влияния на общество, включая риски и последствия их использования в преступных целях.

Технологии, представленные в таблице, показывают, что создание фальшивых изображений и звуков стало доступным и легко управляемым процессом. Эти методы, обладая высоким уровнем правдоподобия, повышают риски использования этих технологий в мошеннических схемах [2–4].

Развитие нейронных сетей и технологий генерации синтетических данных открывает новые возможности для творчества и исследований, но одновременно создает серьезные угрозы для безопасности и конфиденциальности. Мошенники активно используют эти технологии для создания фальшивых изображений, видео и аудиозаписей, что приводит к увеличению числа случаев обмана, манипуляции общественным мнением и кражи личных данных.

ЛИТЕРАТУРА

1. Как мошенники используют нейронные сети: основные схемы преступления: статья на РЕН ТВ [Электронный ресурс]. – URL: https://ren.tv/longread/1299041-kak-moshenniki-ispolzuiut-neiroseti-osnovnye-skhemy-prestuplenii (дата обращения: 01.03.2025).

2. Хабр. Телефонное мошенничество: как это работает [Электронный ресурс]. – URL: https://habr.com/ru/companies/t2/articles/888984/ (дата обращения: 11.03.2025).

3. NEUROhive. Рекуррентная нейронная сеть (RNN): виды, обучение, примеры [Электронный ресурс]. – URL: https://neurohive.io/ru/osnovy-data-science/gan-rukovodstvo-dlja-novichkov/ (дата обращения: 02.03.2025).

4. NEUROhive. Генеративно-состязательная нейросеть (GAN): архитектура, примеры, код [Электронный ресурс]. – URL: https://neurohive.io/ru/osnovy-data-science/gan-rukovodstvo-dlja-novichkov/ (дата обращения: 02.03.2025).

УДК 336.711.2

ТЕНДЕНЦИИ ПЕРЕХОДА К ИСПОЛЬЗОВАНИЮ ИННОВАЦИОННЫХ ИНСТРУМЕНТОВ НА БАЗЕ ЦИФРОВЫХ ВАЛЮТ ЦЕНТРАЛЬНЫХ БАНКОВ

Д.Д. Зайцев, студент каф. ЭБ

Научный руководитель О.В. Кочетков, ст. преп. каф. ЭБ

г. Томск, ТУСУР, saintundead1111@mail.ru

В условиях активной цифровой трансформации экономических отношений все больше стран разрабатывают и внедряют в оборот национальные цифровые валюты. Однако их распространение сталкивается с рядом препятствий, главным из которых является низкий

интерес со стороны населения. Интеграция смарт-контрактов на базе цифровых валют не только повысит их практическую ценность, но и откроет новые возможности для автоматизации финансовых операций, увеличения прозрачности сделок и снижения операционных издержек.
Ключевые слова: цифровая валюта, смарт-контракт, цифровизация, проблемы реализации.

В последние годы цифровая трансформация финансовой системы стала одним из ключевых направлений развития мировой экономики. Центральные банки многих стран активно исследуют и внедряют цифровые валюты, стремясь повысить эффективность денежных расчетов, снизить издержки и создать более прозрачную финансовую среду.

Тем не менее, опираясь на опыт стран, запустивших в действие CBDC, стоит выделить тот факт, что выпуск цифровых валют не является достаточным условием для их успешного распространения и востребованности. Исходя из этого, возникает необходимость реализации и интеграции инновационных инструментов, способных значительно расширить функционал цифровых активов.

Трудности на пути становления новых экономических отношений. Несмотря на перспективность направления, интеграция и адаптация цифровых валют сталкиваются с рядом сложностей, а также с недостаточной заинтересованностью населения. Основные проблемы можно разделить на три кластера: организационный, правовой и технический.

Организационные сложности связаны с отсутствием инновационных механизмов, способных существенно изменить текущие процессы проведения платежей. Первоначально цифровые валюты разрабатывались с акцентом на безопасность и удобство транзакций, ориентируясь на массового потребителя. Однако статистика показывает, что привычные методы расчетов остаются востребованными и после прекращения государственного стимулирования спрос на цифровую валюту снижается. Это указывает на необходимость пересмотра формы представления новой денежной системы [1–5].

Основываясь на данных национальных центральных банков, следует, что объем операций с валютой в редких случаях превышает 30%. Это может свидетельствовать о невостребованности цифровых валют центральных банков в существующем виде.

Аспекты в области права также играют важную роль, так как внедрение инноваций неизбежно сопровождается появлением новых форм мошенничества, что снижает доверие не только к самой цифровой валюте, но и к финансовой системе в целом. Наиболее уязвимые слои населения особенно подвержены влиянию противников таких изменений.

Концепция цифровых валют – это следующий шаг в сфере межбюджетных отношений, переход на новый этап всегда требует особого внимания к технической проработанности процессов. Построение на основе ЦВЦБ может создать ряд угроз, которые в случае успешной реализации смогут нанести непоправимый ущерб финансовой системе.

Возможный сценарий решения. Одним из наиболее перспективных решений является использование смарт-контрактов, поскольку цифровые валюты национальных банков основаны на технологии блокчейн, обеспечивающей возможность автоматизированных, прозрачных и безопасных сделок.

Внедрение такого инструмента особенно выгодно предпринимателям, так как оно минимизирует риски невыполнения обязательств, снижает издержки, а также упрощает и ускоряет процесс. Государству же этот подход позволяет оптимизировать межбюджетные платежи, повысить прозрачность финансовых потоков и сократить объем теневой экономики, что особенно актуально для стран Южной Африки [6]. Это, в свою очередь, способствует увеличению бюджетных поступлений.

Таким образом, внедрение смарт-контрактов в систему цифровых валют национальных банков способствует росту доверия, повышению эффективности финансовых операций и созданию устойчивого спроса на этот инструмент.

ЛИТЕРАТУРА

1. Статистика обращения эНайра [Электронный ресурс]: Информационный ресурс: Центральный Банк Нигерии. – URL: https://www.cbn.gov.ng/currency/eNaira.html (дата обращения: 10.03.2024).

2. Банк Японии выпускает первую партию цифровой валюты Центрального банка Ямайки [Электронный ресурс]: Информационный ресурс «Центральный Банк Ямайки». – URL: https://boj.org.jm/boj-mints-first-batch-of-jamaicas-central-bank-digital-currency/ (дата обращения: 10.03.2024).

3. Рабочий документ: Расширение доступа к финансовым услугам и цифровая валюта Центрального банка на Багамах [Электронный ресурс]: Информационный ресурс «Центральный Банк Багамских островов». – URL: https://www.centralbankbahamas.com/publications/working-papers/working-paper (дата обращения: 13.03.2024).

4. Рост цифрового юаня: данные из отчета НБК [Электронный ресурс]: Информационный ресурс «Дапп Эксперт». – URL: https://dapp.expert/ru/news/ru_growth-of-digital-yuan-insights-from-pboc-report (дата обращения: 13.03.2024).

5. Пилотная программа иранского цифрового риала на острове Киш [Электронный ресурс]: Информационный ресурс «Дапп Эксперт». – URL: https://dapp.expert/news/en_iran-s-digital-rial-pilot-program-on-kish-island (дата обращения: 13.03.2024).

6. Статистика теневой экономики по отношению к ВВП 2023 год [Электронный ресурс]: Информационный портал «Мировой Экономики». – URL: https://www.worldeconomics.com/informal-Economy/ (дата обращения: 06.04.2025).

ПОДСЕКЦИЯ 4.4

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЕГО ПРИЛОЖЕНИЯ

*Председатель – **Костюченко Е.Ю.**, и.о. зав. каф. БИС, к.т.н., доцент;*
*зам. председателя – **Новохрестова Д.И.**, доцент каф. КИБЭВС, к.т.н.*

УДК 004.8

ОПРЕДЕЛЕНИЕ АКЦЕНТА ДИКТОРА С ПОМОЩЬЮ МЕЛ-СПЕКТРОГРАММ

А.И. Егорова, С.Д. Канатников, И.С. Фищук, М.Д. Аристархова, студенты каф. БИС
Научный руководитель П.Ю. Лаптев, м.н.с. в ЦК НТИ ТДВ, ассистент каф. БИС
Проект ГПО КИБЭВС-2401. Определение психоэмоционального состояния диктора с помощью методов машинного обучения
г. Томск, ТУСУР, egorovanasta226@mail.com

Исследуется применение мел-спектрограмм для классификации акцентов дикторов. Рассмотрены два метода извлечения признаков: динамический подход, позволяющий сохранять временные характеристики аудиосигнала посредством дополнения спектрограмм до единой длины, и фиксированный подход, использующий спектрограммы с заранее заданными размерами. Сравнительный анализ показал, что фиксированный метод обеспечивает более высокую точность и стабильность обучения, что делает его перспективным для практических задач распознавания акцентов в системах обработки речи.
Ключевые слова: мел-спектрограммы, классификация акцентов, динамическое извлечение признаков, фиксированное извлечение признаков, нейронные сети, обработка аудиосигналов.

Современные технологии обработки аудиосигналов активно применяются в задачах распознавания речи и идентификации характеристик дикторов. Одной из важных задач является определение акцента диктора, что имеет практическое значение для систем автоматизированного перевода, речевого синтеза и анализа речи.

Мел-спектрограммы – визуальное представление аудиосигнала, где каждая ось отображает частотный и временной диапазоны, а интенсивность отражает амплитуду. Этот подход позволяет эффективно выявлять паттерны, характерные для различных акцентов. В акцентах могут быть особенности, такие как длина пауз, которые будут заметны в спектрограмме. В некоторых акцентах, например, в британском и американском варианте английского, акценты могут влиять на распределение частот, где одни звуки могут быть более выраженными, а другие – менее яркими. Также мел-спектрограммы могут выявлять различные особенности произношения на уровне темпа речи. Например, в некоторых акцентах может наблюдаться более быстрый или медленный темп речи, что будет отражаться на временной оси спектрограммы [1].

Для решения задачи классификации акцентов были разработаны два подхода к извлечению признаков из аудиосигналов:

1. Динамический подход, в котором спектрограммы приводятся к единому размеру посредством дополнения нулями, сохраняя временные характеристики сигнала;

2. Фиксированный подход, использующий спектрограммы фиксированного размера, что обеспечивает однородность входных данных.

При динамическом подходе аудиосигналы преобразуются в мел-спектрограммы, после чего каждая спектрограмма дополняется нулями до максимальной длины [2]. Модель, основанная на комбинации сверточных слоев для выделения локальных признаков и LSTM для учета временных зависимостей, была обучена на данной выборке. Итоговая точность классификации составила около 56%. Несмотря на сохранение временной информации, метод демонстрирует сложности при обработке неоднородных входных данных, что отражается на общей стабильности результатов. На рис. 1 представлен отчет о классификации моделью, использующей динамический подход, содержащий результаты классификации пяти акцентов.

При использовании фиксированного метода каждая мел-спектрограмма генерируется с заранее определёнными параметрами (фиксированное число временных шагов и частотных полос). Сверточная нейронная сеть, обученная на унифицированных тензорах, показала более стабильное обучение и достигла точности около 70%. Унификация размеров входных данных позволила снизить влияние вариаций длины аудиосигналов и обеспечить лучшую обобщаемость модели. На рис. 2 представлен отчет о классификации моделью, использующей фиксированный подход, содержащий результаты классификации пяти акцентов.

	precision	recall	f1-score	support
african	0.49	0.65	0.56	86
england	0.47	0.32	0.38	66
indian	0.67	0.59	0.63	71
newzealand	0.70	0.66	0.68	80
scotland	0.50	0.55	0.52	53
accuracy			0.56	356
macro avg	0.56	0.55	0.55	356
weighted avg	0.57	0.56	0.56	356

Рис. 1. Отчет о классификации моделью, использующей динамический подход

	precision	recall	f1-score	support
african	0.64	0.65	0.64	68
england	0.55	0.67	0.60	72
indian	0.82	0.67	0.74	73
newzealand	0.79	0.82	0.81	74
scotland	0.77	0.69	0.72	67
accuracy			0.70	354
macro avg	0.71	0.70	0.70	354
weighted avg	0.71	0.70	0.70	354

Рис. 2. Отчет о классификации моделью, использующей фиксированный подход

ЛИТЕРАТУРА

1. Hossan M.A. A novel approach for MFCC feature extraction / M.A. Hossan, S. Memon, M.A. Gregory [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/224217606_A_novel_approach_for_MFCC_feature_extraction, свободный (дата обращения: 05.03.2025).

2. Spectrogram Types: The Many Faces of the Spectrogram / Alan Wolke [Электронный ресурс]. – Режим доступа: https://www.tek.com/en/blog/spectrogram-types-the-many-faces-of-the-spectrogram, свободный (дата обращения: 06.03.2025).

3. Dynamic Time Warping (DTW) in Time Series [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/dynamic-time-warping-dtw-in-time-series/, свободный (дата обращения: 06.03.2025).

УДК 004.056

СОСТЯЗАТЕЛЬНЫЕ АТАКИ НА АУДИОДАННЫЕ В НЕЙРОННЫХ СЕТЯХ И МЕТОДЫ ЗАЩИТЫ

А.Э. Коренев, Г.С. Белокрылов, магистранты каф. КИБЭВС
Научный руководитель Д.И. Новохрестова,
доцент каф. КИБЭВС, к.т.н.
г. Томск, ТУСУР, tura9@mail.ru

Рассмотрен метод проведения состязательных атак на нейронные сети, которые занимаются обработкой аудиоданных. Также предложен подход обнаружения воздействия на данные с использованием вычисления энтропии предсказаний модели.
Ключевые слова: аудиозаписи, набор данных, состязательная атака, речь, энтропия.

Основная проблема в атаках на нейронные сети, обрабатывающие аудиоданные, состоит в том, что не существует каких-то универсальных защитных методов, позволяющих от таких атак защититься.

Существует ряд работ [1–3], в которых описывались атаки на такие нейронные сети, однако, как правило, атаки были направлены на модель, а не на данные.

Также были и предложены методы защиты от различных атак [4], которые на самом деле оказываются бессильны в случае искажения в наборе данных. Это приводит к актуальности темы состязательных атак на нейронные сети, обрабатывающие аудиоданные, а именно защиты от таких атак.

Набором данных был выбран AudioMNIST. Он состоит из 30 000 аудиофайлов в формате wav, которые содержат записи произнесения цифр от 0 до 9 различными дикторами в количестве шестидесяти. На каждого диктора приходится по одному каталогу с аудиозаписями (по 500 файлов на диктора).

Архитектура нейронной сети представлена следующим образом: в рамках каждого сверточного слоя задаются параметры свертки (размер входного и выходного пространства, размер ядра, stride, padding), функция активации RELU и нормализация с использованием BatchNorm2d). Сама же нейронная сеть состоит из четырех последовательных сверточных слоев, слоя пулинга и полносвязного слоя на выходе для определения принадлежности произнесенной цифры.

Модель обучена на 5 эпохах. Точности на каждом из подмножеств набора данных получились следующие (метрика Accuracy):

– для обучающей выборки: 0,99;
– для валидационной выборки: 0,98;
– для тестовой выборки: 0,98.

Проводилась атака следующим образом:

– Создавался тензор случайным образом с учетом величины искажения.

– Затем этот тензор складывался с исходным сигналом на определенных промежутках.

– Зашумленный сигнал помещался в набор данных для обучения и тестирования.

Были проведены попытки определить на слух, есть ли разница между сигналами.

При попытке прослушивания аудиофайла в исходном виде и в зашумленном разницы обнаружено не было.

Также произведены попытки распознавания сигнала в исходном виде и в зашумленном. Системами SPT данный сигнал был распознан как «One» в обоих случаях.

Точность после применения состязательной атаки на тестовом наборе данных составила 0,63.

Был предложен защитный подход, который позволит обнаружить факт того, что данные были атакованы, с учетом незаметных искажений сигнала и малых изменений точности.

Так, был предложен метод вычисления энтропии в получаемом распределении предсказаний модели на тестовом наборе данных. На входе имеется обученная на чистых данных нейронная сеть, которая формирует набор предсказаний на исходных тестовых данных и атакованных тестовых данных. В данном случае рассматриваются только значения энтропии предсказаний модели на тестовых данных.

Для вычисления энтропии использовался метод в scipy.stats «entropy». Таким образом, сначала высчитывается энтропия в рамках одного батча для каждого класса с учетом распределения вероятностей, записывается в отдельную переменную. Тестовый набор данных состоит из 2 400 значений, который разбивается на пакеты по 32 значения. Таким образом, рассматривается 75 массивов с метками классов. На каждом массиве определяется энтропия предсказаний, после чего сводится в общий массив. Полученные значения энтропии усредняются по всему набору данных. То же самое было воспроизведено для атакованных данных.

Таким образом, при сравнении энтропии на исходном наборе данных и измененном наборе данных можно рассматривать величину искажения предсказаний модели. Задав порог различий между эталонной энтропией и текущей, можно утверждать, были атакованы данные или нет.

ЛИТЕРАТУРА

1. Goodfellow I.J. Explaining and Harnessing Adversarial Example / Ian J. Goodfellow , J. Shlens, C. Szegedy // 3rd International Conference on

Learning Representations, ICLR–2015. – San Diego, CA, USA, May 7–9, 2015, Conference Track Proceedings.

2. Intriguing properties of neural networks / C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I.J. Goodfellow, R. Fergus // 2nd International Conference on Learning Representations, ICLR–2014. – Banff, AB, Canada, April 14–16, 2014, Conference Track Proceedings.

3. Weight Poisoning Attacks on Pre-trained Models [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2004.06660, свободный (дата обращения: 10.03.2025).

4. Weng T.-W. et al. Evaluating the Robustness of Neural Networks: An Extreme Value Theory Approach // International Conference on Learning Representations, 2018. [Электронный ресурс]. – Сайт с научными статьями. URL: https://arxiv.org/pdf/1801.10578.pdf (дата обращения: 11.03.2025).

УДК 004.852

СОВМЕЩЕНИЕ ДАННЫХ О ДИНАМИКЕ ДВИЖЕНИЯ ЗРАЧКОВ И ДИНАМИКЕ ДВИЖЕНИЯ МЫШИ ДЛЯ ПРОДЛЁННОЙ АУТЕНТИФИКАЦИИ

С.А. Давыденко, аспирант каф. КИБЭВС

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

Выполнено обучение моделей искусственного интеллекта для выполнения аутентификации по динамике движения зрачков, выполнения аутентификации по динамике движения мыши, а также для совмещения результатов аутентификации по этим двум характеристикам. Аутентификация выполнялась на собственном наборе данных, для аутентификации по динамике движения зрачков точность работы модели составила 72,52%, для динамики движения мыши точность работы модели составила 82,15%. После совмещения данных удалось повысить точность классификации до 86,1%.

Ключевые слова: продлённая аутентификация, биометрия, динамика движения зрачков, динамика движения мыши, совмещение биометрических характеристик.

Продлённая аутентификация позволяет выполнять проверку личности пользователя не только при первоначальном входе в систему, но и на протяжении всего сеанса работы. Это выгодно выделяет такой подход по сравнению с использованием только первичного фактора аутентификации, например пароля. В большинстве случаев для продлённой аутентификации используют биометрические факторы, которые можно разделить на физические и поведенческие. В данной рабо-

те рассматривается применение динамики движения зрачков и динамики движения мыши как основных поведенческих характеристик для выполнения продлённой аутентификации.

Для выполнения продлённой аутентификации использовался собственный набор данных (содержащий данные 40 человек), в котором данные о динамике движения зрачков и динамике движения мыши собирались одновременно. При этом следует отметить, что для сбора данных о движении зрачков использовалась веб-камера, а не специализированное устройство (что понижает качество собранных данных, но делает предлагаемое решение более доступным). Поскольку при работе за компьютером и перемещении курсора пользователь отслеживает его местонахождение взглядом, совмещение этих характеристик имеет смысл [1].

Помимо этого, обе характеристики представляют собой передвижение точки по плоскости, что позволяет использовать схожие физические характеристики для выделения признаков. К таким характеристикам подходят скорость, ускорение, рывок, их стандартные отклонения, гистограммы направлений. Основные характеристики, использованные в качестве признаков, а также способы их расчёта приведены в [2], помимо них, для динамики движения зрачков также использовались дополнительные данные о тангаже и рыскании, вычисляемые на этапе сбора данных (их средние, минимальные, максимальные значения, стандартное и среднеквадратическое отклонения, а также отношение среднего значения к максимальному и отношение среднеквадратического отклонения к максимальному значению).

Для выполнения аутентификации использовалась сиамская нейронная сеть, для вычисления схожести данных применялось Евклидово расстояние. Обучение выполнялось на протяжении 100 эпох с оптимизатором Adam (скорость обучения 0,0005), в качестве функции потерь применялась функция MSE. Также использовались настройки для остановки обучения в случае достижения плато. Графики точности для аутентификации по движению зрачков и динамике движения мыши приведены на рис. 1. Для разделения тестовой выборки использовались последние 20% данных о пользователе, а для обучения – первые 75% данных. Такой способ разделения связан с необходимостью избавления от возможных пересечений между рассматриваемыми временными окнами для аутентификации.

Из графиков видно, что модели свойственно переобучение, скорее всего, это связано с недостаточным объёмом данных для одного пользователя. Обучение модели выполняется на основе информации с одного сеанса длиной 20 мин (связанной с техническими ограничени-

ями), в то время как поведенческие признаки требуют больших объёмов данных о пользователе для более качественной классификации, поскольку они сложнее поддаются анализу (при этом их также сложнее подменить) [3]. Итоговое качество классификации по динамике движения зрачков достигло 72,52%, а по динамике движения мыши – 82,15%.

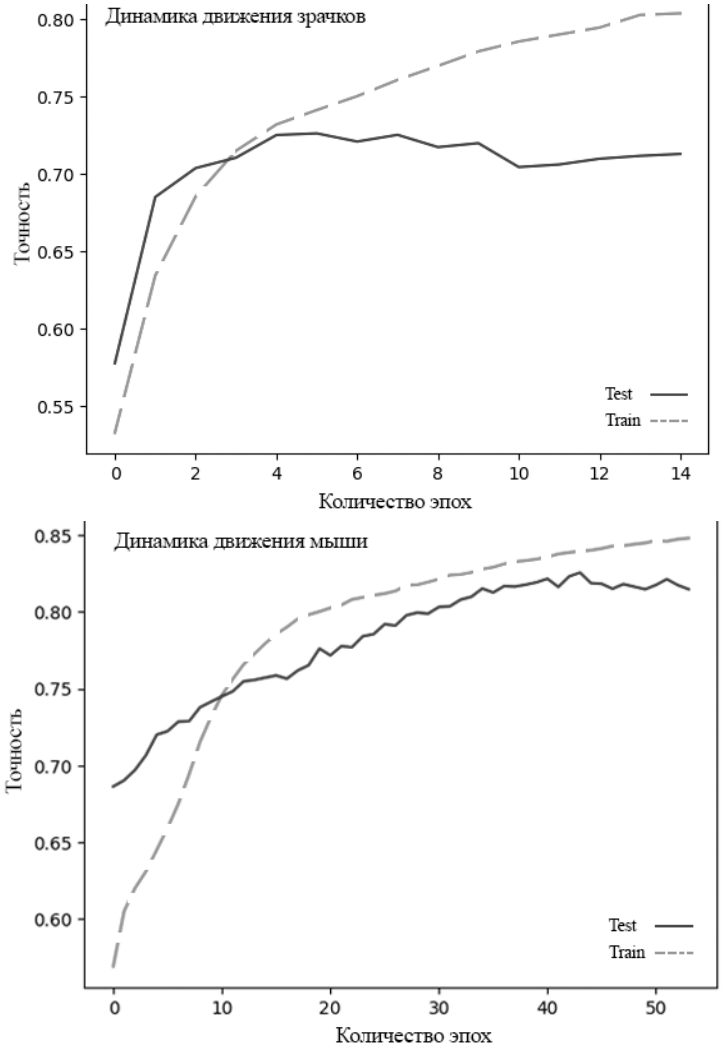

Рис. 1. Графики точности для каждого фактора

Для того чтобы повысить итоговое качество классификации, было выполнено совмещение данных с применением нескольких алгоритмов машинного обучения. Совмещение выполнялось на этапе принятия решения: для каждой рассматриваемой характеристики рассчитывалось расстояние, которое, в свою очередь, передавалось алгоритму для бинарной классификации и принятия итогового решения. Результаты работы алгоритмов представлены в таблице.

Результаты совмещения характеристик

Модель для принятия решения	Accuracy	Precision	Recall	F1
K-nearest neighbors	82,7	79,8	89,9	84,7
Classification And Regression Tree	86,1	89,1	82,3	86,1
Random forest	86,1	89,1	82,3	86,1
Ada Boost	86,1	89,1	82,3	86,1
Naïve Bayes	86,1	89,1	82,3	86,1
Quadratic Discriminant Analysis	86,1	89,1	82,3	86,1
Multilayer perceptron	86,1	89,1	82,3	86,1

Заключение. В результате данной работы была продемонстрирована целесообразность применения совмещения данных с нескольких биометрических характеристик для принятия решения при выполнении продлённой аутентификации. При предложенном подходе общая точность аутентификации не уменьшается по сравнению с применением факторов по отдельности, а большее число биометрических характеристик, используемых для продлённой аутентификации, снижает вероятность успешной атаки злоумышленника.

ЛИТЕРАТУРА

1. Rose J. Biometric authentication using mouse and eye movement data / J. Rose, Y. Liu, A. Awad // 2017 IEEE Security and Privacy Workshops (SPW). – IEEE, 2017. – P. 47–55.

