МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
МЕЖДУНАРОДНАЯ АКАДЕМИЯ ИНФОРМАТИЗАЦИИ
СОЮЗ МАШИНОСТРОИТЕЛЕЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ РЯЗАНСКОЙ ОБЛАСТИ
РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ

СТНО-2026

IX МЕЖДУНАРОДНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ФОРУМ

Сборник трудов

Том 3

Рязань
2026

УДК 004 + 001.1 + 681.2+ 681.2+ 681.3+681.5
С 568

Современные технологии в науке и образовании – СТНО-2026 [текст]: сб. тр. IX междунар. науч.-техн. форума: в 11 т. Т.3./ под общ. ред. О.В. Миловзорова. – Рязань: Рязан. гос. радиотехн. ун-т, 2026.

ISBN 978-5-7722-0443-6

Т.3: – 254 с.,: ил.

ISBN 978-5-7722-0446-7

Сборник включает труды участников IX Международного научно-технического форума «Современные технологии в науке и образовании» СТНО-2026.

В сборнике освещаются вопросы математического моделирования, новых технологий в радиотехнике, телекоммуникациях, электротехнике и радиоэлектронике, вопросы полупроводниковой наноэлектроники, приборостроения, лазерной, микроволновой техники, силовой промышленной электроники, новые технологии в измерительной технике и системах, биомедицинских системах, алгоритмическое и программное обеспечение вычислительной техники, вычислительных сетей и комплексов, вопросы разработки и применения элементов искусственного интеллекта в информационных системах и образовании, различные аспекты автоматизированного проектирования, обработки изображений и управления в технических системах, перспективные технологии в машиностроительном и нефтехимическом производствах, новые технологии и методики в высшем образовании, в т.ч. вопросы гуманитарной и физико-математической подготовки студентов, обучения их иностранным языкам, перспективные технологии электронного обучения, в том числе, дистанционного, вопросы экономики, управления предприятиями и персоналом, менеджмента, а также вопросы гуманитарной сферы.

Авторская позиция и стилистические особенности сохранены.

УДК 004 + 001.1 + 681.2+ 681.2+ 681.3+681.5

ISBN 978-5-7722-0443-6

© Рязанский государственный
радиотехнический университет, 2026

ISBN 978-5-7722-0446-7

ИНФОРМАЦИЯ О IX МЕЖДУНАРОДНОМ ФОРУМЕ «СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ» СТНО-2026

IX Международный научно-технический форум «Современные технологии в науке и образовании» СТНО-2026 состоялся 03.03.2026-05.03.2026 в г. Рязань в Рязанском государственном радиотехническом университете имени В.Ф. Уткина.

В рамках форума «Современные технологии в науке и образовании» СТНО-2026 состоялась работа четырех Международных научно-технических конференций:

«Современные технологии в науке и образовании. Радиотехника и электроника», секции

- Радиотехнические системы;
- Радиотехнические устройства;
- Телекоммуникационные системы и устройства;
- Цифровые информационные технологии реального времени;
- Промышленная силовая электроника, электроэнергетика и электроснабжение;
- Физика полупроводников, микро- и наноэлектроника;
- Микроволновая, оптическая и квантовая электроника;
- Актуальные задачи химических технологий;

«Современные технологии в науке и образовании. Вычислительная техника, математическое моделирование и автоматизированные системы», секции

- Алгоритмическое и программное обеспечение вычислительных систем и сетей;
- Искусственный интеллект и информационные технологии;
- ЭВМ и системы;
- Модели искусственного интеллекта в САПР;
- Информационные технологии в конструировании электронных средств;
- Интеллектуальные системы и технологии в образовании;
- Информационные системы и защита информации;
- Математические методы и модели в научных исследованиях и прикладных проблемах. К 90-летию И.П. Карасева - основателя теории управления "в малом";
- Обработка данных, изображений и управление в технических системах;
- Геоинформационные и космические технологии;
- Автоматизация производственно-технологических процессов в приборо- и машиностроении;
- Информационно-измерительные устройства и системы в технике и медицине.
- Стандартизация и управление качеством;
- Информационные системы и технологии;

«Современные технологии в науке и образовании. Экономика и управление», секции;

- Современные технологии государственного и муниципального управления;
- Экономика, менеджмент и организация производства;
- Бухгалтерский учет, анализ и аудит;
- Экономическая безопасность;

«Современные технологии в науке и образовании. Новые технологии и методы в высшем образовании», секции

- Современные технологии электронного обучения;
- Иностранный язык в техническом вузе;
- Лингвистика и межкультурная коммуникация;
- Направления и формы гуманитаризации высшего образования и гуманитарная подготовка студентов;
- Методы преподавания и организация учебного процесса в вузе;
- Физико-математическая подготовка студентов;

- Особенности военного образования на современном этапе.