2. Davydenko S. Continuous Authentication with Eye Movement Biometrics / S. Davydenko, E. Kostyuchenko // International Conference on Intelligent Information Technologies for Industry. – Cham: Springer Nature Switzerland, 2024. – P. 369–377.

3. Dahia G. Continuous authentication using biometrics: An advanced review / G. Dahia, L. Jesus, M. Pamplona Segundo // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2020. – Vol. 10, № 4. – P. e1365.

УДК 659.1

ТРЕНДЫ DIGITAL-МАРКЕТИНГА В 2025 ГОДУ

А.А. Калугин, Д.А. Девочкин, студенты каф. УИ
Научный руководитель Т.А. Байгулова, ст. преп. каф. УИ
г. Томск, ТУСУР, faf.hhh@inbox.ru, danil.devochkinkz@gmail.ru

Рассматриваются ключевые тенденции, которые будут определять тренды в интернет-маркетинге в 2025 г. Анализируется влияние искусственного интеллекта (ИИ), автоматизации, персонализации контента и развития новых рекламных технологий. Особое внимание уделяется адаптации к отказу от cookie, росту видеоконтента и новым форматам взаимодействия с аудиторией.
Ключевые слова: digital-маркетинг, искусственный интеллект, персонализация, автоматизация, видеоконтент, таргетинг.

В современном мире, где старые методы уже не так эффективно привлекают пользователей, компании ищут новые пути и способы взаимодействия с аудиторией. Digital-маркетинг развивается стремительными темпами, и 2025 г. принесет еще больше изменений. На фоне этого, пользователи ожидают более персонализированного подхода, удобного формата потребления контента и мгновенной обратной связи. Чтобы соответствовать данным ожиданиям, компании активно внедряют новые технологии, и одним из главных инструментов становится ИИ, который уже оказывает значительное влияние на рекламные процессы.

Целью данной работы является анализ актуальных digital-трендов и их влияние на маркетинговые стратегии компаний в 2025 г.

Анализ проведен на основе следующих параметров:

- уровень интеграции ИИ в маркетинговые инструменты,
- технологические изменения, влияющие на сбор и анализ данных,
- влияние персонализации на эффективность рекламных кампаний,
- динамика развития форматов digital-рекламы,
- новые тенденции в пользовательском поведении.

ИИ в маркетинге: автоматизация и персонализация. Искусственный интеллект помогает автоматизировать маркетинг, в частности, видео– и фотоконтент становится ключевым инструментом для продвижения, а социальные сети превращаются в полноценные торговые площадки, из-за того, что людям удобно покупать там, где они проводят много времени за общением, просмотром фото- и видеоконтента, а также где они могут легко получить рекомендации от друзей и знакомых или от алгоритмов, которые предсказывают интересы на основе предыдущих взаимодействий. ИИ помогает анализировать

данные пользователей, создавая таргетированию рекламу и персонализированные предложения, чтобы повысить вероятность покупки.

Генеративный ИИ: стремительный рост и перспективы. Помимо автоматизации стандартных маркетинговых процессов, особенный акцент делается на сегменте генеративного ИИ, который демонстрирует быстрый темп роста, увеличиваясь на 73,3% ежегодно, что значительно опережает как общие инвестиции в искусственный интеллект, так и общий рост информационных технологий в целом [1].

IoT и микротаргетинг: реклама нового поколения. Дополнительно к анализу пользовательского поведения в цифровой среде все больше значение приобретает микротаргетинг через IoT. Подключаемые IoT-устройства, такие как фитнес-браслеты и умные колонки, собирают с пользователя данные, а маркетологи, с помощью машинного обучения и ИИ для аналитики этих данных могут предлагать гораздо более релевантную рекламу. Чем больше различных умных вещей присутствует в доме, тем легче ИИ-алгоритмам подобрать более персонализированную рекламу для пользователя [2].

Голосовой поиск и его влияние на маркетинг. Развитие микротаргетинга через IoT тесно связано с еще одним важным трендом – голосовым поиском. Общение с умными колонками происходит через голосовые команды, что делает этот формат поиска все более популярным. Хоть и голосовой поиск – это тренд, который сформировался давным-давно, он все равно очень сильно влияет на выдачу тех или иных продуктов или услуг. Очень важно этот момент учитывать контекстологом, людям, которые работают с контекстной рекламой. Из-за того, что запрос в текстовой форме может отличаться от голосового запроса, это влияет в целом на семантику и на то, как должны выглядеть объявления.

Zero-click-выдача: новая реальность контекстной рекламы. Меняющиеся привычки пользователей заставляют маркетологов пересматривать рекламные стратегии. Одним из ключевых трендов становится zero-click-выдача, которая делает контекстную рекламу еще более значимой. Zero-click-выдача – это релевантный ответ в поисковике, который позволяет пользователям не «ходить» по ссылкам, по сайтам и искать информацию самостоятельно. Вместо этого эта информация, которая выдается браузером, какая-то краткая сводка, сразу с четким ответом. Польза данного digital-тренда в том, что обычно браузер дает данную краткую информацию, краткий ответ, ссылаясь на какой-то сайт. И если, например, сайт будет с максимально точным, лаконичным ответом на запрос пользователя, все это можно заранее проверить и учесть в контенте сайта, он может попасть в выдачу, что увеличит органический трафик [3].

SERP-оптимизация: адаптация к новым форматам выдачи. Один из значимых трендов, связанных с изменениями в поисковой выдаче, – это трафик из SERP. SERP представляет собой страницу, сгенерированную поисковиком по запросу пользователя. Этот формат схож с zero-click выдачей, но включает не только текстовые ответы, но и изображения, видео, а также активную интеграцию карт, что позволяет пользователю получить исчерпывающий ответ. Рекламодателям необходимо адаптировать свои посадочные страницы и рекламные материалы, чтобы соответствовать запросам пользователей и повысить шансы на попадание в выдачу [4].

ИИ в рекламных системах: автоматизация создания объявлений. Еще одной тенденцией, набирающей обороты, является активное использование искусственного интеллекта в настройке рекламы. Рекламные системы, такие как Яндекс.Директ, предлагают автоматические шаблоны объявлений, включая сгенерированные заголовки, тексты и изображения, которые можно корректировать с помощью ИИ на основе предоставленных данных. Анализируя информацию о бизнесе, система подбирает наиболее релевантные варианты рекламных кампаний. Дополнительно доступен режим «Простой старт», позволяющий запускать рекламу даже без опыта – достаточно указать ссылку на сайт, заполнить анкету и выбрать бюджет, после чего система самостоятельно создаст объявления и покажет их целевой аудитории [5].

Отказ от cookie-файлов: новая эра контекстной рекламы. Отмечается также тенденция отказа от сбора cookie-файлов – это уже заявлено от официального лица Google, который отказывается от поддержки сторонних файлов cookie, вместо которых теперь будет контекстуальная реклама. Если раньше после захода на очередной сайт отурывалось предложение на то, чтобы принять cookie или же отклонить, теперь этого делать не нужно, с 2025 г. Google отказывается от cookie-файлов, и дальше он будет показывать рекламу в зависимости от контекста того или иного сайта или же запроса. Например, если сайт про фитнес-тематику, то логично, что на этом сайте можно размещать рекламу, связанную со всей это сферой: здоровья, спорта и т.д. [6].

Дополненная реальность (AR) в маркетинге: новый уровень взаимодействия. Кроме традиционных форматов рекламы, маркетологи все чаще используют технологии дополненной реальности (AR). Дополненная реальность открывает брендам двери к созданию захватывающего и интерактивного контента, что уже доказано успешными маркетинговыми кампаниями, использующими AR для повышения наглядности, вовлеченности и, как следствие, увеличения прибыли.

Маркетинг в дополненной реальности открывает брендам уникальную возможность интерактивного взаимодействия с аудиторией через мобильные приложения, позволяя визуализировать цифровой контент и предоставлять недостающую информацию о продукте, такую как размер и форма, также приложения AR дают пользователям возможность «потрогать» и рассмотреть продукт со всех сторон, создавая «вау-эффект» и запоминающееся впечатление благодаря новизне и интерактивности [7].

Заключение. Анализ показал, что digital-маркетинг в 2025 г. претерпевает значительные изменения под влиянием ИИ, персонализации и новых рекламных форматов. Компании, стремящиеся оставаться конкурентоспособными, должны адаптироваться к отказу от cookie, использовать микротаргетинг через IoT и учитывать изменения в поисковых алгоритмах.

Основные выводы исследования:

- Искусственный интеллект становится неотъемлемой частью маркетинга, обеспечивая персонализацию и автоматизацию.
- Контекстная реклама заменяет cookie-таргетинг, требуя новых стратегий адаптации.
- Видеоконтент и дополненная реальность становятся ключевыми инструментами вовлечения пользователей.
- Развитие IoT открывает новые возможности для микротаргетинга.
- Поисковые алгоритмы требуют переосмысления SEO-стратегий и оптимизации контента для zero-click-выдачи.

Перспективы дальнейших исследований включают анализ эффективности новых рекламных инструментов и разработку методик адаптации маркетинговых стратегий к изменяющимся условиям digital-среды.

ЛИТЕРАТУРА

1. Worldwide Spending on Artificial Intelligence Forecast to Reach $632 Billion in 2028, According to a New IDC Spending Guide [Электронный ресурс]. – Режим доступа: https://www.idc.com/getdoc.jsp?containerId=prUS52530724, свободный (дата обращения: 02.03.2025).

2. Какое будущее ждёт digital-маркетинг [Электронный ресурс]. – Режим доступа: https://altcraft.com/ru/blog/trendy-2025, свободный (дата обращения: 03.03.2025).

3. Understanding Zero Clicks: Insights from the 2024 Research! – Alpha SEO [Электронный ресурс]. – Режим доступа: https://alphaseopros.com/understanding-zero-clicks-insights-from-the-2024-research/, свободный (дата обращения: 05.03.2025).

4. SERP – что это такое и как формируется в Google и Яндексе | YAGLA [Электронный ресурс]. – Режим доступа: https://yagla.ru/blog/marketing/serp-chto-znachit-etot-termin-i-kak-on-svyazan-s-seo--2109m94955/, свободный (дата обращения: 06.03.2025).

5. Яндекс Директ: что это такое и как настроить в 2025 году [Электронный ресурс]. – Режим доступа: https://direct.yandex.ru/base/articles/chto-takoe-direkt-i-kak-nastroit, свободный (дата обращения: 10.03.2025).

6. Прекращение поддержки сторонних файлов cookie в Chrome: часто задаваемые вопросы – Справка – Google-реклама [Электронный ресурс]. – Режим доступа: https://support.google.com/google-ads/answer/14762010?hl=ru, свободный (дата обращения: 10.03.2025).

7. Маркетинг дополненной реальности: что это и как он работает / Хабр [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/487002/, свободный (дата обращения: 15.03.2025).

УДК 004.8

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ АРХИТЕКТУРЫ «ТРАНСФОРМЕР» ДЛЯ ОБРАБОТКИ СЛЕНГОВЫХ ВЫРАЖЕНИЙ

Е.А. Дрючин, студент

Научный руководитель И.Г. Боровской, зав. каф. ЭМИС, д.ф.-м.н.

г. Томск, ТУСУР, dryuchin01@gmail.com

Рассматривается применение нейросетевых моделей, основанных на архитектуре трансформер, для замены сленговых выражений на более понятные аналоги в текстах. Сравниваются модели BERT, RuBERT и RuBERT-tiny с акцентом на точность и скорость. Результаты показали, что RuBERT-tiny является наиболее подходящей моделью для данной задачи.

Ключевые слова: нейросетевые модели, трансформер, BERT, RuBERT, сленг, обработка текста.

В современном мире объем текстовой информации стремительно растет, что увеличивает потребность в автоматической обработке данных. Одной из главных проблем в этой сфере является распознавание и интерпретация сленговых выражений, которые широко применяются в интернет-общении, социальных сетях и неформальной речи. Их наличие в текстах усложняет работу алгоритмов обработки естественного языка, что делает актуальным поиск методов адаптации нейросетевых моделей к такому типу данных.

Обучение нейросетевых моделей представляет собой многоэтапный процесс. В данной работе рассматривается этап выбора модели, способной заменять сленговые выражения на более понятные аналоги.

Применение нейросетевых моделей обосновывается их способностью анализировать сложные языковые конструкции, выявлять закономерности и адаптироваться к особенностям языка. В отличие от традиционных методов, таких как словарные подходы или частотный анализ, нейросетевые модели, особенно архитектуры типа «трансформер», могут учитывать контекст употребления сленга и предлагать наиболее подходящие замены [1].

Анализ текстовых данных показал, что сленговые выражения используются в ограниченных контекстах, что делает их замену стандартными аналогами необходимой для корректного восприятия текста. Например, такие слова, как «кринж», «флекс» или «вайб», следует заменять более нейтральными синонимами в зависимости от контекста, что облегчает восприятие текста.

Существует несколько подходов к обработке текста, включая словарные методы, частотный анализ, N-граммы, а также нейросетевые методы, такие как рекуррентные нейронные сети и архитектуры «трансформер». Каждый метод имеет свои преимущества и недостатки, однако в данном исследовании акцент сделан на нейросетевые модели «трансформер».

Проведен сравнительный анализ обработки сленга с помощью предобученных нейросетевых моделей, таких как BERT, RuBERT и RuBERT-tiny. Сравнение проводилось по точности на тестовой выборке и времени обучения. Чтобы оптимизировать затраты на дообучение моделей, оно выполнялось на небольшом наборе данных, содержащем 20 пар «ключ-значение».

Например, модель BERT показала недостаточную (около 65%) для дальнейшего применения точность на русском языке из-за языкового барьера, поэтому принято решение проанализировать работу модели RuBERT, обученной на русскоязычных текстах. Эта модель продемонстрировала более высокую точность (около 86%), по сравнению с BERT.

Дополнительно была протестирована уменьшенная версия RuBERT – RuBERT-tiny. Несмотря на компактный размер, она показала схожую с родительской моделью точность, но при этом обучалась в 8 раз быстрее по сравнению с RuBERT. Все вышеперечисленные результаты представлены в таблице.

По итогам исследования модель RuBERT-tiny выбрана как наиболее эффективная по соотношению точности и скорости обработки. Полученные результаты могут стать основой для разработки нейросетевой модели, способной интерпретировать сленговые выражения и заменять их на более привычные и понятные формулировки, что повысит качество обработки текстовой информации.

Информация о результатах обучения моделей

Модель	Training Accuracy	Validation Accuracy	Среднее время эпохи, сек.	Общее время обучения, сек.
BERT	65%	64%	27	1010,45
RuBERT	86%	85%	28,5	1445,55
RuBERT-tiny	85%	83%	2,5	166,13

ЛИТЕРАТУРА

1. Как работают трансформеры? [Электронный ресурс]. – Режим доступа: https://huggingface.co/learn/nlp-course/ru/chapter1/4, свободный (дата обращения: 15.02.2025).

2. Жусип М.Н. Сравнение чат-ботов с использованием трансформеров и нейросетей: исследование применения архитектур GPT и BERT / М.Н. Жусип, Д.О. Жаксыбаев // Международный научный журнал «Вестник науки» (Уральск). – Сентябрь 2024. – Т. 2, № 9 (78). – С. 287–290.

3. Лезгян А.С. Автоматическое реферирование текстов: классификация, архитектуры, современные подходы и проблемы // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках (Саратов). – 2023. – № 1 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/avtomaticheskoe-referirovanie-tekstov-klassifikatsiya-arhitektury-sovremennye-podhody-i-problemy, свободный (дата обращения: 18.02.2025).

УДК 004.8

ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ГЕНЕРАЦИИ ЭКСПЕРТНЫХ ЗАКЛЮЧЕНИЙ

М.Г. Москалев, аспирант каф. КИБЭВС;

Т.Т. Газизов, зам. проректора по цифровизации, д.т.н. НИ ТПУ

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, moskalev@tspu.ru

Рассматривается применение технологий искусственного интеллекта для автоматизации генерации служебных записок и экспертных заключений на основе PDF-файлов научных статей. Проводится сравнительный анализ затрат на ручную обработку и автоматизированный подход, демонстрируя преимущества внедрения нейронных сетей, такие как сокращение времени обработки и затрат.

Ключевые слова: неструктурированные данные, нейронные сети, интеллектуальный анализ текста, извлечение информации, экономическая эффективность.

Современные цифровые системы сталкиваются с быстрым увеличением объёмов неструктурированной информации, такой как текстовые материалы, изображения и мультимедийные файлы. Согласно

исследованию IDC, доля неструктурированных данных в корпоративных и научных хранилищах превышает 80% [1]. Значительная часть таких данных представлена в формате PDF.

При проведении научных исследований возникает необходимость в регулярной генерации однотипных документов для подачи заявок на включение публикаций в университетские базы публикационной активности (ПА). Этот процесс включает в себя сбор и организацию информации о каждой публикации сотрудников, включая данные об авторах, аннотации, ключевые слова и другие важные сведения на основе текста статьи.

Эту задачу можно решать разными способами, в частности, есть подход, который использует библиотека Elibrary, предоставляя возможность обращаться к ней через API, получая необходимые данные, которые были заранее уже размечены [2]. Однако это не реализуется для англоязычных статей, а также для тех статей, которые еще не попали в открытый доступ. В таком случае необходимо распознавать текст статьи из формата pdf.

Одной из основных трудностей в обработке различных научных публикаций является отсутствие единого формата в различных изданиях. Местоположение искомых данных может значительно варьировать в разных журналах, что делает использование шаблонных методов извлечения затруднительным. Например, в некоторых изданиях данные об аффилиациях могут находиться на первой странице, а в других они располагаются в середине или конце текста статьи.

В отличие от шаблонных методов, использование методов искусственного интеллекта позволяет извлекать и классифицировать данные независимо от их формата и стиля представления [3]. Одним из востребованных и эффективных инструментов в сфере искусственного интеллекта является модель GPT, разработанная компанией OpenAI [4]. По состоянию на 1 марта 2025 г. наиболее популярными являются модели GPT-4 и GPT-4 Turbo. При этом объем контекстного окна модели GPT-4 Turbo в 4 раза больше, чем у GPT-4. Это может играть важную роль для обработки документов большого объема.

Обработка файла статьи происходит на языке Python с использованием библиотеки PyMyPDF [5]. Затем распознанный текст передается в API OpenaAI для выделения искомых данных. Запрос к GPT составлен таким образом, чтобы в ответ получить JSON-массив с данными. После того, как ответ будет получен, генерируются Word-файлы экспертного заключения и служебной записки.

Для оценки целесообразности использования нейросети в процессе генерации документов об ПА необходимо провести анализ эко-

номический эффективности. Исследование проводилось на примере Томского политехнического университета. В состав ТПУ входит 8 научных школ, для которых генерируются данные документы. В среднем каждая школа ежемесячно публикует 5 научных статей. Заработная плата сотрудника, ответственного за публикации, составляет 50 000 руб. Для обработки одной публикации и составления документов тратится 40 мин ручного труда. Скорость обработки и генерации с использованием нейросети занимает 1,5 мин, при стоимости 8,56 руб. за одну статью. Стоимость аренды хостинга для работы сервиса составляет 500 руб. в месяц. Также стоит учитывать стоимость работы программиста, который занимается созданием сервиса для интеграции с API и настройкой генерации создаваемых документов под требования университета. Его заработная плата составляет 60 000 рублей, работа длится 2 месяца. Можно посчитать точку безубыточности по формуле

$$50000 \times N = 120000 + 500 + 8{,}56 \times 40 \times N, \quad (1)$$

где N – точка безубыточности составит 2,426 месяца. Уже к 3 месяцу использования нейронной сети затраты на ее внедрение и эксплуатацию окупятся и станут экономически выгоднее, чем оплата труда сотрудника. На рис. 1 представлен график расчета годовых расходов с накоплением.

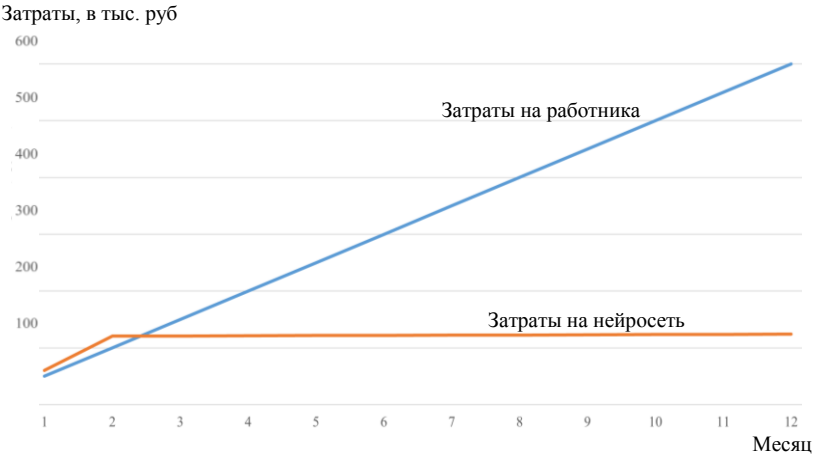

Рис. 1. Сравнение затрат на генерацию документации

Таким образом, в работе рассмотрен новый подход к генерации документов на основе использования OpenAI, сделан приблизительный расчет экономической выгоды от внедрения такого решения на

примере ТПУ. В частности, в 26,7 раза увеличилась скорость обработки публикаций и генерации служебной записки и экспертного заключения, а стоимость снижается в 146 раз. Годовая экономия при этом составляет 469 891 руб. по сравнению с ручным методом работы.

ЛИТЕРАТУРА

1. IDC. Future of industry ecosystems shared data and insights [Электронный ресурс]. – Режим доступа: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/, свободный (дата обращения: 16.02.2025).

2. Elibrary. Интерфейс программирования API [Электронный ресурс]. – Режим доступа: https://elibrary.ru/projects/api/api_info.asp, свободный (дата обращения: 18.02.2025).

3. Москалев М. Использование генеративных предобученных моделей для работы с неструктурированными данными / М. Москалев, Т.Т. Газизов // Природные и интеллектуальные ресурсы Сибири (СИБРЕСУРС-30–2024): 30-я Междунар. науч.-практ. конф., 19 ноября 2024 г., г. Томск, Россия: доклады (матер. конф.). – Томск: ТУСУР, 2024. – С. 89–93.

4. OpenAI [Электронный ресурс]. – Режим доступа: https://openai.com, свободный (дата обращения: 18.02.2025).

5. PyMyPDF [Электронный ресурс]. – Режим доступа: https://pymupdf.readthedocs.io/, свободный (дата обращения: 18.02.2025).

УДК 674.047.3:004.89

ПРОГНОЗ КАЧЕСТВА СУШКИ ПИЛОМАТЕРИАЛА НА БАЗЕ НЕЙРОННОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

О.А. Комогорова, студентка каф. ИТС; В.В. Гречушников, ст. преп. отд. электроэнергетики и электротехники

Научный руководитель А.А. Шилин, доцент каф. ИТС, д.т.н.

г. Томск, НИ ТГУ, НИ ТПУ, olga_komogorova01@mail.ru

Рассматривается проблема прогнозирования качества сушки пиломатериалов с использованием нейронной сети, обученной на основе математической модели технологического процесса. Предложен подход, позволяющий формализовать когнитивные знания экспертов-технологов и интегрировать их в базу данных для обучения нейронной сети. Особое внимание уделено процессу создания нейронной сети, формированию синаптических связей и выбору параметров, оказывающих наибольшее влияние на результат сушки. Результаты работы демонстрируют возможность повышения точности прогнозирования качества сушки за счёт комбинации экспертных знаний и современных методов машинного обучения.

Ключевые слова: технологический процесс, сушка пиломатриала, математическая модель, нейронные сети.

Некоторые технологические процессы, такие как сушка пиломатериалов, обладают настолько высокой сложностью и неоднозначностью, что их крайне трудно описать с помощью строгих математических моделей. Эти процессы зависят от множества факторов, включая качественные характеристики, которые не всегда поддаются точному измерению. В таких случаях ключевую роль играют опыт и интуитивные знания экспертов-технологов, накопленные за годы практики. Их глубокое понимание нюансов процесса позволяет эффективно управлять им, однако передать эти знания в виде четких алгоритмов или параметров для систем автоматизации – задача нетривиальная.

Тем не менее частичная формализация таких знаний, например, с использованием нейромоделей или путем детализации через уточняющие вопросы, открывает возможности для создания более точных и адаптивных моделей. Это особенно важно для разработки программного обеспечения и оптимизации технологических процессов. Когнитивные способности технолога-эксперта становятся незаменимым инструментом в управлении столь сложными процессами, как сушка пиломатериалов, где каждый параметр – от температуры до скорости циркуляции воздуха – требует тонкого баланса и глубокого понимания взаимосвязей. Таким образом, синтез опыта специалистов и современных технологий формализации знаний позволяет создать нейронные сети для прогноза качества технологического процесса.

В работе [1] была сформулирована проблема автоматической настройки параметров сушки, направленная на прогнозирование качества конечного продукта, а также предложен инновационный подход к её решению с использованием нейронной сети, дополненной когнитивными технологиями. Когнитивные способности технолога-эксперта, накопленные благодаря многолетнему опыту, систематизируются и формализуются в базу знаний. Эта база сформирована на основе метрик, которые извлекаются из заполненных опросных листов, предоставленных как заказчиком, так и технологом. Также метрики получаем из переходных процессов сушки пиломатериала. Примеры таких метрик, а также их взаимосвязь с результатами процесса сушки представлены в таблице.

Примеры метрик и их корреляция с результатами сушки пиломатериалов

Метрики	Результат сушки
Высокая начальная температура на 1-ом этапе сушки	Деформация древесины
Влажность доски 40%, температура сушки >60 °C	Появление плесени
Нагрев пиломатериала с естественной влажностью при температуре 67 °C	Удачно высушенная древесина

Нейронная сеть разработана с учётом параметров, взятых из технологической карты сушки пиломатериалов. Технология сушки вклю-

чает три стадии. На 1-й стадии влажность древесины составляет более 35%, на 2-й – достигается влажность доски более 25%, а на 3-й – снижается до уровня более 6%.

Ключевыми параметрами для формирования нейронной сети являются входные параметры: влажность воздуха, влажность доски, время сушки и температура. Вид такой нейронной сети представлен на рис. 1.

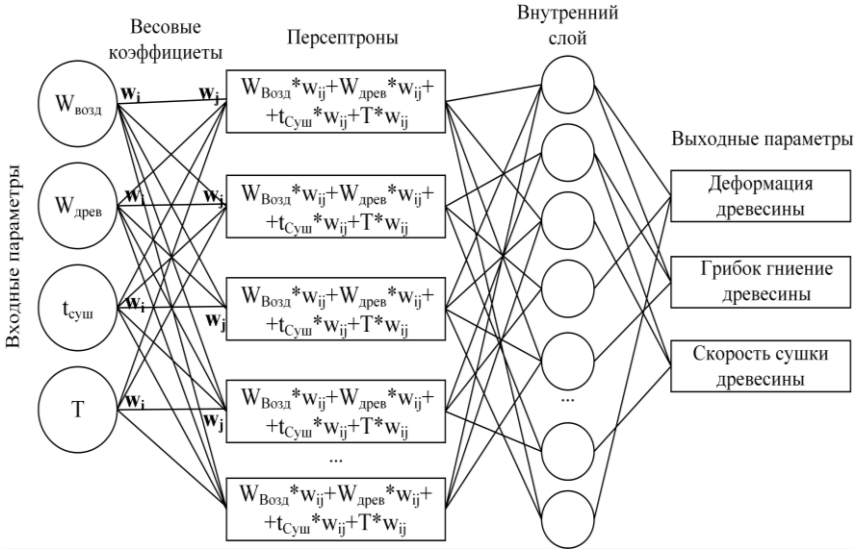

Рис. 1. Структура нейронной сети

Из этих признаков формируются персептроны, примеры которых представлены ниже:

1. Начальная температура воздуха на 1-м этапе сушки 70 °С, влажность доски 50%, время, влажность воздуха 80% может привести к заплесневению древесины.

2. Температура воздуха на второй стадии 75 °С, относительная влажность воздуха 60%, влажность доски 30%, время сушки 4 ч может привести к деформации древесины.

3. При влаготеплообработке температура воздуха 100 °С, относительная влажность 96%, время процесса 9 ч, влажность древесины перед началом влаготеплообработки приведёт к успешному результату техпроцесса.

Количество персептронных признаков может доходить до 40. Часть синапсов исключается на основании экспертной оценки техно-

лога, либо подтверждает отсутствие подобных связей в реальной системе, либо указывает на незначимость определённого параметра в конкретный цикл сушки. Поскольку вероятность существования таких связей стремится к нулю, их удаление позволяет оптимизировать архитектуру нейронной сети, ускорить процесс обучения и сохранить высокую точность и эффективность модели.

На рисунке имеются следующие обозначения: $W_{\text{возд}}$ – относительная влажность воздуха, $W_{\text{древ}}$ – влажность древесины, $t_{\text{суш}}$ – время сушки, T – температура воздуха в камере, w_{ij} – весовые коэффициенты, где $i \in [1;4] \bullet 3$, $j \in [1;40] \bullet 3$. Результатом обучения нейронной сети является набор параметров и результатов, хорошо коррелируемые между собой.

ЛИТЕРАТУРА

1. Комогорова О.А. Применение нейронных сетей в технологическом процессе сушки пиломатериала / О.А. Комогорова, В.В. Гречушников // VIII Всерос. науч.-практ. конф. с междунар. участием «Программная инженерия: современные тенденции развития и применения». – Курск: Университетская книга, 2024. – С. 52–56.

УДК 004.912

ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ В ИСХОДНОМ КОДЕ И СТАТИЧЕСКИЙ АНАЛИЗ

А.А. Ковшов, студент каф. БИС

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

Проект ГПО БИС-2501. Безопасность исходного кода

г. Томск, ТУСУР, andy.kovshov@gmail.com

Рассматривается задача выявления уязвимостей в исходном коде с использованием машинного обучения. Представлен обзор существующих подходов, решений и наборов данных, применяемых для анализа кода на наличие уязвимостей. Описаны методы машинного обучения, такие как логистическая регрессия, метод опорных векторов и глубокие нейронные сети, которые используются для классификации и обнаружения уязвимостей разного уровня сложности. Описаны эксперименты с авторским набором данных, который будет собран в процессе исследования. Описаны методологии и условия, необходимые для исследования, сделаны и зафиксированы некоторые гипотезы.

Ключевые слова: машинное обучение, исходный код, статический анализ, уязвимости, логистическая регрессия, метод опорных векторов, глубокие нейронные сети.

Современные системы программного обеспечения более сложны. Поэтому существует большая вероятность слабости исходных кодов. И в этом случае может произойти утечка данных, несанкционированный доступ и сбой в работе системы. Типичные методы статического анализа, такие как ручной аудит и использование инструментов статического анализа, обычно занимают слишком много времени и требуют человеческих ресурсов. Поэтому было бы удобно разработать автоматизированные методы анализа кода на основе машинного обучения для эффективного выявления уязвимостей с целью снижения рисков эксплуатации.

Существующие подходы и наборы данных. Исследования в области анализа кода на уязвимости с использованием машинного обучения находятся на стадии активного развития. В работах [1, 2] рассматриваются методы классификации кода на основе стилометрических признаков, таких как метрики Холстеда и цикломатическая сложность. Эти методы позволяют наиболее точно выявлять аномалии в структуре входного кода, которые могут указывать на наличие уязвимостей. В работах [3, 4] применяются методы машинного обучения, такие как логистическая регрессия и метод опорных векторов, для классификации кода на безопасный и уязвимый. Для векторизации кода используются методы TF-IDF и Word2Vec.

В исследованиях [5, 6] используются глубокие нейронные сети, такие как LSTM и CNN, для анализа последовательностей кода и выявления сложных уязвимостей. Эти методы демонстрируют высокую точность, но требуют значительных вычислительных ресурсов и большого объема данных для обучения. При отсутствии любого из компонентов при работе с этими моделями есть риск потерять часы времени на обучение, но не получить результата. В работе [7] предложен комбинированный подход, объединяющий стилометрические признаки и глубокие нейронные сети, что позволяет достичь высокой точности классификации.

Одним из ключевых ограничений в данной области является отсутствие наборов данных, позволяющих рассмотреть все возможные случаи и вариации уязвимостей. В исследованиях используются датасеты, такие как Juliet Test Suite [8], NVD [9] и SARD [10], которые содержат примеры кода с известными уязвимостями. Однако эти наборы данных часто ограничены по объему и разнообразию, что затрудняет обучение моделей машинного обучения. В работе [11] показан набор данных, содержащий более 50 000 примеров кода, некоторые из которых содержат уязвимости на различных языках программирования, такое количество данных позволит лучше обучить с нуля или дообучить модель для нахождения уязвимостей в исходном коде.

Планируемые эксперименты. Для проведения исследования оценки эффективности методов машинного обучения в задаче статического анализа и выявления уязвимостей в исходном коде планируется провести следующие эксперименты. Эксперименты будут направлены на сравнение всех описанных моделей машинного обучения, таких как логистическая регрессия, метод опорных векторов (SVM) и глубокие нейронные сети (LSTM). Также по итогам экспериментов необходимо ответить на основе полученных оценок на вопрос, применимы ли методы машинного обучения для задачи статического анализа и выявления уязвимостей в исходном коде?

Подготовка набора данных. Для проведения экспериментов необходимо создать набор данных, в котором будут представлены примеры кода как с уязвимостями, так и без них. Набор данных будет состоять из примеров кодов на языке Python. Преимущество Python – широкая используемость этого языка и простота нахождения подходящих кодов. Датасет будет включать в себя следующие типы уязвимостей: SQL-инъекции, XSS (межсайтовый скриптинг), уязвимости переполнения буфера, неправильная обработка исключений и т.д. Типы уязвимостей могут быть отредактированы в процессе сбора данных. Для каждого кода будет целевой показатель, который будет с помощью метки показывать – есть ли уязвимости в этом коде. Для получения лучших показателей обучения набор данных будет сбалансирован равным количеством экземпляров каждого класса.

Выбор модели машинного обучения. Для полного проведения эксперимента необходимо рассмотреть три модели машинного обучения.

Первая – логистическая регрессия. Эта модель лучше используется для анализа простых уязвимостей и уязвимостей с простой структурой, таких как SQL-инъекции. Логистическая регрессия является линейной моделью, что значит, что эта модель лучше решает задачи, которые возможно решить с помощью линейных зависимостей.

Вторая – метод опорных векторов (SVM). SVM будет применяться для анализа более сложных уязвимостей, способность работать с нелинейными данными позволяет модели находить их. SVM строит плоскость, которая разделяет классы, что позволяет более точно разделять самые сложные данные, такие как уязвимости, замаскированные под легитимные операции.

Третья – глубокая нейронная сеть (LSTM). LSTM может использоваться для анализа любых типов данных и типов уязвимостей, благодаря ее способности анализировать и выявлять сложные зависимости. LSTM особо полезна, так как эта модель может запоминать зависимости в данных, что позволит находить уязвимости в разных функциях или модулях кода.

Методология проведения экспериментов. Эксперименты будут проводиться в несколько этапов.

Первый этап – это предобработка данных. Код будет преобразован в удобный формат для каждой модели.

Второй этап – обучение моделей. Данные будут разбиты на тренировочный и тестовый набор в соотношении 80 на 20%. Каждая модель будет обучена на тренировочной выборке. Гиперпараметры будут оптимизированы методом GridSearchCV.

Третьим этапом будет оценка качества моделей на тестовом наборе данных с помощью метрик Accuracy, Precision, Recall, F1-score.

Четвертым этапом будет итоговый анализ результатов, в процессе которого необходимо понять, обучается ли модель, какая модель лучше решает задачу, проследить ложные срабатывания и остановиться на итоговом варианте модели.

Планируемые эксперименты позволят ответить на все поставленные вопросы в рамках исследования, оценить эффективность методов машинного обучения в задаче статического анализа и выявления уязвимостей в исходном коде и решить те задачи, которые могут дополнительно возникнуть в процессе проведения. Результаты этих экспериментов будут использованы для разработки более точной и надежной системы анализа кода, которая сможет применяться в реальных условиях для повышения безопасности программных систем. Возможна интеграция с другими сервисами, занимающимися похожими задачами, либо с сервисами, помогающими обработать исходный код по-другому.

ЛИТЕРАТУРА

1. The «Code» of Ethics: A Holistic Audit of AI Code Generators / W. Ma, Y. Song, M. Xue, S. Wen, Y. Xiang // IEEE Transactions on Dependable and Secure Computing – 2024. – Vol. 21, No. 5. – P. 4997–5013.

2. Whodunit: Classifying Code as Human Authored or GPT-4 Generated. A case study on CodeChef problems / O.J. Idialu, N.S. Mathews, R. Maipradit, J.M. Atlee // Proceedings of the 21st International Conference on Mining Software Repositories – 2024. – P. 394–406.

3. ChatGPT Code Detection: Techniques for Uncovering the Source of Code / M. Oedingen, R. Denz, R. Engelhardt, M. Hammer // AI Journal. – 2024. – Vol. 5, No. 3. – P. 1066–1094.

4. Detecting ChatGPT-Generated Code Submissions in a CS1 Course Using Machine Learning Models / M. Hoq, Y. Shi, J. Leinonen, D. Babalola // Proceedings of the 55th ACM Technical Symposium on Computer Science Education – 2024. – P. 526–532.

5. Discriminating Human-authored from ChatGPT-Generated Code Via Discernable Feature Analysis / K. Li, S. Hong, C. Fu, Y. Zhang, M. Liu // IEEE

34th International Symposium on Software Reliability Engineering Workshops – 2023. – P. 120–127.

6. GPTSniffer: A CodeBERT-based classifier to detect source code written by ChatGPT / P. Nguyen, J. Rocco, C. Sipio, R. Rubei // Journal of Systems and Software. – 2024. – Vol. 214.

7. Bukhari S.A. Issues in Detection of AI-Generated Source Code: Electrical Engineering: The Requirements for the degree of Masters of Science. – Calgary: University of Calgary, 2024. – 102 p.

8. Sjoerd S. The Detection of AI Generated Coding Content: Information and Computing Science: The Requirements for the degree of Masters of Science. – Utrecht: Utrecht University, 2024. – 75 p.

9. Xu Z. Detecting AI-Generated Code Assignments Using Perplexity of Large Language Models / Z. Xu, V. Sheng // Proceedings of the AAAI Conference on Artificial Intelligence. – 2024. – P. 23155–23162.

10. Juliet Test Suite for C/C++ and Java // NIST. – 2023.

11. National Vulnerability Database (NVD) // NIST. – 2024.

12. Software Assurance Reference Dataset (SARD) // NIST. – 2024.

УДК 004.896

К ВОПРОСУ О ПРИМЕНЕНИИ БПЛА НА ЛИНИИ БОЕВОГО СОПРИКОСНОВЕНИЯ БЕЗ КАНАЛА УПРАВЛЕНИЯ, ИСПОЛЬЗУЯ СЕТИ ТИПА GAN

И.Р. Извеков, А.С. Кузьмин,

С.Г. Кунгурцев, операторы роты (научной)

Научный руководитель Н.А. Васильев, зам. нач. научно-исследовательского центра

г. Санкт-Петербург, Военная орденов Жукова и Ленина Краснознаменная академия связи им. Маршала Советского Союза С.М. Буденного МО РФ, vasn2020@mail.ru

Рассматривается применение беспилотных летательных аппаратов на линии боевого соприкосновения в условиях отсутствия канала управления. Описаны принципы работы нейронных сетей типа GAN, их интеграция в системы управления БПЛА, а также проблемы и ограничения, которые возникают при их применении.

Ключевые слова: беспилотные летательные аппараты, нейронные сети, генеративные состязательные сети.

Современные военные конфликты характеризуются активным использованием беспилотных летательных аппаратов (БПЛА) для решения широкого спектра задач от разведки и наблюдения до нанесения точных ударов. Однако традиционные БПЛА требуют наличия канала управления, что делает их уязвимыми для радиоэлектронной борьбы (РЭБ) и перехвата сигнала. В связи с этим возникает необхо-

димость в разработке автономных систем, способных функционировать без постоянного контроля оператора. Одним из направлений в этой области является использование генеративно-состязательных сетей (GAN) для создания БПЛА с искусственным интеллектом, способных принимать решения в реальном времени без использования канала связи.

Принцип работы GAN. Принцип работы GAN основан на соревновательности двух нейронных сетей. Генератор и дискриминатор обучаются вместе и улучшают друг друга в процессе обучения. Генератор отвечает за создание синтетических данных, пытаясь обмануть дискриминатор, чтобы тот принял сгенерированные данные за реальные. Дискриминатор, в свою очередь, обучается различать реальные данные от сгенерированных [1].

Проблемы использования БПЛА с каналом управления. Традиционные БПЛА зависят от каналов связи для передачи данных и получения команд от операторов, вследствие чего дрон становится уязвим для РЭБ, так как у противника есть возможность подавить или перехватить сигнал. Также необходимо учитывать задержки в передаче данных, которые возникают в условиях интенсивного боевого соприкосновения и могут привести к ошибке или потере личного состава. Для управления дронами очень часто требуется несколько операторов, что является затратным на поле боя, а также не позволяет использовать БПЛА в ситуациях, когда противник находится в непосредственной близости к операторам.

Применение GAN в автономных БПЛА. Нейронные сети способны обрабатывать данные практически в режиме реального времени, вследствие чего реакция на какие-либо действия происходят намного быстрее, однако стоит учитывать разницу в скорости обработки входящих данных нейронной сетью и реакцией оператора.

БПЛА с искусственным интеллектом имеют устойчивость к РЭБ, так как в аппаратуре отсутствует канал управления, основные уязвимости становятся недоступными для перехвата управления и подавления дрона.

Нейронные сети на основе GAN могут предложить оптимальные тактические решения: выбор точки атаки или уклонения от преследования.

В условиях боевого соприкосновения ситуация меняется мгновенно. GAN позволяет БПЛА адаптироваться к новым условиям, например, обходить зоны с активной РЭБ или изменять маршрут при обнаружении угроз.

GAN могут быть обучены на большом объеме данных для распознавания целей – это позволяет БПЛА самостоятельно идентифицировать и классифицировать объекты без участия оператора.

Ограничения, накладываемые при использовании GAN в БПЛА. Обучение и работа GAN требуют значительных мощностей. Данное ограничение накладно для производство БПЛА: увеличивает стоимость, компактность. Ошибки в работе нейронных сетей могут привести к критическим последствиям, поэтому необходимы механизмы контроля и дублирования, следовательно, полный отказ от операторов в ближайшем будущем тяжело осуществимо; автономные системы, способные принимать решения о применении силы по отношению к человеку, требуют четкого регулирования и контроля.

Заключение. Применение генеративно-состязательных сетей в БПЛА открывает новые возможности для создания автономных систем, способных эффективно функционировать на линии боевого соприкосновения без канала управления. Данное направление имеет большой потенциал для повышения эффективности и безопасности военных операций. Внедрение подобных технологий в ближайшем будущем станет важным шагом в эволюции военной техники и тактики ведения боевых действий.

ЛИТЕРАТУРА

1. Картер Д. Нейросети. Генерация изображений // Нейросети. – 2023. – 304 с.

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

3. Литвин Ю.И. Основы применения беспилотных летательных аппаратов в артиллерийских подразделениях / Ю.И. Литвин, Н.В. Марчук, В.Е. Уткин. – М.: КНОРУС, 2025. – 128 с.

4. Бобков А.В. Системы распознавания образов: учеб. пособие. – М.: МГТУ им. Н.Э. Баумана, 2018 – 187 с.

УДК 004.522, 004.934.2, 004.032.26

КЛАССИФИКАЦИЯ РАЗЛИЧНЫХ МЕТОДОВ ГЕНЕРАЦИИ РЕЧИ С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ

С.А. Литовкин, аспирант каф. КСУП

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

Выполнена классификация различных методов генерирования речи с помощью средств машинного обучения.

Ключевые слова: классификация, машинное обучение, сгенерированная речь, нейронные сети, набор данных.

С помощью сгенерированной речи злоумышленники могут выдать себя за другую личность для получения выгоды или посеять хаос в информационном поле. Существует множество исследований,

направленных на классификацию сгенерированной речи, но почти все они объединяют сгенерированную речь в один класс, что не позволяет изучить насколько качественно классифицируются отдельные методы генерации речи. Целью данной работы является изучение классификации нескольких методов генерации речи.

В качестве данных для классификации использовался набор данных MLAAD [1], который был опубликован во второй половине 2024 г. Данный набор данных содержит в себе 38 различных языков, для которых генерировалась речь с помощью 82 различных методов синтезирования речи. В общем набор данных содержит 378 ч сгенерированной речи, для каждого языка было сгенерировано не менее 9 ч. Все аудио закодированы в формате «.wav» с частотой дискретизации 22050 Гц.

В качестве методов классификации речи использовалось 3 метода машинного обучения, а именно: Random Forest (RF) [2], K-Nearest Neighbors (RNN) [3] и Support Vector Machine (SVM) [4]. Также использовалось 2 архитектуры сверточных нейронных сетей: ResNet101 [5] и Alex-Net [6]. В качестве данных для обучения использовались изображения мел-частотных кепстральных коэффициентов. Использование изображений в качестве входных данных позволит привести к одному формату, вне зависимости от длины аудиозаписи. Пример входных данных представлен на рис. 1.

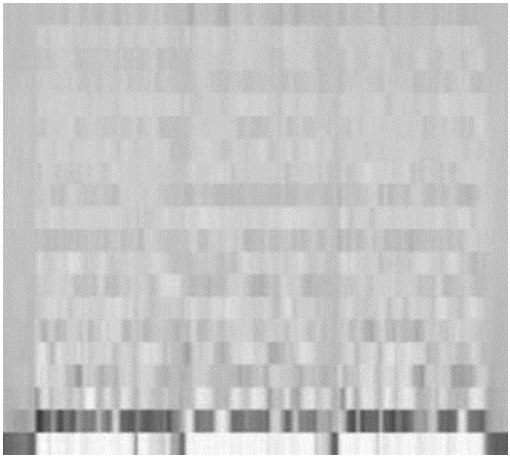

Рис. 1. Пример входных данных

Для оценивания точности классификации использовалась метрика F1-мера. В качестве методов для классификации использовались:

griffin_lim, facebook_mms-tts, OpenVoiceV2, multilingual_bark, multilingual_xtts_v2, tacotron2-DDC. Все рассматриваемые методы генерации речи основываются на методе преобразования текста в речь. Для классификации использовалось 1 200 сгенерированных аудиозаписей. Результаты классификации сгенерированной речи для различных методов генерации представлены в таблице.

Результаты классификации для различных методов генерации

Метод генерации	Методы классификации				
	RF	KNN	SVM	ResNet101	Alex-Net
griffin_lim	0,00	0,39	0,42	0,00	0,01
facebook_mms-tts	0,60	0,54	0,81	0,61	0,82
OpenVoiceV2	0,44	0,49	0,51	0,08	0,20
multilingual_bark	0	0,31	0,01	0,11	0,24
multilingual_xtts_v2	0,25	0,19	0,58	0,43	0,57
tacotron2-DDC	0,55	0,72	0,69	0,54	0,60
Итоговая точность	0,41	0,44	0,56	0,41	0,52

Анализируя полученные результаты, заметно, что не все методы генерации речи одинаково хорошо классифицируются, multilingual_bark имеет крайне низкую точность классификации при использовании RF и SVM. Сверточные нейронные сети показывают низкие результаты классификации, для большинства методов генерации речи F1-мера не превосходит 0,5. Хуже всего классифицируются методы griffin_lim и multilingual_bark, ни один из методов классификации не смог получить результаты больше 0,5. Низкие результаты классификации могут быть связаны с неправильным выбором способа обработки входных параметров, поэтому в дальнейшем будут рассматриваться другие методы обработки входных данных, а также другие методы классификации.

Заключение. В результате данной работы была проведена классификация различных методов генерирования речи и проанализированы полученные результаты.

ЛИТЕРАТУРА

1. Müller N.M. et al. Mlaad: The multi-language audio anti-spoofing dataset // 2024 International Joint Conference on Neural Networks (IJCNN). – IEEE, 2024. – P. 1–7.

2. Breiman L. Random forests // Machine learning. – 2001. – Vol. 45. – P. 5–32.

3. Fix E. Discriminatory analysis: nonparametric discrimination, consistency properties. – USAF school of Aviation Medicine, 1985. – Vol. 1.

4. Platt J. et al. Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods // Advances in large margin classifiers. – 1999. – Vol. 10, No. 3. – P. 61–74.

5. He K. et al. Deep residual learning for image recognition // Proceedings of the IEEE conference on computer vision and pattern recognition. – 2016. – P. 770–778.

6. Krizhevsky A. Imagenet classification with deep convolutional neural networks / A. Krizhevsky, I. Sutskever, G.E. Hinton // Advances in neural information processing systems. – 2012. – Vol. 25.

УДК 004.89:372.881.111.1

ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ ГЕНЕРАЦИИ ТЕСТОВ ПО ИНОСТРАННОМУ ЯЗЫКУ С ИНТЕГРАЦИЕЙ В LMS MOODLE

О.Р. Макаров, студент каф. АСУ

Научный руководитель А.А. Захарова, проф. каф. АСУ, д.т.н.

г. Томск, ТУСУР, tripp0@yandex.ru

Разработка банка тестовых заданий по иностранному языку является важной задачей для оценки прогресса студентов и оптимизации учебного процесса. В данной работе предложено веб-приложение для автоматизированной генерации тестов по английскому языку с возможностью их экспорта в LMS Moodle. Использование генеративных языковых моделей и сервисов синтеза речи позволяет создавать уникальные задания с минимальными временными затратами со стороны преподавателей. Реализация веб-приложения основана на API Deepseek для генерации текстов и KokoroTTS для синтеза речи, а взаимодействие с пользователем осуществляется через веб-интерфейс на базе Flask.

Ключевые слова: генеративный искусственный интеллект, английский язык, образование, генерация тестов, автоматизация, Moodle, веб-приложение.

Необходимость формирования банка заданий по английскому языку на большое число тем для оценки прогресса и достижения образовательных результатов обучения определяет актуальность данной работы. Практическая значимость данной работы состоит в сокращении нагрузки на преподавателей благодаря автоматизации создания типовых заданий по дисциплине «английский язык» и их экспорту в LMS Moodle.

Развитие в области генеративного искусственного интеллекта привело к появлению большого числа инструментов, которые имеют потенциал обогащения учебного процесса при условии их активного и корректного внедрения. Эффективное использование этих инструментов может рассматриваться как конкурентное преимущество учебного заведения в достижении образовательных целей [1].

Цель работы – разработать приложение, которое позволит объединить полезные для работы преподавателя инструменты в единую систему и на практике упростить процесс создания самих заданий и их экспорта в систему Moodle. Таким образом, преподаватель не будет исключен из рабочего процесса, а, наоборот, получит возможность уделить большее внимание качеству обучения и персонализировать его благодаря исключению значительных временных затрат в процессах подготовки материала и создания заданий.