Организационный комитет Форума:

Гусев С.И., проректор по научной работе и инновациям, д.т.н., проф.;

Миловзоров О.В., зам. начальника управления организации научных исследований, к.т.н, доц. – координатор, главный редактор сборника трудов Форума;

Миронов Вал.В., профессор кафедры высшей математики, д.ф.-м.н., проф. – ответственный редактор сборника трудов Форума;

Устинова Л.С., начальник отдела информационного обеспечения – отв. за информационную поддержку;

члены оргкомитета:

Аронов Л.В., доцент кафедры радиоуправления и связи, к.т.н., доц.;

Бабаян П.В., зав. кафедрой автоматики и информационных технологий в управлении, к.т.н., доц.;

Бубнов С.А., доцент кафедры вычислительной и прикладной математики, к.ф.-м.н., доц.;

Витязев В.В., зав. кафедрой телекоммуникаций и основ радиотехники, д.т.н., проф.;

Волченков В.А., доцент кафедры телекоммуникаций и основ радиотехники, к.т.н.;

Горлин О.А., доцент кафедры электронных приборов, к.т.н., доц.;

Городничева Е.В., ассистент кафедры автоматизации информационных и технологических процессов;

Гостин А.М., доцент кафедры систем автоматизированного проектирования вычислительных средств, к.т.н., доц.;

Губарев А.В., доцент кафедры информационно-измерительной и биомедицинской техники, к.т.н., доц.;

Гуржин С.Г., доцент кафедры информационно-измерительной и биомедицинской техники, к.т.н., доц.;

Дмитриев В.Т., зав. кафедрой радиоуправления и связи, д.т.н., доц.;

Дмитриева Т.А., доцент кафедры вычислительной и прикладной математики, к.т.н., доц.;

Евдокимова Е.Н., зав. кафедрой экономики, менеджмента и организации производства, д.э.н., проф.;

Еремеев В.В., директор НИИ «Фотон», д.т.н., проф.;

Есенина Н.Е., зав. кафедрой иностранных языков, к.п.н., доц.;

Жулев В.И., зав. кафедрой информационно-измерительной и биомедицинской техники, д.т.н., проф.;

Каширин И.Ю., доктор технических наук, профессор, профессор кафедры вычислительной и прикладной математики, д.т.н., проф.;

Киселёва О.В., доцент кафедры экономической безопасности, анализа и учета, к.э.н., доц.;

Кислицына Т.С., старший преподаватель кафедры радиотехнических систем;

Клейносова Н.П., директор центра дистанционного обучения, к.п.н., доц.;

Клочко В.К., профессор кафедры автоматики и информационных технологий в управлении, д.т.н., проф.;

Коваленко В.В., зав. кафедрой химической технологии, к.т.н., доц.;

Корячко В.П., зав. кафедрой систем автоматизированного проектирования вычислительных средств, д.т.н., проф.;

Костров Б.В., зав. кафедрой электронных вычислительных машин, д.т.н., проф.;

Кошелев В.И., зав. кафедрой радиотехнических систем, д.т.н., проф.;

Крошилина С.В., доцент кафедры вычислительной и прикладной математики, к.т.н., доц.;

Круглов С.А., зав. кафедрой промышленной электроники, д.т.н., доц.;

Кузьмин Ю.М., доцент кафедры информационной безопасности, к.т.н., доц.;

Куприна О.Г., доцент кафедры иностранных языков, к.филол.н., доц.;

Ленков М.В., зав. кафедрой автоматизации информационных и технологических процессов, к.т.н., доц.;

Литвинов В.Г., зав. кафедрой микро- и наноэлектроники, д.ф.-м.н., доц.;

Лукьянова Г.С., зав. кафедрой высшей математики, к.ф.-м.н., доц.;

Маметова Ю.Ф., доцент кафедры иностранных языков, к.п.н., доц.;

Миронов В.В., старший преподаватель кафедры Воздушно-космических сил;

Митрошин А.А., доцент кафедры систем автоматизированного проектирования вычислительных средств, к.т.н., доц.;

Мишустин В.Г., доцент кафедры микро- и наноэлектроники, к.ф.-м.н., доц.;

Овечкин Г.В., зав. кафедрой вычислительной и прикладной математики, д.т.н., проф.;

Паршин А.Ю., доцент кафедры радиотехнических устройств, к.т.н., доц.;

Паршин Ю.Н., зав. кафедрой радиотехнических устройств, д.т.н., проф.;

Перфильев С.В., зав. кафедрой государственного, муниципального и корпоративного управления, д.э.н., проф.;

Подгорнова Н.А., доцент кафедры государственного, муниципального и корпоративного управления, к.э.н., доц.;

Пржегорлинский В.Н., зав. кафедрой информационной безопасности, к.т.н., доц.;

Пылькин А.Н., профессор кафедры вычислительной и прикладной математики, д.т.н., проф.;

Саблина В.А., доцент кафедры электронных вычислительных машин, к.т.н., доц.;

Сапрыкин А.Н., доцент кафедры систем автоматизированного проектирования вычислительных средств, к.т.н., доц.;

Семенов А.Р., доцент кафедры химической технологии, к.ф.-м.н.;

Скрипкина О.В. доцент кафедры экономической безопасности, анализа и учета, к.э.н., доц.;

Соколов А.С., зав. кафедрой истории, философии и права, д.и.н;