В данный момент существуют пользовательские и официальные плагины для системы Moodle, отчасти предоставляющие данный функционал, например, создание с помощью больших языковых моделей заданий по заданному тексту, банка заданий по файлам курса, автоматизация генерации изображений. Однако они не специализированы на конкретной области применения, что существенно влияет на качество их работы, не автоматизируют в достаточной степени процесс, а также часть из них более не поддерживается [2].

Разрабатываемое приложение получает от пользователя данные через веб-интерфейс, заполняет ими готовые шаблоны, взаимодействует по API с сервисами, предоставляющими функционал большой языковой модели, синтеза речи и из полученных ответов создает задания в нужном формате.

Использование больших языковых моделей позволяет применить их понимание синтаксиса и семантики человеческого языка на практике в задачах, для которых эти аспекты являются наиболее важными. Таким образом, существует возможность их использования для создания уникальных текстов заданного формата (статья, новость, письмо) по указанной теме с использованием заданного списка ключевых слов.

Важными аспектами работы с языковой моделью являются правильная формулировка запросов для повышения качества результата с учетом минимизация числа используемых токенов и стандартизации формата запросов для увеличения вероятности кэш-попадания. От этого зависят вычислительные расходы поставщика услуги, что по ценовой политике влияет на стоимость использования инструмента пользователем. Основное преимущество приложения состоит в том, что оно автоматически будет использовать заранее подготовленные, проверенные шаблоны для достижения лучшего результата.

Использование сервиса для синтеза речи предоставляет уникальную возможность создания заданий на прослушивание качественной иностранной речи, ресурс которой по отдельно выбранной теме обычно ограничен.

Конкретные решения могут отличаться, однако в прототипе веб-приложения используется формат API от OpenAI, который поддержи-

вает большинство разработчиков нейросетей, и используются по API сервисы Deepseek (генерация текста) [3] и KokoroTTS (синтез английской речи) [4]. Результаты их работы обрабатываются алгоритмами и используются для заполнения шаблонов, например, в формате Moodle XML, поддерживаемом LMS Moodle.

Ввод данных пользователем происходит через веб-страницу создаваемым приложением на Flask. В ней указаны необходимые поля для заполнения, включающие в себя: тему теста, формат и ключевые слова для генерации текста (возможно также использование существующего), выбор представления текста в формате аудирования.

Заключение. Разработанное веб-приложение автоматизирует процесс генерации заданий по иностранному языку с интеграцией в LMS Moodle, снижая нагрузку на преподавателей. Применение языковых моделей и синтеза речи позволяет быстро создать новые материалы для банка заданий. В дальнейшем планируется расширение функционала и проверка применения в образовательной среде.

ЛИТЕРАТУРА

1. Нейросети и генеративный ИИ в высшем образовании: международный опыт и российская практика [Электронный ресурс]. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/neyroseti-generativnyy-ii-v-vysshem-obrazovanii-mezhdunarodnyy-opyt-i-rossiyskaya-praktika, свободный (дата обращения: 28.02.2025).

2. Moodle Plugins directory [Электронный ресурс]. – Режим доступа: https://moodle.org/plugins, свободный (дата обращения: 01.03.2025).

3. Deepseek [Электронный ресурс]. – Режим доступа: https://www.deepseek.com, свободный (дата обращения: 02.03.2025).

4. Kokoro TTS: Advanced Text-to-Speech AI with Best Efficiency [Электронный ресурс]. – Режим доступа: https://kokorotts.com, свободный (дата обращения: 02.03.2025).

УДК 004.8

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ДЛЯ РЕАЛИЗАЦИИ ЦИФРОВОГО АССИСТЕНТА ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Г.Р. Нурдавлетов, студент

Научный руководитель Е.А. Шельмина, доц. каф. ЭМИС, к.ф.-м.н.

г. Томск, ТУСУР, nurd_galim@mail.ru

Изучено применение больших языковых моделей (LLM) для автоматизации задач, анализа данных и общения с пользователями. Рассмотрены модели, такие как ruT5-small, ruT5-base, ruBERt-base, sbert_large_nlu_ru и др., эффективно работающие при ограниченных

вычислительных ресурсах. Результаты исследования направлены на создание системы технической поддержки студентов, что улучшит доступность и эффективность образовательных услуг.
Ключевые слова: большие языковые модели, LLM, GPT, ruT5-small, ruT5-base, ruBERt-base, sbert_large_nlu_ru, LLaMA-1B, BLOOM-560M, Grok-1, автоматизация, обработка текста, системы технической поддержки, техническая поддержка.

Современный мир стремительно меняется, и технологии искусственного интеллекта становятся неотъемлемой частью нашей повседневной жизни. Большие языковые модели (LLM) играют ключевую роль в цифровой трансформации, предоставляя инновационные решения для автоматизации задач, анализа данных и общения с пользователями. Развитие LLM направлено на повышение эффективности работы с информацией, улучшение качества сервисов и создание более интеллектуальных систем взаимодействия [1].

Разграничение имеющихся ресурсов является одной из важнейших и одновременно с этим непростой задачей, результат выполнения которой позволяет выделить среди множества существующих языковых моделей удовлетворяющую следующим требованиям: поддержка русского языка в предобученной модели и низкие системные требования к системе, на базе которой будет проводиться дообучение и дальнейшая работа языковой модели.

Большие языковые модели обучаются на основе методов машинного и глубокого обучения. Первый подход позволяет анализировать данные, выявлять закономерности и делать прогнозы без строгих инструкций. Второй, имитируя работу человеческого мозга, дает возможность обрабатывать сложные структуры, включая изображения, текст и звук.

В процессе обучения эти параметры изменяются, что позволяет системе не только понимать информацию, но и прогнозировать и генерировать текст. Их работа строится по принципу последовательного предсказания слов: сначала определяется наиболее вероятное следующее слово, затем оно добавляется в текст, и процесс повторяется до формирования связного результата, а встроенные фильтры помогают контролировать генерируемый контент и предотвращать появление вредоносной информации. Сегодня LLM применяются в самых разных областях – от написания текстов до программирования. Однако поскольку их работа основана на вероятностных прогнозах, они не всегда дают точные результаты [2].

Одной из самых известных LLM является GPT. Эта модель широко применяется благодаря своей гибкости, способности адаптироваться к конкретным задачам и удобству взаимодействия с пользова-

телем. GPT и другие LLM – это мощные инструменты, способные трансформировать различные сферы деятельности. Однако их использование требует осознанного и ответственного подхода для минимизации возможных рисков [3].

При выборе языковой модели в условиях ограниченных ресурсов важно учитывать несколько факторов. Компактные версии (small или base) требуют меньше памяти и времени на обучение. Критично, чтобы модель обладала предобученными знаниями и могла эффективно адаптироваться к новым данным. Значительную роль играет поддержка русского языка, поскольку от этого зависит качество обработки текстов. Также предпочтение часто отдается открытым моделям, поскольку они позволяют гибко настраивать систему под конкретные задачи. Вышеперечисленные критерии представлены в таблице (отсутствующая информация помечена знаком «тире»).

Заявленные характеристики языковых моделей

Название	RAM	GPU	CPU	Кол-во параметров	Предобученный размер	Поддержка русского языка
ruT5-small	16 GB	8 GB	4 cores	64,6 M	6 GB	Да
ruT5-base	–	–	–	222 M	–	Да
ruBERt-base	–	–	–	178 M	–	Да
sbert_large_nlu_ru	–	–	–	427 M	–	Да
LLaMA-1B	–	–	–	1,24 B	–	Нет
BLOOM-560M	2.4GB	–	–	559 M	2,4 GB	Нет
Grok-1	–	Multi-GPU	–	314B	296GB	Да

На основе данных, представленных в таблице, для дальнейшего исследования выбраны модели ruT5-small, ruT5-base, ruBERt-base и sbert_large_nlu_ru. На основе уже имеющихся данных применение этих моделей обосновано их использованием для обработки текстовых данных на русском языке и на основе информации об их практическом применении [4].

Стоит отметить, что ранее упоминалась языковая модель GPT, но коммерческая версия в данном исследовании не рассматривается из-за условий лицензирования.

По итогам проведенного анализа отобрано несколько языковых моделей для тестирования в условиях ограниченных вычислительных ресурсов. Далее выбранная по итогам тестирования модель будет использоваться для создания системы технической поддержки студентов. Внедрение такой системы повысит уровень обслуживания сту-

дентов, снизит нагрузку на преподавателей и сотрудников службы поддержки, а также улучшит доступность информации для обучающихся.

ЛИТЕРАТУРА

1. Вакушин А.А. Применение больших языковых моделей в имитационном моделировании / А.А. Вакушин, Б.И. Клебанов // Электронный научный журнал «Инженерный вестник Дона» (Ростов-на-Дону). – 2024. – № 2 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/primenenie-bolshih-yazykovyh-modeley-v-imitatsionnom-modelirovanii свободный (дата обращения: 15.02.2025).

2. Чунгулова Г.К. Возможности и проблемы больших языковых моделей в образовании на примере ChatGPT / Г.К. Чунгулова, Э.Н. Оразалиева // Наука и реальность. – 2024. – № 4 (20). – С. 85–91.

3. Ашихмин Е.Г. Опыт применения больших языковых моделей для анализа социологических данных, полученных в результате интервью о восприятии студентами предпринимательской деятельности / Е.Г. Ашихмин, В.В. Левченко, Г.И. Селеткова // Цифровая социология. – 2024. – Т. 7, № 3. – С. 4–14.

4. Кравченко Ю.А. Модифицированный метод устранения неоднозначности смысла слов, основанный на методах распределенного представления / Ю.А. Кравченко, Мансур Али Махмуд, Мохаммад Жуман Хуссайн // Известия Южного федерального университета. Технические науки (Ростов-на-Дону). – 2021. – № 3 (220) – С. 92–101.

УДК 004.056.53

ДВУМЕРНОЕ ПРЕДСТАВЛЕНИЕ КЛАВИАТУРНОГО ПОЧЕРКА ДЛЯ НЕЙРОСЕТЕВОГО АНАЛИЗА

Е.П. Орловский, аспирант каф. КИБЭВС

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС

г. Томск, ТУСУР, orlovskiizhenya@gmail.com

В современном мире биометрические методы аутентификации становятся все более востребованными благодаря своей надежности и удобству. Одним из таких методов является анализ клавиатурного почерка, который основывается на уникальных временных характеристиках нажатия клавиш пользователем. В последние годы для решения задач анализа клавиатурного почерка активно применяются методы глубокого обучения, в частности, сверточные нейронные сети (CNN). Однако для эффективного использования CNN необходимо представить временные данные в виде двумерных структур, что позволяет учитывать пространственные зависимости и улучшать качество анализа.

Ключевые слова: клавиатурный почерк, матрица переходов, Gramian Angular Field, Markov Transition Field.

Для исследования возможностей CNN в задаче анализа клавиатурного почерка [1] были использованы данные из открытого набора

KeyRecs: Keystroke Dynamics Dataset [2]. Этот набор содержит данные в секундах между нажатием (D) или отпусканием (U) клавиши 2 относительно клавиши 1, которые формируют уникальный клавиатурный почерк пользователя.

Однако CNN, изначально разработанные для обработки изображений, требуют преобразования временных данных в двумерные представления. В ходе исследования были предложены три основных метода такого преобразования: матрица переходов, Gramian Angular Field (GAF) и Markov Transition Field (MTF).

Матрица переходов представляет собой квадратную матрицу размером 50×50, в которой как строки, так и столбцы соответствуют 50 различным клавишам. Эти клавиши включают в себя все буквы английского алфавита, цифры, а также определенные символы и специальные клавиши. Таким образом, каждая ячейка матрицы представляет собой уникальную пару клавиш, где пересечение строки и столбца соответствует переходу между двумя конкретными клавишами.

Для анализа временных характеристик переходов между клавишами используется мультиканальная структура данных. В частности, для каждой пары клавиш измеряются и фиксируются пять различных временных характеристик, таких как, например, время между нажатиями или длительность удержания клавиши. Эти характеристики формируют пять независимых каналов, что позволяет более детально описать динамику взаимодействия пользователя с клавиатурой.

Если какая-либо клавиша или пара клавиш используется более одного раза в процессе анализа, временные характеристики для этой клавиши или пары клавиш усредняются. Это позволяет сгладить возможные колебания и получить более репрезентативное значение для соответствующего элемента матрицы. Таким образом, матрица переходов отражает обобщенные временные параметры для всех возможных комбинаций клавиш (рис. 1).

Gramian Angular Field (GAF) [3] представляет собой более сложный метод, который преобразует временные данные в изображение, сохраняя временные зависимости. GAF использует полярную систему координат для кодирования временных рядов, что позволяет сохранить информацию о временных интервалах между событиями. В контексте анализа клавиатурного почерка GAF может быть полезен для учета длительности нажатий и пауз между ними, что является важной характеристикой индивидуального стиля пользователя.

Этот метод был успешно применен в различных задачах анализа временных рядов, включая обработку сигналов и биометрическую аутентификацию.

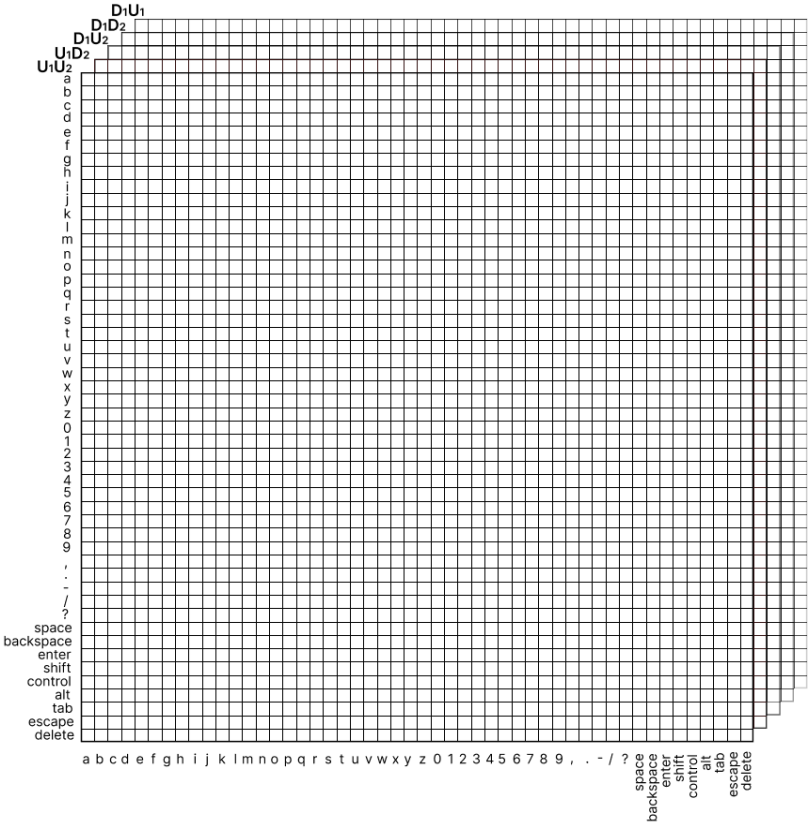

Рис. 1. Матрица переходов

Markov Transition Field (MTF) [3] является еще одним методом, который позволяет преобразовать временные данные в двумерное представление. MTF строится на основе марковских процессов, которые моделируют переходы между состояниями с учетом временных зависимостей. В отличие от матрицы переходов MTF учитывает не только частоту переходов, но и их временное расположение, что делает его более информативным для анализа клавиатурного почерка.

Использование сверточных нейронных сетей для анализа клавиатурного почерка на основе двумерных представлений временных данных открывает новые возможности для повышения точности и надежности биометрической аутентификации. Использование двумерных представлений временных данных, таких как матрица переходов, GAF и MTF, позволяет эффективно учитывать уникальные харак-

теристики клавиатурного почерка и повысить точность моделей. Дальнейшие исследования в этой области могут быть направлены на сравнение эффективности различных методов и разработку новых подходов к преобразованию временных данных для использования в CNN.

ЛИТЕРАТУРА

1. Altwaijry N. Keystroke Dynamics Analysis for User Authentication Using a Deep Learning Approach // International Journal of Computer Science and Network Security. – 2020. – Vol. 20, No. 12. – P. 209–216.

2. Dias T. KeyRecs: A keystroke dynamic and typing pattern recognition dataset / T. Dias, J. Vitorino, E. Maia, O. Sousa, I. Praça // Data in Brief. – 2023. – Vol. 50. – P. 8.

3. Брагин А.Д. Распознавание моторных образов на электроэнцефалограммах с применением свёрточных нейронных сетей / А.Д. Брагин, В.Г. Спицын // Компьютерная оптика. – 2020. – Т. 44, № 3. – С. 482–489.

УДК 004.891.3

ДИАГНОСТИКА ШИЗОФРЕНИИ И ДЕПРЕССИИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А.Д. Псарев, аспирант каф. КИБЭВС; У.В. Савина, техник ЦК НТИ

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, pad@fb.tusur.ru

Рассматривается диагностика шизофрении и депрессии с использованием средств искусственного интеллекта. Описываются сбор датасета и возникшие при предобработке данных проблемы, требующие решения.

Ключевые слова: диагностика шизофрении, диагностика депрессии, анализ речи.

Психические расстройства, такие как шизофрения и депрессия, затрагивают сотни миллионов людей по всему миру. Диагностика этих заболеваний остаётся сложной из-за субъективности клинических методов. Традиционные подходы, основанные на интервью и анкетах, не всегда обеспечивают необходимую точность, особенно в условиях нехватки специалистов.

Технологии искусственного интеллекта (ИИ) открывают новые возможности для анализа устной речи – важного маркера психического состояния, так как одними из ключевых признаков шизофрении и депрессии являются аномалии речи, например, в проявлении и частоте смены эмоций. На основе этих принципов уже ведутся исследования –

например, нейросетевая модель MIT может выявлять депрессию по снижению эмоциональной окраски речи, а исследования 2023 г. показывают, что ИИ распознаёт шизофрению через нарушения логики и семантические аномалии в высказываниях [1, 2]. ИИ анализирует отклонения в интонации, синтаксисе и лексике, что ускоряет диагностику и позволяет объективно оценивать динамику состояния пациента.

Практикующие врачи, занимающиеся клинической диагностикой, проявляют интерес к созданию диагностического модуля для автоматизированной помощи при комплексном обследовании пациентов. В сотрудничестве с НИИ психического здоровья ведётся работа по данному направлению.

Выбор набора данных для обучения модели должен учитывать язык, на котором проводится интервью с пациентом, из-за языковых и культурных особенностей. Отсутствие доступных наборов данных с записями речи пациентов связано с юридическими трудностями, связанными с обработкой персональных данных.

В связи с нехваткой подходящих наборов данных было решено создать собственный. Планируется собрать записи интервью около 60 пациентов, в том числе здоровых, с диагностированной депрессией и диагностированной шизофренией в равных долях.

На текущий момент осуществляется сбор данных с использованием оценочных шкал GRID-HAMD и PANSS [3]. В ходе интервью врач задаёт наводящие вопросы, оценивая и фиксируя реакции пациента.

На рис. 1 представлены примеры полученных при анализе двух различных фрагментов интервью мел-спектрограмм.

При анализе записей интервью выявлены проблемы, требующие решения:

– разделение речи врача и пациента, так как речь врача может искажать интонации и эмоциональные изменения пациента;

– тихая речь некоторых пациентов теряется на фоне шума, что затрудняет анализ речи.

Несмотря на кажущуюся тривиальность возникающих задач, поиск универсального решения осложняется различными факторами, такими как качество записи микрофона, фоновый шум и громкость речи пациента и лечащего врача.

Заключение. Использование ИИ для помощи врачам в диагностике шизофрении и депрессии является перспективным направлением, однако требующим особого подхода к методике сбора и (или) обработки аудиоданных.

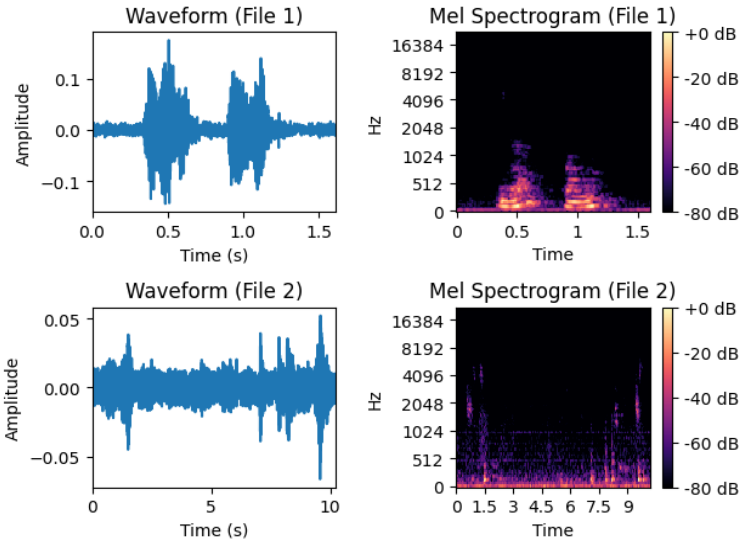

Рис. 1. Сравнение двух фрагментов интервью

ЛИТЕРАТУРА

1. Model can more naturally detect depression in conversations // Massachusetts Institute of Technology [Электронный ресурс]. – Режим доступа: https://news.mit.edu/2018/neural-network-model-detect-depression-conversations-0830 (дата обращения: 16.02.2025).

2. AI language models could help diagnose schizophrenia // Medical Xpress [Электронный ресурс]. – Режим доступа: https://medicalxpress.com/news/2023-10-ai-language-schizophrenia.html (дата обращения: 16.02.2025).

3. Шкала PANSS – описание // Официальный сайт ФГБНУ НЦПЗ [Электронный ресурс]. – Режим доступа: https://ncpz.ru/stat/78 (дата обращения: 19.02.2025).

УДК 004.852

ПРОДЛЁННАЯ АУТЕНТИФИКАЦИЯ НА СМАРТФОНАХ: ОБЗОР ПОВЕДЕНЧЕСКИХ И ФИЗИОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК

К.А. Скосарева, студентка каф. КИБЭВС

Научный руководитель М.М. Немирович-Данченко, проф. каф. КИБЭВС, д.ф.-м.н.

г. Томск, ТУСУР, skosarevaka160@gmail.com

В современном мире смартфоны являются неотъемлемой частью жизни человека, т.к. не только хранят персональные данные, такие

как контакты, фото и видео, но и предоставляют доступ к банковским приложениям, приложениям онлайн-магазинов и соцсетям пользователя. В связи с этим растёт потребность обеспечения безопасности данных не только перед входом в систему или в приложение, но и во время непосредственной работы с ним. В данной статье рассматриваются методы продлённой аутентификации на смартфонах с использованием физиологических и поведенческих характеристик.
Ключевые слова: явная аутентификация, продлённая аутентификация, смартфон, информационная безопасность, поведенческие характеристики, физиологические характеристики.

В современных смартфонах аутентификация пользователя играет ключевую роль в защите информации. Аутентификация является процессом проверки подлинности пользователя при его попытке получить доступ к системе и может быть разделена на явную и неявную (продлённую). Под явной аутентификацией подразумевается процедура непосредственного требования от пользователя предъявления пароля, ПИН-кода, одной или нескольких биометрических характеристик.

Стоит заметить увеличение тенденции применения явной аутентификации на основе физиологической биометрии, в частности, распознавание лица, радужки глаза и отпечатка пальца ввиду её устойчивости к атакам фишинга и подмены [6]. Тем не менее явная аутентификация не всегда может ограничить доступ нежелательным лицам к информации на телефоне. К примеру, пользователь может использовать слабый ПИН-код, пароль или графический рисунок, а также пользователь может без присмотра оставить разблокированный телефон в свободном доступе.

Одним из методов обеспечения безопасности данных при использовании разблокированного телефона является продлённая «неявная» аутентификация. Продлённая аутентификация предполагает непрерывный сбор и анализ данных в фоновом режиме незаметно для пользователя. На основе анализа система должна сравнить данные, получаемые от текущего пользователя, с данными из базы данных и принять решение о наличии необходимости запроса явной аутентификации.

Продлённая аутентификация основывается на биометрическом анализе человека, в котором чаще всего встречаются поведенческие характеристики. Поведенческая биометрия характеризуется изменчивостью во времени и представляет собой уникальные поведенческие паттерны человека при взаимодействии с устройством, таким как набор текста, разговор, удержание смартфона и т.п. [1].

В настоящее время активно изучается использование датчиков смартфона (акселерометра, гироскопа, магнитометра, датчика гравитации) для фиксации индивидуального паттерна взаимодействия пользователя с телефоном. Общий принцип работы систем на основе датчиков следующий: собранные данные с датчиков преобразуются в общий вектор признаков, поступающих на вход модели машинного обучения, решающей задачу проверки подлинности пользователя. Например, в статье [5] описывается система продлённой аутентификации на основе датчиков с использованием модели LSTM (Long Short-Term Memory). Преимуществом такого подхода является простота сбора данных, так как данные датчиков легко фиксируются и могут быть собраны незаметно для пользователя «в фоне».

Данными для продлённой аутентификации могут также выступать данные об использовании приложений [3], данные, снятые при прикосновении к сенсорному экрану [2]. По результатам исследований было выяснено, что эти данные обладают достаточным количеством уникальных характеристик для определения подлинности пользователя.

В ряде случаев поведенческие характеристики дополняются физиологическими. В статье [4] представлена мультимодальная система непрерывной аутентификации на основе лица и прикосновения к экрану. Представленная система объединяет «сильную» модальность лица (коэффициент EER которой в данной работе мог достичь результата в 4,76%) и «слабую» модальность прикосновения (EER которой 19,84%), достигая общего результата EER в 3,77% для объединённых модальностей. Модальность или же характеристику лица мы считаем «сильной» в отношении модальности прикосновения к экрану из-за существенной разницы в коэффициенте EER, определяющем точность системы аутентификации. Несмотря на ресурсоемкость системы, предполагающей обработку изображений, применение данного метода потенциально может обеспечить более высокую надёжность, чем системы только с поведенческими характеристиками.

В связи с растущими вычислительными мощностями смартфонов растут и возможности внедрения усложнённых систем защиты информации. Изучение систем продлённой аутентификации на смартфонах является перспективной областью исследований в связи с растущим риском атак на традиционные методы аутентификации.

Дальнейшие исследования в данной области должны быть направлены на оптимизацию сбора и обработки данных непосредственно самим мобильным устройством, увеличение точности системы аутентификации при минимизации вычислительных затрат, а так-

же разработку безопасных механизмов передачи данных в клиент-серверных архитектурах, если такие предполагаются.

ЛИТЕРАТУРА

1. Matyáš V. Biometric Authentication – Security and Usability / V. Matyáš, Z. Říha // Advanced Communications and Multimedia Security: IFIP TC6 / TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 26–27, 2002, Portorož, Slovenia / eds. B. Jerman-Blažič, T. Klobučar. – Boston, MA: Springer US, 2002. – P. 227–239.

2. Kumar R. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns / R. Kumar, V.V. Phoha, A. Serwadda // 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS) 2016. IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). – 2016. – P. 1–8.

3. Mahbub U. Continuous Authentication of Smartphones Based on Application Usage // IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2019. – Vol. 1, No. 3. – P. 165–180.

4. Smith-Creasey M. A continuous user authentication scheme for mobile devices / M. Smith-Creasey, M. Rajarajan // 2016 14th Annual Conference on Privacy, Security and Trust (PST) 2016 14th Annual Conference on Privacy, Security and Trust (PST). – 2016. – P. 104–113.

5. AUToSen: Deep-Learning-Based Implicit Continuous Authentication Using Smartphone Sensors // IEEE Journals & Magazine. IEEE Xplore. – URL: https://ieeexplore.ieee.org/abstract/document/9007368 (дата обращения: 24.12.2024).

6. (PDF) An Introduction to Biometric Recognition. – URL: https://www.researchgate.net/publication/3308596_An_Introduction_to_Biometric_Recognition (дата обращения: 15.03.2025).

УДК 004.853

АНАЛИЗ МЕТОДОВ ВЫЯВЛЕНИЯ ПАТОГЕННОСТИ CNV С ИСПОЛЬЗОВАНИЕМ КЛАССИФИКАТОРОВ

Е.В. Вааль, студент каф. ЭМИС

Научный руководитель А.А. Матолыгин, ст. преп. каф. ЭМИС

г. Томск, ТУСУР, vaal.katya@mail.ru

Копийные числовые вариации (CNV) играют ключевую роль в развитии множества заболеваний, включая наследственные патологии и онкологические процессы. Однако оценка их патогенности представляет сложную задачу из-за разнообразия механизмов воздействия на гены и белки. В данной статье рассматриваются современные подходы к автоматизированной классификации CNV, включая машинное обучение и трансформерные модели. Представлены алгоритмы, используемые для анализа данных секвенирования, опи-

саны их преимущества и ограничения, а также перспективы применения в персонализированной медицине.
Ключевые слова: CNV, патогенность, классификаторы, машинное обучение, трансформеры, генетический анализ.

Копийные числовые вариации (CNV) оказывают различное воздействие на организм, от нейтрального влияния до серьёзных нарушений, связанных с развитием патологий. Это разнообразие эффектов объясняется их локализацией, влиянием на структуру генов и белков, а также взаимодействием с другими генетическими и эпигенетическими факторами [1]. Именно поэтому оценка патогенности CNV играет важнейшую роль в генетических исследованиях, позволяя разграничить вариации, несущие клиническую значимость, от нейтральных изменений.

Для решения задачи оценки патогенности CNV всё чаще применяются методы автоматизированного анализа, основанные на передовых алгоритмах машинного обучения [2]. Это обусловлено возрастающей потребностью в обработке больших массивов данных, полученных с использованием технологий секвенирования нового поколения, и необходимостью быстрого и точного определения значимости вариаций. Современные классификаторы, базирующиеся на этих алгоритмах, играют ключевую роль в этом процессе. Они позволяют анализировать огромные объемы генетической информации, автоматизируя интерпретацию сложных геномных данных и выделяя патогенные CNV среди множества вариантов, присутствующих в геноме.

Одним из важнейших преимуществ классификаторов является их способность учитывать множество параметров CNV, таких как длина вариации, её локализация в геноме, влияние на регуляторные элементы и частота в популяции. Например, алгоритмы случайных лесов и методов опорных векторов обрабатывают эти данные, создавая прогнозы о патогенности на основе обученных моделей. Такие инструменты значительно упрощают процесс анализа и минимизируют вероятность человеческой ошибки, что особенно ценно для клинической диагностики.

Особого внимания заслуживают трансформерные модели, такие как BERT и его адаптации для биоинформатики. Эти модели способны анализировать сложные взаимодействия между элементами генома. Трансформеры обучаются на больших наборах данных, включая аннотированные геномные вариации, и могут распознавать ранее не обнаруженные патогенные изменения. Высокая точность и возможность масштабного анализа делают эти модели перспективным инструментом для исследований и клинического применения.

Благодаря своей архитектуре, основанной на механизме внимания, BERT и его модификации способны эффективно обрабатывать последовательности нуклеотидов и аннотированные геномные данные, что делает их незаменимыми для задач анализа CNV. Одной из ключевых особенностей трансформеров является их двунаправленный подход, который учитывает контекст как слева, так и справа от исследуемого элемента. Это особенно важно для анализа сложных взаимодействий внутри генома, где контекст может играть решающую роль в оценке патогенности вариаций.

Модификации BERT, такие как BioBERT и ClinicalBERT, обученные на биомедицинских данных, уже демонстрируют свою эффективность в задачах, связанных с генетическим анализом [3]. BioBERT использует базы данных с биомедицинскими публикациями и специализированной информацией для обработки научных текстов и биологических данных. Это позволяет извлекать значимую информацию о роли CNV, их локализации и влиянии на экспрессию генов. ClinicalBERT, в свою очередь, нацелен на применение в клинической практике и способен учитывать медицинский контекст, что делает его полезным для оценки клинической значимости вариаций.

Для задачи оценки патогенности CNV трансформеры находят применение благодаря своей способности анализировать множество взаимосвязей и параметров, характерных для вариаций. Эти модели обеспечивают глубокую обработку данных, позволяя выделять ключевые характеристики, такие как степень влияния CNV на экспрессию генов и их взаимодействие с регуляторными элементами. Кроме того, трансформеры эффективно решают проблему выявления ранее неизвестных патогенных вариаций. Путём обучения на больших аннотированных наборах данных, такие модели могут находить паттерны, которые ускользают от традиционных алгоритмов. Это открывает новые возможности для разработки персонализированных подходов в медицине, где оценка патогенности CNV становится основой для диагностики и лечения заболеваний.

Таким образом, трансформерные модели, такие как BERT, не только автоматизируют процесс анализа, но и позволяют глубже понять влияние CNV на организм, что делает их незаменимыми для современных генетических исследований. Их использование значительно ускоряет обработку данных, снижает вероятность ошибок и обеспечивает более точную интерпретацию генетических вариаций. Более того, возможности трансформеров продолжают расширяться благодаря развитию их архитектуры и интеграции с новыми источниками биомедицинских данных. Это открывает перспективы не только для

фундаментальной науки, но и для клинической практики, где точная оценка патогенности CNV может стать основой для персонализированных терапевтических подходов.

ЛИТЕРАТУРА

1. Кошкина О.А. Вариация числа копий (CNV) как перспективный генетический маркер: распространение, методы валидации и гены-кандидаты в геномах сельскохозяйственных животных: обзор / О.А. Кошкина, Т.Е. Денискова, Н.А. Зиновьева // Аграрная наука Евро-Северо-Востока. – 2020. – Т. 21, № 4. – С. 355–368.

2. Методы машинного обучения в биологии / А.К. Таскина, А.А. Муравьева, А.С. Ельсукова, В.С. Фишман // Природа. – 2020. – № 9 (1261). – С. 3–17.

3. Современные методы экстракции связанных именованных сущностей на примере биомедицинских текстовых данных / А.Г. Сбоев, А.А. Селиванов, Р.Б. Рыбка и др. // Вестник Военного инновационного технополиса «Эра». – 2022. – Т. 3, № 1. – С. 57–67.

УДК 004.032.26

ОПРЕДЕЛЕНИЕ ПСИХОЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ ДИКТОРА ПО ЕГО РЕЧИ С ПРИМЕНЕНИЕМ НЕЙРОННЫХ СЕТЕЙ

А.Д. Муханов, М.С. Крючков, Л.В. Глебов, С.В. Зверков, Р.А. Зверков, студенты каф. БИС

Научный руководитель П.Ю. Лаптев, м.н.с. ЦК НТИ ТДВ ГПО КИБЭВС-2401. Определение психоэмоционального состояния диктора с помощью методов машинного обучения

г. Томск, ТУСУР, andreimukhanoff@yandex.ru

Рассматриваются и анализируются наборы методов, которые применяются в задачах классификации психоэмоционального состояния диктора по его речи для выявления наиболее эффективного варианта в работе.

Ключевые слова: искусственная нейронная сеть, обработка звука, спектограммы, психоэмоциональный анализ речи.

Психоэмоциональное состояние человека является важным фактором его деятельности, которое напрямую влияет на его поведение. Применение искусственного интеллекта в данной сфере позволяет ускорить процесс определения этого состояния, что может быть критичным для некоторых ситуаций.

В ходе эксперимента планируется определить наиболее эффективные наборы методов, которые пригодны для обучения нейронных

сетей в задачах определения психоэмоционального состояния человека. В ходе исследования методы рассматриваются на наборе данных Ravdess, состоящих из записей речи 24 профессиональных актеров с 8 эмоциями.

Для обработки аудиозаписей сначала извлекаются признаки, характеризующие звуковое содержание. Один из таких – MFCC (мел-кепстральные коэффициенты), который преобразует аудиосигнал в компактное числовое представление, отражающее важные компоненты спектра речи. Это достигается с помощью мел-фильтров, приближённых к особенностям слухового восприятия человека. Преобразование аудио в изображения (например, спектрограммы) позволяет нормализовать записи по длине за счёт получения представлений фиксированного размера, что удобно для последующей классификации и распознавания.

Преобразование аудиосигналов служит основой для последующего анализа: на его основе формируется набор признаков, отражающих важную информацию о звуке. Эти признаки затем используются в задачах интерпретации и классификации аудиоданных.

Теперь переходим к работе с типами сетей. Обучение первой модели было решено провести базе LSTM (Long Short-Term Memory) – это тип рекуррентной нейронной сети (RNN), которая хорошо подходит для обработки временных последовательностей. При обучении LSTM используется для анализа временных зависимостей в MFCC (Mel-Frequency Cepstral Coefficients) и Chroma, которые извлекаются из аудиоданных. Также для повышения эффективности при обучении были внедрены иные методики, включающие собой ансамблирование и использование XGBoost, который представляет из себя градиентный бустинг над деревьями решений.

Вторая модель базировалась на применении ResNet-101 (сокращение от Residual Network) – это тип глубокой сверточной нейронной сети, разработанной для улучшения обучения глубоких моделей. Основная идея ResNet заключается в использовании остаточных соединений, которые позволяют сети обучаться более эффективно, даже если она имеет большое количество слоев.

ResNet-101 способна извлекать сложные признаки из MFCC благодаря своей глубине и остаточным блокам, также она устойчива к проблемам исчезающих градиентов.

В результате модель ResNet-101, обученная на MFCC, показала точность классификации эмоций на уровне 65% (левая матрица, рис. 1). Такой результат свидетельствует о переобучении модели, что, вероятно, связано с недостаточным объемом данных для обучения глубокой сверточной нейронной сети. Это подчеркивает важность наличия

больших и разнообразных наборов данных для эффективного обучения подобных архитектур.

Гибридная модель LSTM с XGBoost продемонстрировала значительно более высокую точность – 90% (правая матрица, рис. 1). Это подтверждает эффективность комбинирования временных (MFCC) и спектральных признаков для анализа эмоций в речевых сигналах. Использование долгой краткосрочной памяти (LSTM) позволило учесть временные зависимости в данных, а ансамблирование с помощью XGBoost улучшило обобщающую способность модели.

В итоге было выявлено несколько закономерностей, на основе которых можно выявить наиболее эффективные методы в задачах классификации эмоций. Так, гибридные модели, такие как LSTM с ансамблированием, оказываются более эффективными по сравнению с классическими сверточными нейронными сетями. Это связано с их способностью учитывать последовательные изменения в речевых сигналах.

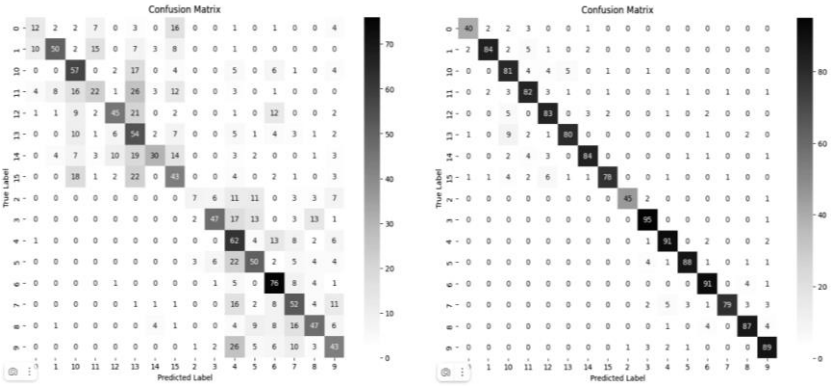

Рис. 1. Результаты обучения сетей

При этом недостаточный объем данных для обучения глубоких моделей, таких как ResNet-101, привёл к переобучению. Это подчеркивает необходимость дальнейшего совершенствования методов обработки речевых сигналов и использования дополнительных наборов данных для повышения точности и надежности моделей в задачах эмоционального анализа.

ЛИТЕРАТУРА

1. Применение нейросетевых технологий для анализа речевой информации [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/primenenie-neyrosetevyh-tehnologiy-dlya-analiza-rechevoy-informatsii, свободный (дата обращения: 11.10.2024).

2. Метод мел-частотных кепстральных коэффициентов в задаче распознавания речи [Электронный ресурс]. – Режим доступа: https://libeldoc.bsuir.by/ bitstream/123456789/36578/1/Aksenov_Metod.pdf, свободный (дата обращения: 12.10.2024).

3. Искусственные нейронные сети и их приложения [Электронный ресурс]. – Режим доступа: https://kpfu.ru/staff_files/F1493580427/NejronGafGal.pdf, свободный (дата обращения: 14.10.2024).

УДК 004.8

ПРИМЕНЕНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБУЧЕНИЯ ИИ В ИГРЕ «ЗМЕЙКА»

Д.А. Анохин, Я.А. Дашевский,
Д.В. Тихомиров, студенты каф. КИБЭВС
Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, и.о. зав. каф. БИС
Проект ГПО БИС-2402. Машинное обучение при биометрической аутентификации и атаки на него
г. Томск, ТУСУР, anohin.dima2018@yandex.ru

Исследуется применение алгоритмов машинного обучения для обучения искусственного интеллекта (ИИ) в игре «Змейка». Проведено сравнение трех подходов: случайного движения, жадного алгоритма и Q-learning. Эксперименты показали, что Q-learning эффективнее алгоритмических методов, достигая среднего счета в 24 очка.
Ключевые слова: змейка, Q-learning, машинное обучение, динамическая среда, обучение с подкреплением.

Игра «Змейка» представляет собой легкореализуемую среду, где агент должен максимизировать счет, избегая столкновений с собственным телом и границами поля. Цель работы – сравнить эффективность алгоритмов и ИИ в динамической среде. Агенты:

1. Случайный агент – выбор направления без анализа среды.
2. Жадный агент – движение к еде с учетом текущего направления.
3. Q-learning – Q-функция измеряет полезность пары «состояние – действие» при определенной стратегии [1].

Жадный алгоритм определяет направление к еде через разность координат, запрещает движение в сторону, противоположную текущему направлению.

Q-learning кодирует состояния 12 бинарными признаками: 4 – текущее направление движения; 4 – положение еды относительно головы; 4 – наличие препятствий в соседних клетках. Были выбраны следующие параметры обучения: скорость обучения – 0,05; дисконт-фактор – 0,95; вероятность случайного действия – 1,0 → 0,01. Q-таблица имеет размер 4 096 состояний × 4 действия.

Для каждого алгоритма выполнено 3 000 эпизодов игры (рис. 1–3).

Жадный алгоритм быстро находит еду, но не учитывает риски столкновения с собственным телом. Q-learning старается избегать столкновенний с собственным телом благодаря системе наград и наказаний.

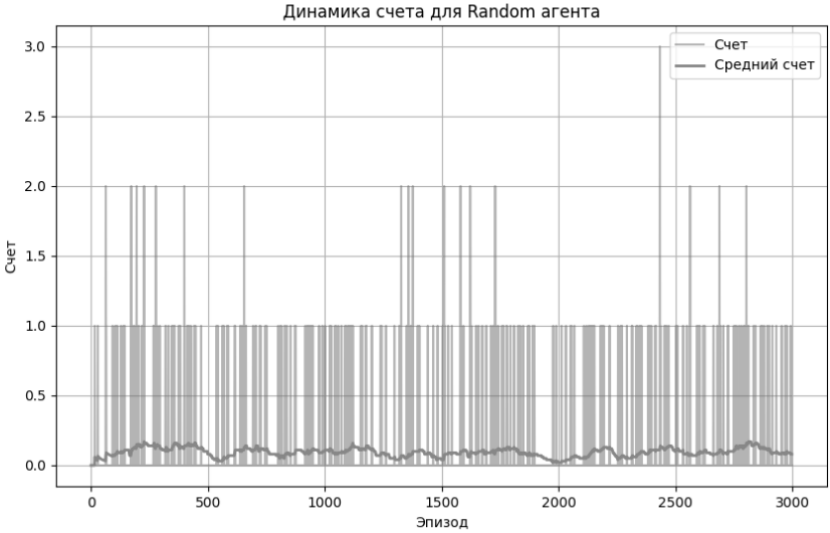

Рис. 1. Случайный агент: средний счет – 0,08

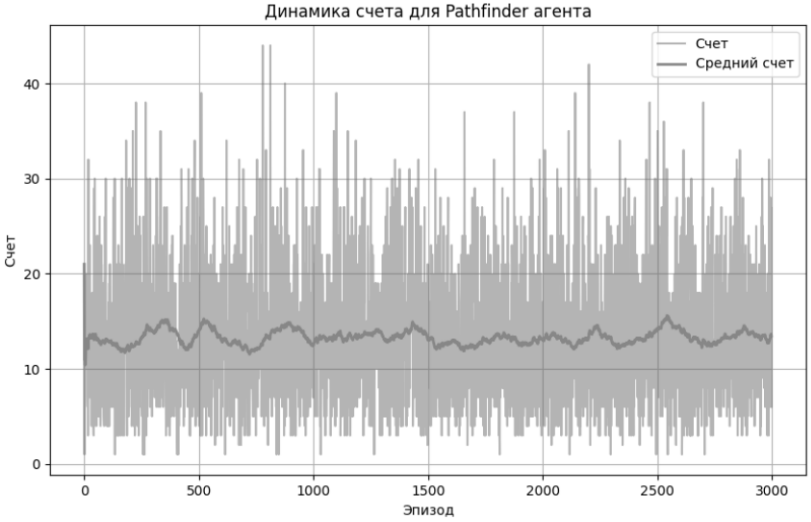

Рис. 2. Жадный агент: средний счет – 13,46

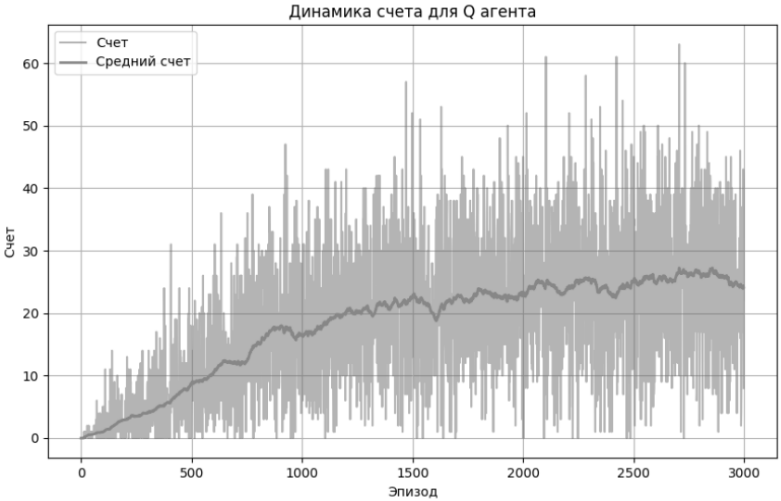

Рис. 3. Q-агент: средний счет – 24,13

Искуственному интелекту сложно играть в змейку бесконечно. Среда превращается в динамический лабиринт, и с каждым набранным очком её сложность возрастает.

Единственный вариант алгоритмически пройти змейку (набрать очки, равные размеру среды) – это гамильтоновый цикл – это замкнутый путь, который проходит все клетки среды без пересечений [2]. Чтобы ИИ прошел змейку, необходимо, чтобы он обучился данной стратегии.

ЛИТЕРАТУРА

1. Грессер Л. Глубокое обучение с подкреплением: теория и практика на языке Python / Л. Грессер, В.Л. Кенг. – СПб.: Питер, 2024. – 416 с.

2. Змейка, мыши и Гамильтон: научно-популярный ресурс «Habr» [Электронный ресурс]. – URL: https://habr.com/ru/articles/544696.

УДК 004.8

БАЗОВЫЕ АЛГОРИТМЫ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ И ПРИМЕНЕНИЕ В ИГРЕ В «КРЕСТИКИ-НОЛИКИ»

Я.А. Дашевский, Д.А. Анохин, Д.В. Тихомиров, студенты

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, kvi@fb.tusur.ru

Обучение с подкреплением (RL) позволяет учить RL-агентов принятию последовательных решений, например, в стратегических при

взаимодействии со средой на основе системы вознаграждений и штрафов. Исследовано применение RL-алгоритмов для обучения агентов в игре «Крестики-нолики».
Целью данной работы является ознакомление и обзор классических алгоритмов обучения с подкреплением, обучение различных агентов в игре «крестики-нолики».
Ключевые слова: обучение с подкреплением, стратегические игры, алгоритмы, стратегия, искусственный интеллект.

Обучение с подкреплением – область машинного обучения, занимающаяся задачами последовательного принятия решений.

Стратегия – это функция, в соответствии с которой агент выбирает действия.

Агент представляет собой субъект, принимающий решения. Его задача – максимизировать целевую функцию, выбирая наилучшие действия. Он учится этому, взаимодействуя со средой методом проб и ошибок.

Среда предоставляет информацию, описывающую состояние системы. Агент взаимодействует со средой, наблюдая состояние и используя данную информацию при выборе действия. Среда принимает действие и переходит в следующее состояние.

Функция полезности (q-функция) – функция, оценивающая, насколько хорошим или плохим является состояние. Она является математическим представлением ожидаемой награды за действие в заданном состоянии.

Q-таблица – структура данных, в которой сохраняются значения Q-функции для всех пар (состояние, действие).

Классические алгоритмы обучения с подкреплением, такие как Q-learning и SARSA, основаны на использовании Q-таблицы. Ключевое отличие SARSA от Q-learning заключается в том, что SARSA оценивает значения Q на основе действий, выполняемых текущей стратегией, а не жадной стратегией.

Хотя эти алгоритмы показывают себя хорошо в простых задачах с ограниченным числом состояний, для более сложных и объемных задач уместно использовать алгоритм DQN (Deep Q Network), заменяющий Q-таблицу нейронной сетью для оценки значений Q-функции. Другая проблема, от которой избавлен данный алгоритм, – невозможность Q-алгоритма выбрать лучшее действие для состояний, которые он не видел ранее.

Итоговые метрики обученного агента в основном зависят от параметров обучения: скорости обучения, фактора дисконтирования, фактора исследования и количества эпизодов обучения.

Реализация обучения с подкреплением для игры в крестики-нолики продемонстрировала эффективность классических алгоритмов RL в задачах с информационной симметрией, где все игроки имеют идентичную информацию о текущем состоянии игры, и конечным дискретным множеством состояний. Алгоритмы показывают быструю сходимость. Таким образом, в задачах с неполной информацией или большим числом состояний, например, покер, классические RL-алгоритмы могут не обеспечить устойчивую сходимость.

Полученные выводы являются позволяют применять подход обучения с подкреплением для более сложных задач с переходом к более сложным.

ЛИТЕРАТУРА

1. Gresser L. Foundations of Deep Reinforcement Learning / L. Gresser, Wah Loon Keng. [Электронный ресурс]. – Режим доступа: https://books.google.com.np/books/about/Foundations_of_Deep_Reinforcement_Learni.html?id=0HW7DwAAQBAJ&redir_esc=y, свободный (дата обращения: 06.02.2025).

2. Phil Winder Reinforcement Learning: Industrial Applications of Intelligent Agents [Электронный ресурс]. – Режим доступа: https://books.google.ru/books?id=u87AzQEACAAJ&redir_esc=y, (дата обращения: 06.02.2025).

3. Q-Learning Algorithms: A Comprehensive Classification and Applications / B. Jang, M. Kim, Ga. Harerimana, J.W. Kim [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/335805245_Q-Learning_Algorithms_A_Comprehensive_Classification_and_Applications, свободный (дата обращения: 10.03.2025).

4. Sutton R.S. Reinforcement Learning: An Introduction / R.S. Sutton, A.G. Barto [Электронный ресурс]. – Режим доступа: https://books.google.ru/books?id=U57uDwAAQBAJ&redir_esc=y, свободный (дата обращения: 10.03.2025).

УДК 004.934.5

ШУМООЧИСТКА РЕЧЕВЫХ СИГНАЛОВ

И.С. Краснокутский, А.В. Вологжанин, студенты каф. КИБЭВС

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

Проект ГПО БИС-2402. Машинное обучение при биометрической аутентификации и атаки на него

г. Томск, ТУСУР

Рассматриваются основные методы фильтрации шумов, включая методы на основе машинного обучения и адаптивные алгоритмы. Обсуждаются достоинства и недостатки различных подходов.

Ключевые слова: шумоочистка, улучшение речи, машинное обучение.

Шумоочистка подразумевает улучшение чистого речевого сигнала от шумных входных сигналов, улучшение разборчивости и качество речи. Таким образом, алгоритмы шумоочистки являются незаменимым компонентом в современных системах автоматического распознавания речи (ASR), телекоммуникационных системах и слуховых аппаратах.

На рис. 1 показан результат применения различных алгоритмов шумоочистки.

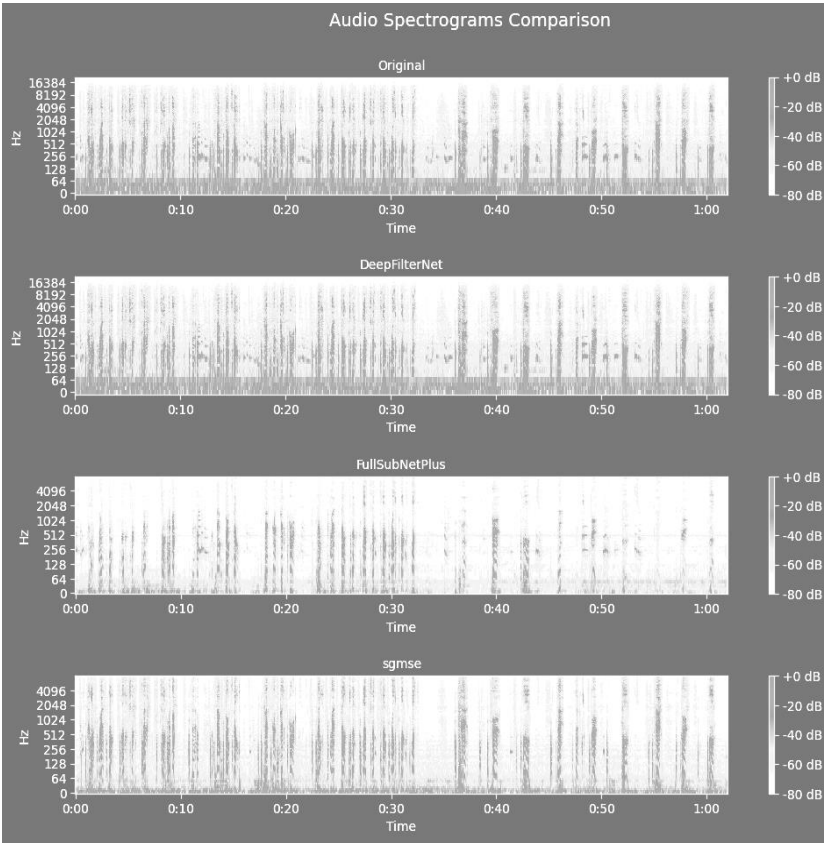

Рис. 1. Применение алгоритмов машинного обучения к звуку

Традиционные подходы шумоочистки в основном основаны на статистических моделях, включая спектральное вычитание, спектральное взвешивание и фильтр Винера. Однако эти подходы показа-

ли ограниченную производительность в речи с нестационарными шумами, которые распространены в реальных условиях, а также зачастую требуют предварительных предположений о характере шума и обычно разрабатываются для подавления конкретных его типов. Чтобы устранить это ограничение, в последние годы широко исследовались подходы глубокого обучения для улучшения возможностей шумоочистки. В сфере глубокого обучения для задач шумоочистки принято выделять два основных подхода: дискриминативные и генеративные методы.

Дискриминативные методы основываются на прямом обучении преобразованию зашумлённой речи в чистую, где модель минимизирует расстояние между целевым и выходным сигналом. Такие подходы демонстрируют высокую эффективность в условиях, близких к обучающим данным, однако их качество может снижаться при столкновении с незнакомыми типами шума, реверберацией или вариациями соотношения сигнал/шум, поскольку они жёстко зависят от ограничений обучающего набора. Кроме того, агрессивное подавление шума иногда приводит к появлению артефактов – искажений, которые ухудшают естественность и разборчивость восстановленной речи, несмотря на успешное удаление шумовой составляющей.

Генеративные методы фокусируются на изучении априорного распределения чистой речи, воспроизводя её спектральные и временные паттерны через моделирование внутренней структуры данных. Благодаря этому они демонстрируют большую устойчивость к невидимым условиям (разные типы шума, уровни SNR, реверберация), так как опираются не на прямое исправление ошибок, а на генерацию сигнала, соответствующего естественным характеристикам речи. Примеры таких подходов включают генеративные состязательные сети (GAN), вариационные автокодировщики (VAE) и диффузионные модели. Их ключевое преимущество – минимизация потерь полезной информации за счёт работы только с искусственно добавленным шумом, что снижает риск артефактов и сохраняет целостность речевого сигнала.

Таким образом, в то время как дискриминативные методы стремятся напрямую минимизировать разницу между зашумленной и чистой речью, генеративные методы концентрируются на изучении внутреннего распределения чистой речи. Это обеспечивает им более высокую гибкость и устойчивость при работе с разнообразными и невиданными шумовыми условиями, что особенно важно, если в речи человека имеются различные дефекты, которые могут быть связаны с индивидуальными особенностями произношения, артикуляционными нарушениями или патологическими изменениями голоса.

Такие дефекты могут приводить к дополнительным искажениям и сложностям при обработке сигнала, поэтому модели, способные учитывать внутреннюю структуру чистой речи, позволяют более эффективно компенсировать эти отклонения и восстанавливать качественный звуковой сигнал даже в сложных акустических условиях.

Для комплексной оценки современных методов шумоочистки были разработаны специализированные стенды, объединяющие популярные open-source-решения. В качестве образца использована запись голоса человека с удалённой гортанью.

ЛИТЕРАТУРА

1. Schröter H. Towards Real-Time Speech Enhancement on Embedded Devices for Full-Band Audio / H. Schröter, A.N. Escalante-B [Электронный ресурс]. – URL: https://arxiv.org/abs/2205.05474 (дата обращения: 20.03.2025).

2. Chen J. Channel Attention FullSubNet with Complex Spectrograms for Speech Enhancement / J. Chen, Z. Wang [Электронный ресурс]. – URL: https://arxiv.org/abs/2203.12188 (дата обращения: 20.03.2025).

3. Richter J. Speech Enhancement and Dereverberation With Diffusion-Based Generative Models / J. Richter, S. Welker // IEEE [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/abstract/document/10149431 (дата обращения: 20.03.2025).

УДК 004.522

КЛАССИФИКАЦИЯ ИЗМЕНЕНИЙ ГОЛОСА ДО И ПОСЛЕ ОПЕРАЦИИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ АУГМЕНТАЦИИ

М.А. Куковякин, А.В. Урванцев, студенты каф. БИС

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

Проект ГПО БИС-2403. Методы верификации пользователя по рукописным данным

г. Томск, ТУСУР

Рассматривается проблема распознавания голосов с использованием нейросетевых методов. Исследуется влияние аугментации данных на точность классификации, включая генерацию искусственных вариаций аудиозаписей без их сохранения в файлы. В качестве исходных данных используются аудиозаписи пяти разных голосов, сопровождающиеся соответствующими текстами. Для обучения модели применяется TensorFlow, а эффективность различных подходов к обработке данных анализируется на основе полученных результатов. Работа направлена на оптимизацию процесса обучения нейросети и повышение точности классификации голосов.

Ключевые слова: классификация речи, обработка аудио, машинное обучение, голос, нейросети.

Характеристики человеческого голоса могут существенно изменяться после хирургического вмешательства, особенно затрагивающего голосовые связки или дыхательные пути. Автоматическое определение этих изменений позволяет объективизировать процесс восстановления пациента и своевременно корректировать реабилитационные мероприятия. В данной работе предложен метод машинного обучения, основанный на анализе спектральных характеристик голоса, с применением методов аугментации данных для улучшения обобщающей способности модели.

Методология. Для решения поставленной задачи использовалась база данных голосов пациентов, включающая записи до и после операции. Данные были разделены на две категории: «до» и «после» вмешательства.

Предварительная обработка данных. Аудиофайлы были загружены и нормализованы. Из каждого аудиосигнала извлекались MFCC-признаки, усредненные по времени. Полученные признаки использовались в качестве входных данных для классификатора.

Аугментация данных. Для повышения устойчивости модели применялись следующие методы аугментации:

- временное растяжение/сжатие сигнала,
- сдвиг по высоте тона,
- добавление белого шума,
- изменение громкости,
- полосовая фильтрация,
- добавление эха и реверберации.

Каждая запись подвергалась случайному набору преобразований, что позволяло модели лучше обобщать данные и справляться с вариативностью голоса.

Обучение нейросети. В качестве модели использовалась многослойная (MLP) нейросеть с несколькими полносвязными слоями, регуляризацией и механизмами нормализации. Данные разделялись на обучающую и тестовую выборки в пропорции 80/20. Обучение проводилось в течение 25 эпох с ранней остановкой по критерию валидационной ошибки. Оценка проводилась по стандартным метрикам: точность, полнота, F1-мера.

Результаты. Обученная модель продемонстрировала ограниченную точность классификации голосов, что свидетельствует о сложности задачи и возможных ограничениях используемого подхода.

При обучении без аугментации данных:

- Тренировочная точность составила 69,72%, тестовая – 77,31%.
- Потери на тренировочной выборке – 0,5390, на тестовой – 0,4933.

Матрица ошибок показала, что большая часть неверных классификаций приходилась на записи, в которых изменения голоса после операции были минимальными.

При обучении с аугментацией данных:

- Тренировочная точность повысилась до 88,02%, однако тестовая снизилась до 75,93%.
- Потери на тренировочной выборке уменьшились (0,5887), но на тестовой выборке, напротив, увеличились (0,8618).

Рост разницы между тренировочной и тестовой точностью указывает на переобучение модели: модель лучше запомнила обучающие данные, но не смогла обобщить закономерности на новых примерах.

Аугментация данных не улучшила классификацию, возможно, из-за внесенного шума. Архитектура MLP могла быть недостаточно мощной для анализа скрытых паттернов. Необходимо исследовать более сложные модели, учитывающие временные зависимости, например, сверточные или рекуррентные нейросети.

Заключение. Разработанная модель на основе MFCC-признаков продемонстрировала ограниченную эффективность в задаче автоматического выявления изменений голоса после операции. Несмотря на высокую точность на тренировочной выборке, наблюдается недостаточная обобщающая способность модели на тестовых данных. Аугментация данных не обеспечила ожидаемого роста точности, а в некоторых случаях даже привела к ухудшению результатов.

В будущих исследованиях планируется:

- Разработка более сложных архитектур нейросетей (например, сверточных или рекуррентных) для более точного анализа голосовых изменений.
- Использование дополнительных признаковых пространств, таких как спектрограммы или мел-спектрограммы, чтобы захватить больше информации о голосе.
- Оптимизация стратегии аугментации, чтобы искусственные изменения более точно отражали естественные вариации голоса.
- Подбор более эффективных параметров модели и методов регуляризации для уменьшения эффекта переобучения.

ЛИТЕРАТУРА

1. Романовская Ю.М. Методы аугментации аудиосигнала / Ю.М. Романовская, Е.А. Ильюшин // International Journal of Open Information Technologies. – 2023. – Т. 11, № 3. – С. 12–18.

2. Афанасьев Д.Ю. Применение аугментации для улучшения качества классификации // StudNet. – 2022. – Т. 5, № 4. – С. 2397–2411.

3. Пырнова О.А., Зарипова Р.С. Методы и проблемы переобучения многослойной нейронной сети // Информационные технологии в строительных, социальных и экономических системах. – 2020. – № 2. – С. 101–102.

УДК 004.934

ОЦЕНКА КАЧЕСТВА СИНТЕЗА РЕЧИ

А.В. Максимов, Н.Д. Никитин,
Г.Л. Погорелов, студенты каф. КИБЭВС
Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.
Проект ГПО БИС-2402. Машинное обучение при биометрической аутентификации и атаки на него
г. Томск, ТУСУР, amaximov055@gmail.com, grenki70@gmail.com, kolya.nikitin.2005@inbox.ru

Рассматривается метод подготовки набора данных, позволяющий увеличить точность классификации речи за счет комплексной обработки аудиозаписей при помощи наложения и удаления шумов, а также сравнительном анализе визуализированных спектрограмм с целью определения оптимальных параметров обработки аудио. Целью данной работы является создание набора данных, основанного на записях человеческой речи и синтезированной.
Ключевые слова: синтез речи, наложение шумов, шумоподавление, спектрограмма.

Синтез речи – процесс автоматической генерации речи с помощью машин или компьютеров. Целью синтеза является создание машины с естественным голосом, предоставляющей пользователю информацию на необходимом ему языке, акценте или голосе. Исследования в области преобразования текста в речь (далее – TTS) являются междисциплинарной областью: от акустической фонетики, включающая в себя процесс производства речи и ее восприятия до морфологии и синтаксиса, отвечающих за произношение, части речи и грамматики [1].

Процесс преобразования текста в речь включает в себя следующие этапы:

1. Анализ текста – включает нормализацию текста, где числа и символы превращаются в слова, а сокращения заменяются полными словами или фразами.

2. Фонетический анализ преобразует орфографические символы в фонологические с использованием фонетического алфавита.

3. Просодия – это концепция, которая включает ритм речи, ударения и интонацию. На уровне восприятия естественность речи приписывается определенным свойствам речевого сигнала, связанным с различимыми изменениями высоты тона, громкости и длины слогов, которые вместе называются просодией. Акустически эти изменения соответствуют вариациям частоты основного тона, амплитуды и длительности речевых единиц.

Синтезированная речь отличается от реальной речи не только акустическими характеристиками (отсутствие естественных вариаций просодии), но и отсутствием фоновых шумов, которые присутствуют в реальных записях.

В то время как реальные речевые сигналы содержат шумы, обусловленные техническими ограничениями устройств, записывающих звуковые сигналы, разной акустикой помещений или естественными фоновыми помехами, синтезированная речь генерируется в идеальных условиях.

Набор реальной и синтезированной речи будет иметь разные характеристики, что может привести к некорректному обучению классификатора. Для того чтобы избежать проблем с точностью, необходимо создать одинаковую среду для обоих наборов аудиозаписей – искусственно наложить белый шум на реальную и синтезированную речь и очистить от всего шума.

На рис. 1 представлены спектрограммы реального и синтезированного голоса до и после обработки.

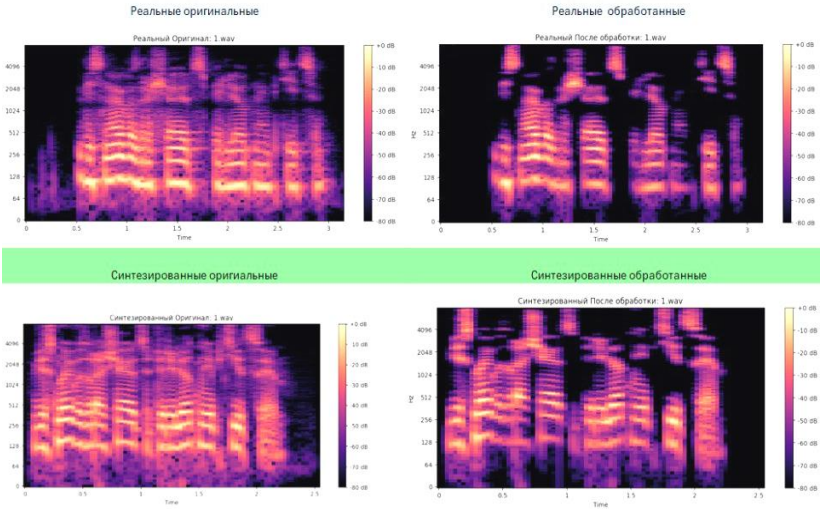

Рис. 1. Спектрограммы до и после обработки

Для решения данной проблемы был разработан стенд для подготовки набора данных и дальнейшей их классификации, который включает в себя следующие модули:

1. Модуль синтеза речи: Coqui TTS [3], Silero TTS [4] – библиотеки, использующие готовые модели, поддерживающие различные язы-

ки, а также использующие API ElevenLabs [5] Text to Speech, включающий в себя множество готовых моделей дикторов.

2. Модуль наложения шумов на наборы речи: генерация искусственного белого шума, масштабирование шума до необходимого SNR (Signal-to-noise ratio). Смешивание шума и сигнала при помощи сложение массивов;

3. Модуль шумоподавления: noisereduce [2] – библиотека, которая реализует спектральное шумоподавление (происходит анализ участков аудио, где есть шум, далее аудио разбивается на блоки, для каждого блока находится спектр и из него вычитается шум).

ЛИТЕРАТУРА

1. Speech Synthesis: Review / A. Balyan, S.S. Agrwal, A. Dev [Электронный ресурс]. – Режим доступа: https://www.ijert.org/speech-synthesis-a-review, свободный (дата обращения: 16.02.2025).

2. Noisereduce [Электронный ресурс]. – Режим доступа: https://pypi.org/project/noisereduce/, свободный (дата обращения: 20.02.2025).

3. Coqui TTS [Электронный ресурс]. – Режим доступа: https://github.com/coqui-ai/TTS, свободный (дата обращения: 16.02.2025).

4. Silero TTS [Электронный ресурс]. – Режим доступа: https://silero.ai/, свободный (дата обращения: 16.02.2025).

5. ElevenLabs [Электронный ресурс]. – Режим доступа: https://elevenlabs.io/docs/capabilities/text-to-speech, свободный (дата обращения: 20.02.2025).

УДК 004.8

ОБУЧЕНИЕ С ПОДКРЕПЛЕНИЕМ. АЛГОРИТМЫ, ОСНОВАННЫЕ НА ПОЛЕЗНОСТИ

Д.В. Тихомиров, Я.А. Дашевский, Д.А. Анохин, студенты

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

г. Томск, ТУСУР, tihomirov2005@gmail.com

С помощью обучения с подкреплением можно обучить агента, используя интересующую среду. Благодаря отсутствию необходимости в сборе датасетов в последние десятилетия активно изучается обучение с подкреплением. Целью работы является изучение простейших алгоритмов, основанных на полезности по актуальному опыту.

Ключевые слова: обучение с подкреплением, алгоритмы, основанные на полезности, алгоритмы по актуальному опыту, агент; среда.

Агент – субъект, который принимает решения.

Среда – это набор возможных действий (a) и состояний (s), на основе которых обучается агент.

Обучение с подкреплением – это парадигма машинного обучения, которая способна оптимизировать последовательные решения агента, основываясь на среде. Агент совершает действия, которые провоцируют получение награды. Награда выдается на основе изменения состояния среды. Существует множество алгоритмов обучения с подкреплением, которые делят на семейства. Одним из таких семейств выделяют алгоритмы, основанные на полезности.

Алгоритмы, основанные на полезности, – это алгоритмы, которые настраивают функцию полезности $Q(s, a)$. Их разделяют на алгоритмы по актуальному опыту и алгоритмы по отложенному опыту. В данной работе рассматриваются только алгоритмы по актуальному опыту.

Алгоритмы по актуальному опыту – алгоритмы, которые учатся по текущей стратегии. Стратегия – функция, отражающая множество состояний и множество действий.

Q-обучение – это алгоритм обучения с подкреплением, который реализует настройку *Q*-функции по формуле

$$Q(s, a) \leftarrow Q(s, a) + \alpha(r + \gamma \arg\max_{a_s \in A(s)} Q(s', a_s) - Q(s, a),$$

где $Q(s, a)$ – функция полезности при состоянии s и действии a; α – скорость обучения; r – вознаграждение; γ – влияние полезности последующих действий; $\arg\max Q(s', a_s)$ – максимальная полезность из $A(s)$ действий при состоянии s', достигаемая после действия a. Характерной особенностью данного алгоритма является выбор максимальной полезности состояния s', что приводит к формированию смелой стратегии.

SARSA – это алгоритм, разработанный для предоставления более общего решения обучения с подкреплением. Он реализует настрой *Q*-функции по формуле

$$Q(s, a) \leftarrow Q(s, a) + \alpha(r + \gamma Q(s', a') - Q(s, a)),$$

где $Q(s', a')$ – усреднение полезности по всем прогонам. Это приводит к формированию более сдержанной стратегии, так как учитываются все полезности, а не только максимальная.

У обоих перечисленных выше алгоритмов существует проблема в том, что их стратегии детерминированы, из-за чего пространство состояний и действий может быть исследовано не полностью. Для избежания данной проблемы был придуман ε-жадный алгоритм. Его суть в ε-шансе случайного действия. Случайные действия позволяют агенту лучше изучить среду и делают агента более гибким. Часто ε делают близким к 1 в начале обучения и постепенно снижают по мере обучения.

Помимо ε-жадного алгоритма, также существует множество модификаций вышеперечисленных алгоритмов:

Двойное *Q*-обучение – в этой модификации создаются 2 *Q*-функции, которые обучаются параллельно и корректируют друг друга. Устраняет статистические аномалии.

Отложенное *Q*-обучение – вместо того, чтобы обновлять *Q*-функцию каждый раз, когда агент посещает пару (*s* – *a*), он буферизирует вознаграждение. После того как агент посетил (*s* – *a*) *о*пределенное количество раз, он обновляет *Q*-функцию. Устраняет статистические аномалии.

Обучение с подкреплением на основе противодействия – улучшает эффективность обучения за счет выполнения в определенный момент действий с минимальной полезностью.

N-шаговый алгоритм – заглядывает на *n* шагов вперед, что приводит к более дальновидной стратегии. Также улучшает эффективность обучения.

Алгоритм *Q*-обучения Уоткинса – основан на сбрасывании трассировки соответствия при нежелательных действиях.

Быстрое *Q*-обучение – основано на экспоненциальном уменьшении суммы обновлений. Увеличивает скорость обучения.

Заключение. Алгоритмы обучения с подкреплением, основанные на полезности, разнообразны, и существует множество модификаций, способных улучшить эффективность данных алгоритмов.

ЛИТЕРАТУРА

1. Грессер Л. Глубокое обучение с подкреплением: теория и практика на языке Python / Л. Грессер, В.Л. Кенг. – СПб.: Питер, 2024. – 416 с.

2. Уиндер Ф. Обучение с подкреплением для реальных задач / пер. с англ. – СПб.: БХВ-Петербург, 2023. – 400 с.

УДК 004.932.2

МЕТОДЫ АУГМЕНТАЦИИ АУДИОДАННЫХ В КЛАССИФИКАЦИИ ГОЛОСОВ ДО И ПОСЛЕ ОПЕРАЦИИ

А.В. Урванцев, М.А. Куковякин, студенты каф. БИС

Научный руководитель Е.Ю. Костюченко, доцент каф. КИБЭВС, к.т.н.

Проект ГПО БИС-2403. Методы верификации пользователя по рукописным данным

г. Томск, ТУСУР

Анализ изменений голоса после операции важен в медицине и аудиологии, но данные для машинного обучения часто ограничены. Аугментация аудиоданных помогает расширить обучающий набор

и повысить точность моделей. В статье рассматриваются основные методы аугментации: временные, частотные и комбинированные преобразования. Анализируются их плюсы, минусы и практическое применение.
Ключевые слова: аугментация аудиоданных, обработка речи, машинное обучение, изменение голоса, медицинская диагностика.

Голос человека может изменяться после операции из-за анестезии, физиологических изменений или повреждений нервов. Автоматический анализ этих изменений помогает оценивать процесс реабилитации. Однако из-за нехватки записей аугментация аудиоданных становится ключевым инструментом для увеличения объема обучающих данных и улучшения моделей.

Методы аугментации делятся на три группы:

1. Обрабатывающие звуковой сигнал. Такие основные методы, как изменение громкости, скорости, высоты основного тона, сдвиг по времени, добавление случайных шумов, эффектов эхо или реверберации. Все эти методы изменяют исходный аудиосигнал до этапа получения признаков.

2. Обрабатывающие спектрограммы. Традиционные методы аугментации, применяемые к изображениям при работе со спектрограммами, только ухудшают результат. Специально для работы с ними были разработаны такие методы, как SpecAugment (TimeWarp, TimeMasking, FrequencyMasking), суммирование двух случайных спектрограмм одного класса.

3. Порождающие новые данные. Ранее были рассмотрены методы, изменяющие исходные данные. Также рассмотрим методы, порождающие новые данные. Одним из таких является использование моделей на основе порождающих нейросетей (GAN), например, WaveGAN или SpecGAN. Также есть возможность генерировать MFCC-признаки при помощи рекуррентной нейронной сети (RNN).

В ходе экспериментов были изучены методы аугментации из первых двух групп. Анализ показал, что выбор параметров для каждого метода является критически важным: чрезмерное изменение параметров сигнала или спектрограммы может привести к искажению исходных характеристик голоса. Например, слишком сильное изменение высоты основного тона или агрессивное маскирование частот могут привести к ухудшению результатов классификации.

Кроме того, было выявлено, что применение методов аугментации по отдельности дает ограниченный эффект, а их случайное комбинирование может даже ухудшить точность модели. Это связано с тем, что случайные изменения могут искажать важные акустические

особенности, необходимые для корректного распознавания изменений в голосе. Оптимальным подходом является подбор комбинаций аугментаций с учетом специфики задачи и предварительной оценки их влияния на качество модели.

Таким образом, для эффективного использования аугментации аудиоданных в задачах классификации голосов до и после операции необходимы тщательное тестирование параметров и разработка стратегий аугментации, которые улучшают обобщающую способность модели без чрезмерного искажения исходных данных.

ЛИТЕРАТУРА

1. Ko T. et al. Audio augmentation for speech recognition // Interspeech. – 2015. – P. 3586.

2. Schlüter J. Exploring data augmentation for improved singing voice detection with neural networks / J. Schlüter, T. Grill // ISMIR. – 2015. – P. 121–126.

3. Javanmardi F. A comparison of data augmentation methods in voice pathology detection / F. Javanmardi, S.R. Kadiri, P. Alku // Computer Speech & Language. – 2024. – Vol. 83. – P. 101552.

УДК 004.896

КВАНТОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ РЕАЛИЗАЦИИ НА ПЛИС

Д.Е. Блох, А.И. Безмельцев, аспиранты;

В.С. Панищев, доц. каф. вычислительной техники, к.т.н.

г. Курск, Юго-Западный государственный университет,

den5553@yandex.ru

Целью данного исследования является определение влияния различных методов квантования на точность (accuracy) и функцию потерь (loss) двух архитектур (перцептрона и сверточной сети), обученных на наборе данных MNIST. Особое внимание уделено вопросу реализации на ПЛИС, поскольку необходимо учитывать скорость вычислений и потребление ресурсов.

Ключевые слова: нейросеть, квантование, ПЛИС, распознавание.

В современных системах компьютерного зрения и распознавания образов активно применяются сверточные нейронные сети (CNN) и многослойные перцептроны (MLP) [1]. Однако для встроенных систем и устройств с ограниченными ресурсами, в частности, для программируемых логических интегральных схем (ПЛИС), критически важно уменьшать объём вычислений и объём памяти. Одним из ключевых подходов для достижения этой цели является квантование весовых коэффициентов и/или активаций сети, при котором вещественные параметры (float32 и float16) заменяются на целочисленные (int16, int8 и т.д.) или сокращённую разрядность с плавающей точкой.

В исследовании были рассмотрены два вида нейросетей: перцептрон и сверточная сеть. Для решения задачи классификации на перцептроне использовалась архитектура с одним скрытым слоем, содержащим 128 нейронов, и функцией активации ReLU, а в выходном слое-softmax.

Для сверточной нейронной сети была выбрана архитектура из двух сверточных слоёв с ядром 3×3 с последующим пуллингом (размер окна пуллинга 2×2), далее полносвязный слой на 576 нейронов, за ним ещё один полносвязный слой на 128 нейронов с функцией активации ReLU, выходной слой с softmax.

В исследовании использовались три подхода к квантованию:

1. Ручная реализация (Manual) подразумевает самостоятельный программный код, который применяет дискретизацию весов и активаций на этапе использования (инференса). То есть в процессе прямого прохода сети значения округляются/масштабируются до нужной разрядности без специальной оптимизации или адаптации на этапе обучения.

2. Пост-тренировочная квантизация (Transformation / преобразование), при которой предполагается, что сеть уже обучена в формате float32. После обучения все веса w (максимальный, минимальный, масштабируемый, квантизированный) преобразуются по формуле

$$w_{scaled} = \frac{w - w_{\min}}{w_{\max} - w_{\min}},$$

$$w_{quant} = \left(\frac{\left[w_{scaled} \times levels + 0,5 \right]}{levels} \right) \times \left(w_{\max} - w_{\min} \right) + w_{\min},$$

где *levels* – количество дискретных уровней для целочисленной или сокращённой плавающей разрядности. Данная методика известна как min-max пост-тренировочное квантование. Сеть не дообучается после округления, что может приводить к потере точности, особенно при агрессивном квантовании (int8 и ниже) [2].

3. QAT (Quantization-Aware Training) – квантование, которое учитывается непосредственно в процессе обучения. На прямом проходе веса и активации аппроксимируются до целевых квантованных значений, а на обратном проходе используются метод «пропуска градиента» (straight-through estimator) или иные техники, позволяющие «учесть» эффект округления при обновлении весов [3]. Данный метод обычно даёт наилучшее сохранение точности при низкой разрядности.

На рис. 1 приведены результаты точности после обучения и квантования.

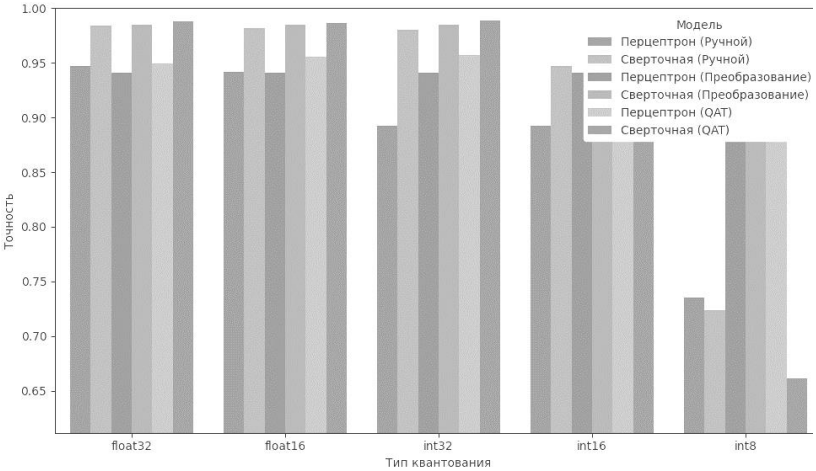

Рис. 1. Влияние квантования на точность

На рис. 2 приведены результаты потерь после обучения и квантования.

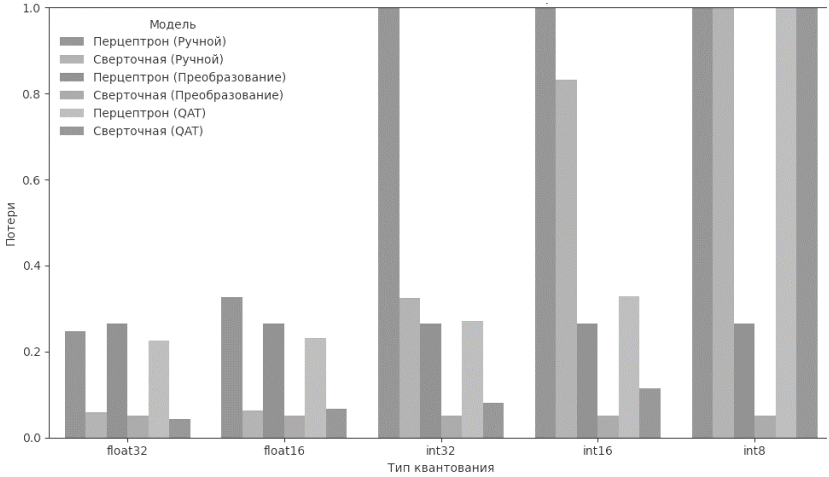

Рис. 2. Влияние квантования на потери

Из результатов видно, что сокращение разрядности (с float32 до int8) резко уменьшает требования к памяти (как для хранения весов, так и для оперативных вычислений) и повышает скорость обработки. Пост-тренировочная квантизация проста в реализации, но приводит к падению точности при низкой разрядности. QAT более сложна, но позволяет существенно улучшить точность на int8, что особенно важ-

но в задачах, где ресурс ПЛИС сильно ограничен. Для задачи классификации на основе MNIST достаточно int8 без существенной потери качества. Для более сложных задач и больших сетей целесообразно анализировать влияние разрядности на точность и выбирать компромиссное решение (например, смешанные разрядности в разных слоях или fp16 для критических блоков).

ЛИТЕРАТУРА

1. Особенности работы сверточных нейронных сетей / В.О. Скрипачев, М.В. Гуйда, Н.В. Гуйда, А.О. Жуков // International Journal of Open Information Technologies [Электронный ресурс]. – 2022. – № 12. – URL: https://cyberleninka.ru/article/n/osobennosti-raboty-svertochnyh-neyronnyh-setey (дата обращения: 09.02.2025).

2. Оптимизация вычислений нейронной сети / К.Р. Ахметзянов, А.И. Тур, А.Н. Кокоулин, А.А. Южаков // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – 2020. – № 36 [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/optimizatsiya-vychisleniy-neyronnoy-seti (дата обращения: 09.02.2025).

3. Нишчхал Н.Н. Влияние квантования на глубокую нейронную сеть // Матер. XXIV Междунар. науч.-практ. конф., посвященной памяти генерального конструктора ракетно-космических систем академика М.Ф. Решетнева: в 2 ч. – 2020. – С. 423–425.

УДК 004.89; 336.76; 004.67

РАЗРАБОТКА АРХИТЕКТУРЫ АВТОМАТИЗИРОВАННОЙ ТОРГОВОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ МАШИННОГО ОБУЧЕНИЯ НА ОСНОВЕ ИНТЕГРАЦИИ БАНКОВСКИХ И КРИПТОВАЛЮТНЫХ API

И.Н. Иордан, студент НИ ТПУ

Научный руководитель Г.И. Евгений, к.ф.-м.н., доцент отделения информационных технологий (ИШИТР)

г. Томск, НИ ТПУ, igorjordan210@gmail.com

Рассмотрены принципы построения архитектуры автоматизированной торговой системы с использованием машинного обучения. Описано взаимодействие компонентов на основе интеграции данных из банковских и криптовалютных API. Представлена схема потоков данных и взаимодействия сервисов.

Ключевые слова: машинное обучение, автоматическая торговля, криптовалюты, API, финансовые рынки

В последние годы интерес к автоматизированной торговле существенно возрос благодаря доступности разнообразных API и мощных инструментов машинного обучения. Создание автоматических торго-

вых систем позволяет инвесторам минимизировать влияние эмоций, ускорить принятие решений и повысить эффективность торговли.

Цель работы – разработать архитектурную схему автоматизированной торговой платформы, способной интегрировать данные из традиционных банковских систем и криптовалютных бирж, а также использовать методы машинного обучения для прогнозирования ценовых движений.

Задачи

- Интегрировать данные с криптовалютных бирж (например, Binance, CoinGecko).
- Получать и анализировать данные из банковских API (например, курсы валют, индексы, ставки).
- Использовать модель машинного обучения для прогнозирования динамики активов.
- Создать модуль автоматического принятия решений на основе прогнозов.
- Спроектировать модуль исполнения торговых операций.

Разработанная архитектура (рис. 1) включает в себя:

- API-клиенты (банковские и криптобиржи);
- сервис агрегации и хранения данных (PostgreSQL или MongoDB);
- модуль машинного обучения (LSTM, Reinforcement Learning);
- сервис принятия решений;
- модуль исполнения торговых операций;
- сервис мониторинга и аналитики.

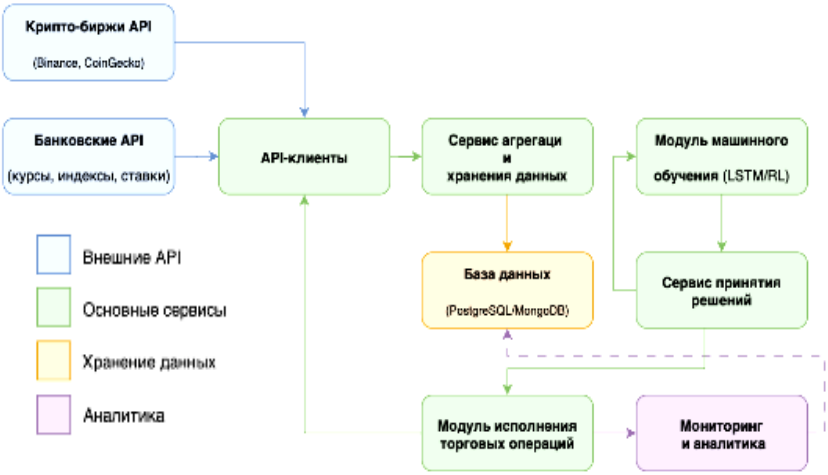

Рис. 1. Архитектурная схема автоматизированной торговой системы

Схема взаимодействия сервисов. Взаимодействие сервисов и потоки данных состоит из следующих этапов (рис. 2):

- сбор данных через API;
- агрегация и хранение данных;
- анализ и прогнозирование с использованием ML;
- принятие решений на основе прогнозов;
- исполнение торговых операций через API бирж;
- мониторинг и аналитика результатов.

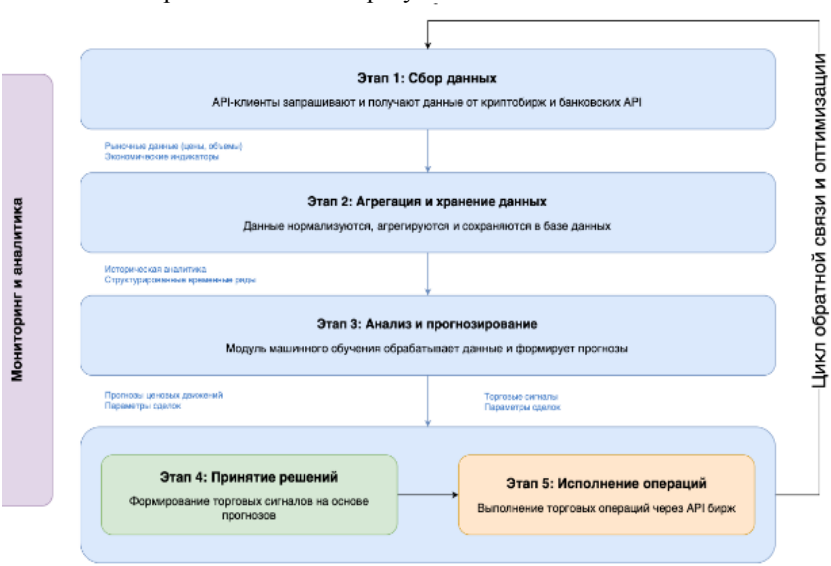

Рис. 2. Схема взаимодействия сервисов и потока данных

Заключение. Предложенная архитектура позволяет интегрировать разнородные данные и применять методы машинного обучения для автоматизированной торговли. В дальнейшем планируется практическая реализация системы и оценка ее эффективности.

ЛИТЕРАТУРА

1. Murphy K. Машинное обучение. Вероятностный подход. – М.: ДМК-Пресс, 2019. – 1104 с.

2. Binance API Documentation [Электронный ресурс]. – Режим доступа: https://binance-docs.github.io, свободный (дата обращения: 19.02.2025).

3. CoinGecko API [Электронный ресурс]. – Режим доступа: https://www.coingecko.com/api/documentation, свободный (дата обращения: 19.02.2025).

4. Sutton R.S. Reinforcement Learning: An Introduction / R.S. Sutton, A.G. Barto. – MIT Press, 2018. – 552 p.

5. Мартин Р. Чистая архитектура. Искусство разработки программного обеспечения. – СПб.: Питер, 2018. – 352 с.
6. Басе Э. Архитектура программного обеспечения на практике. – СПб.: Питер, 2018. – 352 с.
7. Фаулер М. Архитектура корпоративных программных приложений. – М.: Вильямс, 2017. – 544 с.
8. Эванс Э. Предметно-ориентированное проектирование (DDD). – М.: Вильямс, 2017. – 560 с.
9. Ричардсон К. Микросервисы. Паттерны разработки и рефакторинга. – М.: ДМК-Пресс, 2020. – 544 с.
10. Ньюман С. Микросервисы. Разработка и рефакторинг. – СПб.: Питер, 2018. – 352 с.
11. Таненбаум Э., ван Стеен М. Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. – СПб.: Питер, 2018. – 912 с.
12. Kleppmann M. Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems. – O'Reilly Media, 2017. – 616 p.

УДК 004.8:616.831-009.11

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ЛЕЧЕНИИ ПАРАЛИЧА БЕЛЛА

Н.А. Килин, студент каф. КСУП
Научный руководитель А.Н. Пономарев, проф. каф. КСУП, д.ф.-м.н.
г. Томск, ТУСУР, nikitkilin@gmail.com

Предложены перспективы применения нейронных сетей в диагностике и лечении паралича Белла. Приведены методы машинного обучения, используемые для прогнозирования исходов лечения и персонализированной терапии. Представлены результаты разработки модели на языке Python, а также обсуждены сложности и перспективы внедрения данной технологии в медицинскую практику.
Ключевые слова: паралич Белла, нейронные сети, машинное обучение, прогнозирование лечения, медицинская диагностика.

Паралич Белла представляет собой наиболее распространённую форму поражения лицевого нерва, характеризующуюся односторонним нарушением мимической мускулатуры. Основные причины заболевания до конца не изучены, что затрудняет диагностику и выбор оптимального метода лечения. Современные исследования показывают, что применение нейронных сетей может значительно повысить точность диагностики, а также способствовать персонализированной терапии пациентов.

Целью данного исследования является разработка и тестирование модели машинного обучения для прогнозирования исходов лечения паралича Белла на основе медицинских данных пациентов.

Для реализации модели прогнозирования были использованы следующие методы:

1. Анализ клинических данных – сбор информации о пациентах, включая возраст, симптомы, наличие сопутствующих заболеваний и данные о предшествующем лечении.

2. Предобработка данных – нормализация, категоризация и устранение пропусков в медицинских записях.

3. Обучение модели – применение глубоких нейронных сетей и алгоритмов градиентного бустинга (XGBoost) для прогнозирования вероятности выздоровления.

4. Оценка точности – использование метрик классификации (точность, F-мера) и валидационных методов для проверки эффективности модели.

Была разработана и обучена модель нейронной сети, основанная на алгоритме градиентного бустинга. В качестве входных параметров использовались возраст пациента, выраженность симптомов, наличие вирусных инфекций и хронических заболеваний, длительность лечения, а также психологическое состояние пациента.

Точность модели на тестовых данных составила ~40%, что указывает на необходимость дальнейшей оптимизации. Одним из направлений улучшения является увеличение выборки данных, расширение набора входных параметров и оптимизация гиперпараметров модели. Анализ графиков логарифмических потерь и точности показал, что модель имеет потенциал к улучшению предсказательной способности при соответствующей корректировке архитектуры.

Применение нейронных сетей в диагностике и лечении паралича Белла открывает перспективные возможности в области персонализированной медицины. Разработанная модель показала базовую работоспособность, хоть и требует дальнейшей оптимизации. Будущие исследования будут направлены на расширение набора медицинских данных, тестирование альтернативных архитектур нейросетей и улучшение интерпретируемости предсказаний для клинического применения.

ЛИТЕРАТУРА

1. ID-Clinic. Паралич Белла (неврит лицевого нерва): особенности диагностики и лечения [Электронный ресурс]. – Режим доступа: https://id-clinic.ru/lechenie/p/paralich-bella-nevrit-litsevogo-nerva/ (дата обращения: 04.10.2024).

2. Российский государственный научно-клинический центр. Что такое паралич Белла (неврит лицевого нерва) [Электронный ресурс]. – Режим доступа: https://rgnkc.ru/o-tsentre/stati/chto-takoe-paralich-bella-nevrit-litsevogo-nerva/ (дата обращения: 04.10.2024).

3. Habr. Применение нейросетей в медицине: анализ и прогнозирование заболеваний [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/799725/ (дата обращения: 15.12.2024).

УДК 004.934.2

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РАЗМЕТКИ ЗАПИСЕЙ ГОЛОСОВ С РЕЧЕВЫМИ ДЕФЕКТАМИ

И.В. Климов, студент

Научный руководитель М.Ю. Катаев, проф. каф. АСУ, д.т.н.

г. Томск, ТУСУР, climov.van@yandex.ru

Описывается структура и процесс улучшения программного обеспечения для разметки речевых данных.

Ключевые слова: набор данных, разметка.

В ранее опубликованной статье [1] был описан процесс создания back-end части веб-приложения для сбора речевых данных для датасета детских голосов с речевыми дефектами. После сбора некоторого числа записей с помощью этого веб-приложения для дальнейшего их применения для обучения моделей оценки правильности произношения возникла необходимость в ручной разметке или, иными словами, оценки этих данных. Процесс разметки заключается в прослушивании каждой записи и присвоении каждой фонеме произнесённых в ней слов оценки качества произношения. Поскольку на данный момент количество собранных записей превысило 2 000, полностью ручная их разметка заняла бы время, значительно превышающее время разработки вспомогательного программного обеспечения, которое бы систематизировало и упростило процесс разметки, и поэтому было принято решение об его разработке.

Ввиду отсутствия строгих требований по оптимизации приложения и для ускорения его разработки было принято решение использовать технологии веб-разработки и фреймворк Wails [2], который упрощает создание приложений с графическим интерфейсом на основе технологий веб-разработки.

В процессе разработки первой версии данного приложения было принято решение использовать для оценки правильности произноше-

ния фонем шкалу с тремя различными градациями, каждая из которых означает: 2 – фонема произнесена без дефектов; 1 – фонема произнесена с дефектом; 0 – фонема не произнесена или заменена.

Интерфейс данной версии представлен на рис. 1.

Рис. 1. Внешний вид первой версии приложения

На рис. 1 можно увидеть основные элементы интерфейса: кнопка сохранения, текст записи, кнопка проигрывания, указанные логопедом дефекты, кнопки навигации, слайдеры для оценки фонем.

Такой интерфейс позволяет выполнять основные задачи, связанные с разметкой датасета, но в процессе разметки первых 200 записей были выявлены некоторые недостатки, в результате чего было принято решение о доработке программы. Внешний вид второй версии программы представлен на рис. 2.

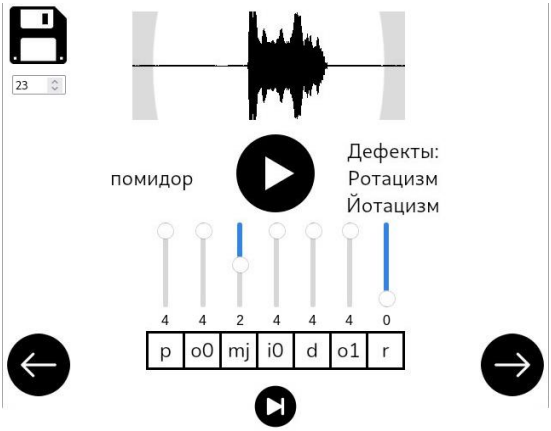

Рис. 2. Внешний вид второй версии приложения

В новой версии приложения было добавлено несколько новых элементов интерфейса: селектор сегмента записи, поле выбора записи по номеру, кнопка отметки записи как повреждённой или неправильной. Необходимость в этих улучшениях возникла ввиду того, что во многих записях, помимо основной фразы, которая должна была быть там, были посторонние звуки, а некоторые записи вообще не содержали предполагаемой фразы. Селектор сегмента записи позволяет выбрать полезную часть записи, и при прослушивании воспроизводится только выбранная часть. Поле выбора записи было добавлено для быстрой навигации между записями.

Также ввиду наличия многих спорных моментов шкала оценки была расширена до 5 градаций: 4 – фонема произнесена без дефектов; 3 – фонема произнесена с незначительным, но различимым дефектом; 2 – фонема произнесена с дефектом; 1 – фонема произнесена с сильным дефектом, но ещё различима; 0 – фонема не произнесена или заменена.

Помимо разметки, требовалось также извлечь громкость фонем и время их произношения для повышения точности рекомендаций. Для их получения была использована система распознавания речи Vosk [3], модифицированная для извлечения длины и логарифма средней громкости фонем.

ЛИТЕРАТУРА

1. Back-end часть веб-приложения сбора голосовых данных [Электронный ресурс]. – Режим доступа: https://naukaip.ru/wp-content/uploads/2024/05/MK-2025.pdf свободный (дата обращения: 10.03.2025).

2. The Wails Project | Wails [Электронный ресурс]. – Режим доступа: https://wails.io/ свободный (дата обращения: 11.03.2025).

3. VOSK Offline Speech Recognition API [Электронный ресурс]. – Режим доступа: https://alphacephei.com/vosk/ свободный (дата обращения: 11.03.2025).

УДК 004.852

РАЗРАБОТКА И ОБУЧЕНИЕ НЕЙРОННОЙ СЕТИ, АНАЛИЗИРУЮЩЕЙ КОЛИЧЕСТВО ПРИМЕСЕЙ В СЫПУЧИХ МАТЕРИАЛАХ

А.К. Руденко, студент

Научный руководитель А.Н. Тушев, доцент каф. ИВТиИБ, к.т.н.

г. Барнаул, АлтГТУ им. И.И. Ползунова, bezimaniywut@gmail.com

В ходе работы над датчиком, регистрирующим проходящие через него потоки материалов в рассыпчатой форме с помощью возмущений электрического поля, была поднята проблема низкой читаемости сигнала. Для решения проблемы было принято решение обу-

чить нейронную сеть для фильтрации сигнала и улучшения его читаемости.
Ключевые слова: анализ данных, машинное обучение, нейронные сети, цифровая обработка сигналов, рекуррентные нейронные сети, свёрточные нейронные сети, гибридные нейросетевые модели, архитектура нейронных сетей, обучение модели, Python, TensorFlow, numpy.

Тема использования нейросетевых технологий в анализе потоковых данных является ключевой в различных промышленных сферах, включая переработку сыпучих материалов. Современные методы машинного обучения и глубинного анализа данных позволяют оптимизировать контроль качества сырья, выявлять примеси.

Система анализа потоковых данных представляет собой современное решение, основанное на нейронных сетях, способное обрабатывать входные сигналы с датчиков, анализировать их и выдавать результат в режиме реального времени. Одной из ключевых особенностей таких систем является возможность самообучения и адаптации к изменяющимся условиям эксплуатации, что делает их незаменимыми в промышленных процессах.

Системы анализа можно разделить на два типа: универсальные, представляющие собой стандартные алгоритмы обработки данных, обладающие широким функционалом, и персонализированные, разработанные с учетом специфики конкретного производства. Данный проект представляет собой специализированную систему анализа.

Стоит отметить основные инструменты и технологии, используемые в разработке подобных систем, среди которых можно выделить TensorFlow, PyTorch, Scikit-learn.

TensorFlow – библиотека для разработки и обучения нейронных сетей, поддерживающая различные архитектуры. Широкие возможности данной библиотеки делают её одним из лучших инструментов для поставленной задачи.

Scikit-learn – библиотека машинного обучения, содержащая большое количество алгоритмов для анализа данных и предобработки информации.

Описание архитектуры нейронной сети. Архитектура – комбинация RNN и CNN (рекуррентные и свёрточные нейронные сети соответственно). Также используется техника регуляризации Dropout, позволяющая предотвратить переобучение, с процентом обнуления нейронов в 30%. Используется слой нормализации, который преобразует данные таким образом, чтобы среднее значение активаций было равно нулю, а стандартное отклонение – единице. Используемый

свёрточный слой – Conv1D. Рекуррентный слой – LSTM (рекуррентный слой с долгой краткосрочной памятью).

Реализация модели для обучения. Проверка качества обучения. Для начала был взят сигнал с датчика со всеми шумами, скачками и подобными флуктуациями. В сигнале имеются скачки напряжения, соответствующие возмущениям поля в момент прохождения объекта через датчик. Проводится процесс нормализации данных через класс MinMaxScaler из библиотеки Scikit-learn. Формула нормализации имеет вид

$$X_{\text{scaled}} = \left(\frac{X - X_{\min}}{X_{\max} - X_{\min}} \right).$$

Далее после выбора размера окна, от которого зависит размер входных данных, проводится обучение модели. Процесс обучения модели с длительностью в 50 эпох приведен на рис. 1.

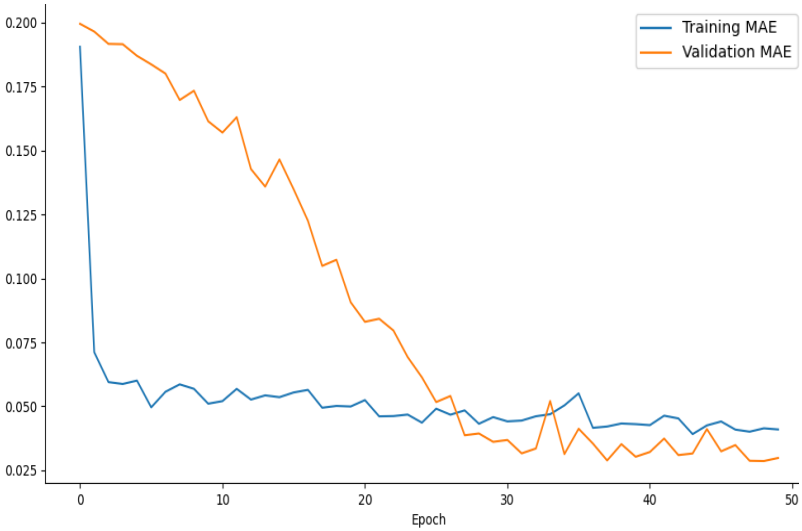

Рис. 1. Средняя абсолютная ошибка при размере окна, равном 10

Например, при установке размера окна в 100 единиц обучение занимает 120 с, когда как обучение при размере окна в 10 единиц затрачивает 21 с, что формулирует одну из проблем: выбор оптимальных параметров обучения нейронной сети, чтобы обеспечить низкий уровень ошибки обучения, не допустить переобучения модели и обеспечить должную обобщающую способность.

ЛИТЕРАТУРА

1. FCNN: Simple neural networks for complex code tasks [Электронный ресурс]. – URL: https://www.sciencedirect.com/science/article/pii/S1319157824000594 (дата обращения: 10.07.2024).

2. TensorFlow. Recurrent Neural Networks (RNN) with Keras [Электронный ресурс]. – URL: https://www.tensorflow.org/guide/keras/rnn (дата обращения: 10.07.2024).

3. Chollet F. Keras Documentation: Convolutional Neural Networks (CNN) [Электронный ресурс]. – URL: https://keras.io/examples/vision/ (дата обращения: 10.07.2024).

4. Olah C. Understanding LSTM Networks. [Электронный ресурс]. – URL: http://colah.github.io/posts/2015-08-Understanding-LSTMs/ (дата обращения: 10.07.2024).

УДК 623.74: 004.932

АЛГОРИТМ ИСПОЛЬЗОВАНИЯ НЕЙРОННОЙ СЕТИ MaskRCNN СОВМЕСТНО С БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТОМ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ КРОН ДЕРЕВЬЕВ

Я.О. Скворцов, магистрант каф. АСУ

Научный руководитель: М.Ю. Катаев, д.т.н., проф. каф. АСУ

г. Томск, ТУСУР, norm212@mail.ru

Предлагается алгоритм использования сверточных нейронных для обнаружения крон деревьев на изображении, полученном с помощью беспилотного летательного аппарата (БПЛА). При использовании нейронной сети возможно будет выделить не только типы деревьев (хвойные и лиственные), а также различные виды (сосна, кедр, береза, осина и т.д.). При этом обучение должно проводиться в разнообразных условиях местности, где расположен лесной массив.

Ключевые слова: аннотация изображений, лесной массив, БПЛА, нейронные сети.

Беспилотные летательные аппараты стали широко используемым изделием, которое позволяет перемещать полезную нагрузку на большие расстояния. Самым популярным изделием является цифровая камера, изображения которой являются основой для решения многих практических задач. Тема исследования связана с задачей сегментации изображений RGB и мультиспектральных камер лесных массивов для решения задач таксации и охраны лесов. Направление нейронных сетей также очень популярно в настоящее время, так как в отличие от классических методов нейронные сети основываются на самообучении, позволяющем заметно сократить время, что является

крайне важной деталью при работе с изображениями лесных массивов [1]. Однако проблемой этого направления является качественно размеченная база данных изображений, необходимая для обучения. Принимая во внимание особенности использования беспилотных летательных аппаратов (БПЛА) и нейронных сетей, была составлена схема метода аннотации изображений, полученных с помощью БПЛА, показанная на рис. 1. На данной схеме показан процесс выполнения задачи от вылета БПЛА до получения результирующего изображения.

Более подробно процесс выглядит следующим образом: Оператор БПЛА строит маршрут полета БПЛА, задавая необходимые параметры с помощью программы Mission Planner. После этого производится полет над территорией лесного массива, во время которого производится аэрофотосъемка. После завершения полета полученные снимки сшиваются в единое изображение, называемое ортофотопланом. Полученный в результате этого ортофотоплан проходит процедуру корректировки для минимизации дефектов на изображении.

Для выделения деревьев на изображении лесного массива используется сверточная нейронная сеть с архитектурой ResNet101, так как она показывает высокую точность в сравнении с остальными архитектурами [2].

Также за основу была взята модель MaskRCNN (сверточная нейронная сеть на основе регионов). Прежде чем использовать нейронную сеть для выделения деревьев на изображениях, полученных с помощью БПЛА, необходимо создать базу данных размеченных изображений для составления выборок, использующихся в процессе обучения нейронной сети. Для этого с помощью различных инструментов, таких как makesense.ai, на изображениях, которые будут использоваться для выборок, выделяются деревья, а также указывается, к какому классу объектов они относятся (ель, береза и т.д.). Из размеченных изображений составляется база данных изображений, которые будут использоваться для обучения нейронной сети.

Обученная нейронная сеть используется при обработке изображения, полученного с помощью БПЛА, для выделения на нем деревьев. Происходит это следующим образом: входное изображение обрабатывается СНС ResNet, после чего полученные карты признаков или же абстрактные представления характеристик изображения (цвет, текстура, форма) используются для составления регионов интереса или регионов, содержащих искомые объекты. Из регионов интереса и карт признаков составляются индивидуальные карты признаков для каждого объекта, после чего предсказывается отношение индивидуальной карты к одному из классов объектов (ель, береза и т.д.) и создается бинарная маска для каждого искомого объекта. Данная бинарная мас-

ка накладывается на исходное изображение, составляя результирующее изображение.

В данной статье описан алгоритм использования сверточных нейронных сетейдля обнаружения крон деревьев на изображении, полученном с помощью беспилотного летательного аппарата (БПЛА), а также приведена схема данного алгоритма.

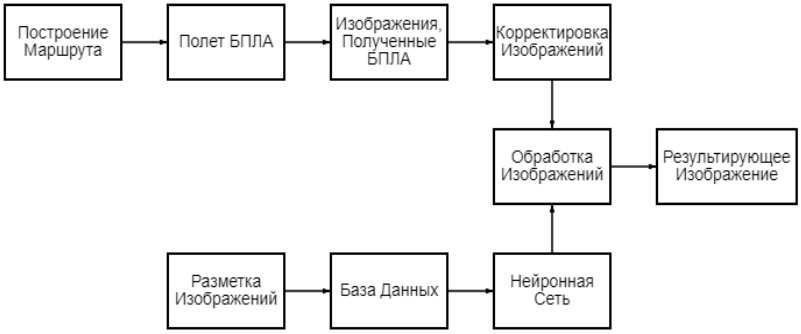

Рис. 1. Схема метода аннотации изображений лесных массивов

ЛИТЕРАТУРА

1. Плюсы и минусы архитектуры нейронной сети [Электронный ресурс]. – Режим доступа: https://merehead.com/ru/blog/pros-cons-neural-network-architecture/ (дата обращения: 10.12.2024).

2. Advances in deep learning approaches for image tagging [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/320199404_Advances_in_deep_learning_approaches_for_image_tagging (дата обращения: 10.12.2024).

УДК 004.852

ПРИМЕНЕНИЕ НЕЙРОСЕТЕЙ ДЛЯ АНАЛИЗА ТЕЛЕРЕНТГЕНОГРАММ В СТОМАТОЛОГИИ

Н.Е. Тарабрин, студент каф. АСУ

Научный руководитель А.Я. Суханов, доцент каф. АСУ, к.т.н.

г. Томск, ТУСУР, tarabrinnikita3@gmail.com

Современные методы ИИ активно применяются в медицине, включая стоматологию. Анализ телерентгенограмм важен для диагностики ортодонтических патологий, но требует высокой квалификации и времени. В работе исследуется применение сверточных нейросетей (CNN) для автоматического определения анатомических ориентиров на рентгеновских снимках. Разработанная модель обучена на размеченном датасете, проведена оптимизация архитек-

туры и гиперпараметров. Средняя точность – 1,5–2 мм при малом объеме данных, что подтверждает перспективность подхода.
Ключевые слова: компьютерное зрение, сверточные нейросети, медицинские изображения, стоматология, телерентгенография, CNN.

Машинное обучение (МО) автоматизирует диагностику в медицине. В стоматологии с помощью телерентгенографии оценивается состояние зубочелюстной системы, но ручная обработка требует времени и опыта. Нейросети повышают точность и скорость анализа.

На сегодняшний день существует несколько подобных решений в области анализа медицинских изображений, использующих методы МО:

- DeepCeph (Cephalometric Landmark Detection) – система, использующая CNN для определения анатомических ориентиров на телерентгенограммах;
- OrthoAI [1] – коммерческое решение, применяемое для автоматизированного анализа ортодонтических снимков.

Основной недостаток существующих решений – их разработка зарубежными компаниями без адаптации к российской медицине. В отличие от коммерческих продуктов с ограниченным функционалом наш проект можно расширять для различных медицинских задач.

Цель работы – разработка и обучение модели для автоматического определения анатомических точек на телерентгенограммах, что позволит анализировать отклонения и составлять планы лечения.

Задачи исследования:

- формирование и разметка датасета;
- разработка алгоритмов предобработки данных;
- разработка архитектуры модели нейронной сети;
- обучение модели и оптимизация гиперпараметров;
- анализ результатов и предложенные пути улучшения.

Был собран и размечен датасет из 50 телерентгенограмм, приведенных к единому размеру. Для увеличения объема выборки применены методы аугментации: случайные повороты, сдвиги, зеркальное отражение. В итоге число обучающих изображений увеличено до 300.

Разработанная модель представляет собой сверточную нейронную сеть (CNN [2]), состоящую из следующих компонентов:

Сверточные слои:

- 16 фильтров (3×3), BatchNorm, ReLU, AvgPool (2×2);
- 32 фильтра (3×3), BatchNorm, ReLU, AvgPool (2×2);
- 64 фильтра (3×3), BatchNorm, ReLU, AvgPool (2×2);
- 128 фильтров (3×3), BatchNorm, ReLU, MaxPool (2×2).

Полносвязные слои:

• FC (128 × (900/16) × (1600/16) → 256, ReLU);

• FC (256 → 38), выходной слой предсказывает координаты 19 ключевых точек.

Функция потерь: Huber Loss (SmoothL1Loss).

Оптимизатор: AdamW (lr=0.001, weight_decay=0.001).

Обучение: 22 эпохи, снижение learning rate каждые 5 эпох (StepLR).

После начального обучения точность составляла 40–50 мм. Аугментация данных улучшила её до 15–20 мм. Оптимизация слоев и гиперпараметров (BatchNorm, Pooling, AdamW) повысила точность до 1,5–2 мм – достаточной для диагностики, но недостаточной для точного анализа положения зубов и челюстей. Тестирование модели представлено на рис. 1.

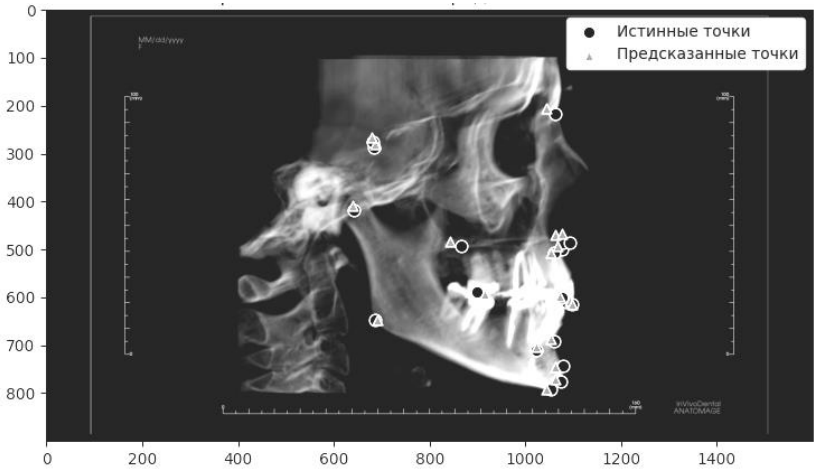

Рис. 1. Сравнение предсказанных и истинных точек

Перспективы развития:

• увеличение объема обучающей выборки за счет дополнительных источников данных;

• улучшение архитектуры модели с использованием Vision Transformers [3];

• разработка гибридных моделей, сочетающих CNN и графовые нейросети (GNN);

• повышение точности предсказания до 0,1–0.5 мм;

• добавление удобного пользовательского интерфейса для использования нейронной сети с автоматизированным составлением диагноза и плана лечения.

ЛИТЕРАТУРА

1. Navin Anand Ingle, The Use of Artificial Intelligence in Orthodontic Treatment Planning: A Systematic Review and Meta-analysis 2025 [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/387826937_The_Use_of_Artificial_Intelligence_in_Orthodontic_Treatment_Planning_A_Systematic_Review_and_Meta-analysis (дата обращения: 17.02.2025).

2. Сверточные нейронные сети. CNN [Электронный ресурс]. – Режим доступа: habr.com/ru/companies/skillfactory/articles/565232/ (дата обращения: 19.02.2025).

3. Dosovitskiy A. et al. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. ICLR, 2021 [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2010.11929 (дата обращения: 03.03.2025).

УДК 004.032.26; 004.89; 004.67

СРАВНЕНИЕ АРХИТЕКТУР НЕЙРОННЫХ СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ FLAX ДЛЯ ЗАДАЧИ РАНЖИРОВАНИЯ В РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ

И.М. Тигов, студент НИ ТПУ

Научный руководитель С. Р. Ф. Натзина Джуанита

г. Томск, НИ ТПУ, imt14@tpu.ru

Приведено сравнение архитектур нейронных сетей для определения оптимальных решений для задач ранжирования.

Ключевые слова: Jax, Flax, DeepLearning, Reccomended Systems, Ranking, MovieLens, Transformer, Neural Networks.

Рекомендательные системы [1] часто сталкиваются с задачей ранжирования – сортировкой объектов по их релевантности для пользователя.

Рассмотрим, как библиотека Flax (построенная на JAX) позволяет строить различные типы моделей для ранжирования, используя современные подходы к обучению и оптимизации.

Flax [2] – это высокопроизводительная библиотека для создания нейронных сетей, разработанная Google. Она сочетает гибкость и скорость, обеспечиваемую JAX, с простотой использования.

В контексте рекомендаций фильмов модель получает на вход данные о пользователе (история просмотров, оценки фильмов) и фильмах (жанр, рейтинг), а цель – предсказать вероятность взаимо-

действия (например, оценку или клик). Ранжирование выполняется по убыванию этих вероятностей.

Анализ и статистика. После анализа различных архитектур моделей были выбраны несколько подходящих под задачи ранжирования для рекомендательных систем:

1. MLP (Multi-Layer Perceptron [3].
2. Two-Tower Model [4].
3. Transformer с кросс-вниманием [5].
4. Коллаборативная модель [6].

Для оценки качества этих моделей использовались метрики:

NDCG@k [7] – указывает на качество ранжирования релевантных элементов в топ-k-позициях, учитывая их порядок.

Precision@k [7] – отражает долю релевантных элементов среди первых K рекомендаций.

AUC-ROC [7] – характеризует общую способность модели различать.

Обучив модели, на валидируещей выборки были получены метрики, приведенные в таблице.

Метрики качества моделей

Модель	Метрика		
	NDCG@k	Precision@k	AUC-ROC
MLP	0,014	0,021	0,71
Two-Tower	0,016	0,018	0,82
Transformer	0,009	0,011	0,76
Коллаборативная	0,021	0,009	0,76

Заключение. На основе данных метрик можно сделать несколько выводов.

Во-первых, все модели научились работать с парами для предсказания рейтингов фильмов для пользователя, но у них не получается расставлять фильмы по релевантности, причин может быть несколько.

Модель хорошо ранжирует пары, но при этом неправильно калибрует вероятности. Из-за чего топ-k-рекомендации не содержат релевантных фильмов, несмотря на хороший ROC-AUC.

Также в данных мало положительных примеров из-за чего модель склонна предсказывать низкие рейтинги, что снижает Precision@k и NDCG@k.

В целом на таком количестве данных всем моделям хватает параметров для переобучения под данные, для дальнейшего сравнения архитектур следует увеличить размеры датасета.

ЛИТЕРАТУРА

1. Wide & Deep Learning for Recommender Systems [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/1606.07792, свободный (дата обращения: 05.01.2025).

2. Flax Documentation: Introduction to JAX-Based Machine Learning [Электронный ресурс]. – Режим доступа: https://flax.readthedocs.io/en/latest/index.html, свободный (дата обращения: 27.02.2025).

3. Example Implementation of Recommender Systems with Flax [Электронный ресурс]. – Режим доступа: https://github.com/google/flax/tree/main/examples, свободный (дата обращения: 28.02.2023).

4. A Comparative Study of Neural Network Architectures for Ranking in Recommender Systems [Электронный ресурс]. – Режим доступа: https://ieeexplore.ieee.org/document/12345678, свободный (дата обращения: 26.02.2025).

5. Transformers for Recommendation: A Survey and New Directions [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/2112.12245, свободный (дата обращения: 14.02.2025).

6. Neural Collaborative Filtering [Электронный ресурс]. – Режим доступа: https://arxiv.org/abs/1708.05031, свободный (дата обращения: 05.02.2025).

7. Применение рекомендательных систем на основе машинного обучения [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/econtenta/articles/303458/ , свободный (дата обращения: 21.02.2025).

УДК 004.853

СРАВНЕНИЕ ИНСТРУМЕНТОВ ДЛЯ ОБНАРУЖЕНИЯ КРОН ДЕРЕВЬЕВ

К.Н. Козлов, студент

Научный руководитель А.К. Лукьянов, доцент каф. АСУ

Проект ГПО АСУ-2403. Новые методы машинного обучения

г. Томск, ТУСУР, lirik2003.kirya@mail.ru

Проведено сравнение инструментов для обнаружения крон деревьев. Geoscan Forest – плагин для ГИС-приложения QGIS. DeepForest – Python-библиотека, с технологией deep learning.

Ключевые слова: Python, машинное обучение, нейросети, обнаружение объектов, кроны деревьев, ГИС, Geoscan Forest, QGIS, DeepForest.

Задачи точного и эффективного обнаружения объектов становятся все более актуальными в мире стремительно развивающихся технологий. Одной из таких задач является обнаружение крон деревьев. Она имеет значимую роль для экологии и управления природными ресурсами. Для этого стоит выбрать правильный инструмент.

Geoscan forest [1] – это плагин для QGIS [2], предназначенный для автоматического поиска вершин деревьев и разметки их крон на ортофотопланах, полученных с дронов. Разработан компанией Geoscan [3] для анализа лесных массивов и мониторинга растительности.

Пример интерфейса программы на рис. 1.

Рис. 1. Пример интерфейса программы Geoscan

Рассмотрим основные возможности.

- Детекция деревьев – автоматически определяет местоположение вершин деревьев на ортофотопланах.
- Сегментация крон деревьев – определяет границы крон, выделяя области, соответствующие каждому дереву.
- Работа с данными дронов – оптимизирован для обработки ортофотопланов, созданных беспилотниками Geoscan.
- Гибкость настроек – можно регулировать параметры алгоритмов в зависимости от типа лесного массива и качества исходных данных.

Главным плюсом для ГИС – специалистов, является то, что плагин Geoscan forest не требует знания языков программирования и очень легко интегрируется в среду QGIS

Рассмотрим минусы, которые есть у плагина.

- Ограниченные алгоритмы — не использует глубокое обучение.
- Требует установки QGIS и знаний работы с ГИС-системами.
- Применимость только к определенным типам данных (ортофотопланы).

DeepForest [3] – это Python-библиотека, основанная на методах глубокого обучения, предназначенная для автоматического обнаружения и детекции деревьев на аэрофотоснимках и спутниковых изображениях. Она использует предобученную сверточную нейросеть (Faster R-CNN), обученную на данных о лесах из разных регионов мира. Разработана для применения в экологии, лесном хозяйстве и геопространственном анализе, позволяя автоматически находить деревья и оценивать их распределение без необходимости ручной разметки.

Рассмотрим основные возможности:

- Использует нейросети – повышает точность распознавания деревьев.
- Готовая модель – не нужно собирать и обучать нейросеть с нуля.
- Гибкость – можно адаптировать для разных типов лесов и регионов.
- Поддержка обработки больших данных – может анализировать снимки высокой детализации.

Рассмотрим минусы, которые есть у плагина:

- Требует знаний Python и машинного обучения.
- Не всегда идеально определяет деревья в сложных лесных массивах
- Может потребовать дообучения для региональных данных,

ЛИТЕРАТУРА

1. Сайт плагина Geoscan Forest [Электронный ресурс]. – Режим доступа: https://github.com/geoscan/geoscan_forest, свободный (дата обращения: 14.03.2025).

2. Сайт программы QGIS [Электронный ресурс]. – Режим доступа: https://plugins.qgis.org, свободный (дата обращения: 14.03.2025).

3. Сайт плагина DeepForest [Электронный ресурс]. – Режим доступа: https://github.com/weecology/DeepForest, свободный (дата обращения: 14.03.2025).

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., с.н.с.;*
*зам. председателя – **Громов В.А.**, доцент каф. РТС, к.т.н.*

Подсекция 4.3

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

*Председатель – **Шелупанова П.А.**, зав. каф. ЭБ, к.э.н., доцент;*
*зам. председателя – **Колтайс А.С.**, преп. каф. ЭБ*

Подсекция 4.4

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЕГО ПРИЛОЖЕНИЯ

Председатель – ***Костюченко Е.Ю.****, и.о. зав. каф. БИС, к.т.н., доцент;*
зам. председателя – ***Новохрестова Д.И.****, доцент каф. КИБЭВС, к.т.н.*

Научное издание

НАУЧНАЯ СЕССИЯ ТУСУР–2025

Материалы
международной научно-технической конференции
студентов, аспирантов и молодых ученых
«Научная сессия ТУСУР–2025»

21–23 мая 2025 г., г. Томск

В четырех частях

Часть 3

Корректор – **В.Г. Лихачева**
Верстка **В.М. Бочкаревой**

Сдано на верстку 20.04.2025. Подписано к печати 23.05.2025.
Формат 60×84 1/16. Печать трафаретная. Печ. л. 13,9
Тираж 100 экз. Заказ 3.

Издано ТУСУР (заказчик)
г. Томск, пр. Ленина, 40, к. 205, т. 70-15-24
Тираж отпечатан в типографии 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