Соловьева И.П., доцент кафедры экономики, менеджмента и организации производства, к.э.н., доц.;

Таганов А.И., профессор кафедры космических технологий, д.т.н., проф.;

Тарасова В.Ю., ассистент кафедры электронных вычислительных машин, магистр;

Торженова Т.В. доцент кафедры экономической безопасности, анализа и учета, к.э.н., доц.;

Харитонов А.Ю., нач. военного учебного центра, полковник, к.т.н., доц;

Холопов С.И., зав. кафедрой автоматизированных систем управления, к.т.н., доц.;

Цыцына М.И., ассистент кафедры космических технологий, магистр;

Чеглакова С.Г., зав. кафедрой экономической безопасности, анализа и учета, д.э.н., проф.;

Челебаев С.В., доцент кафедры автоматизированных систем управления, к.т.н., доц.;

Щевьев А.А., доцент кафедры истории, философии и права, к.п.н., доц.

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ. РАДИОТЕХНИКА И ЭЛЕКТРОНИКА»

СЕКЦИЯ «ЦИФРОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РЕАЛЬНОГО ВРЕМЕНИ»

УДК 621.372.542; ГРНТИ 47.05.17

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ БПФ НА ПЛИС: ДОБАВЛЕНИЕ АЛГОРИТМА ЦОС В ПРОЕКТ СБОРА ДАННЫХ

Н.О. Кудимов

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, kudimov.edu@yandex.ru

Аннотация. В данной работе является представлены исследования по реализации системы цифровой обработки сигналов на ПЛИС. На основе созданного ранее проекта с работоспособными модулями пред- и постобработки для интерфейса JESD204B выполняется интеграция алгоритма БПФ. Рассматриваются этапы добавления весовой функции, IP-ядра БПФ в среде Vivado и организации обработки данных ЦАП-АЦП.

Ключевые слова: *ПЛИС, ЦОС, БПФ, спектральный анализ, JESD204B, Vivado, IP-ядро.*

PRACTICAL IMPLEMENTATION OF FFT ON FPGA: ADDING A DSP ALGORITHM TO A DATA ACQUISITION PROJECT

N.O. Kudimov

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, kudimov.edu@yandex.ru

Abstract. This paper research on the implementation of a digital signal processing system on FPGAs is presents. Building upon a pre-existing project with operational modules for JESD204B interface pre- and post-processing, the work focuses on integrating a Fast Fourier Transform (FFT) algorithm. The paper details the implementation steps, including incorporating a window function, configuring the FFT IP core within the Vivado design suite, and establishing a complete DAC-ADC data processing chain.

Keywords: FPGA, DSP, FFT, spectral analysis, JESD204B, Vivado, IP core.

Введение

В первой части данного исследования [1] была представлена архитектура системы цифровой обработки сигналов на базе программируемой логической интегральной схемы (ПЛИС) и модуля FMC133V. В работе проведен детальный анализ ключевых компонентов платформы, таких как высокоскоростной аналого-цифровой преобразователь (АЦП) AD9680, встроенный цифровой понижающий преобразователь (DDC) и высокоскоростной последовательный интерфейс передачи данных JESD204B. Основным практическим результатом стала успешная разработка и отладка специализированных модулей предварительной и последующей обработки. Эти модули сформировали надежный цифровой конвейер, гарантирующий передачу оцифрованных данных от АЦП без потерь и искажений.

Данная статья является логическим завершением проекта и посвящена ключевому этапу – интеграции алгоритма быстрого преобразования Фурье. Целью работы является модификация готового канала передачи данных в полнофункциональную систему спектрального анализа, способную в реальном времени выполнять обработку сигналов, поступающих с АЦП. В рамках исследования решаются следующие задачи: настройка и внедрение IP-ядра БПФ в средстве разработки Vivado, реализация весовой функции для минимизации спектральных искажений, организация полного цикла обработки от синтеза тестового сигнала через цифро-аналоговый преобразователь до захвата и спектрального анализа через АЦП, а

также экспериментальная верификация работоспособности всей системы на примере модельных и реальных сигналов.

Описание алгоритма работы модулей, реализующих алгоритм БПФ

Алгоритм обработки реализован с помощью трёх последовательных этапов, интегрированных в единый конвейер обработки данных:

1. Взвешивание сигнала (применение оконной функции);
2. Расчёт спектра (использование IP-ядра быстрого преобразования Фурье);
3. Вычисление амплитудного спектра (функция модуля).

На первом этапе отсчеты входного сигнала, предварительно разделенные на действительную и мнимую составляющие, поступают на модуль оконной обработки, где происходит их перемножение с оконной функцией Ханна, заранее рассчитанной в среде Matlab и сохраненной в BRAM памяти на ПЛИС. Результат перемножения также будет сохранен в отдельной памяти для накопления кадра и последующей передачи данных единым потоком на следующий этап.

Следующим этапом является подключение и конфигурирование готового IP-ядра БПФ. В его настройках указываются ключевые параметры, такие как размер преобразования (количество точек) и представление данных (фиксированная или плавающая точка). Сконфигурированное ядро интегрируется в проект и передаёт рассчитанный спектр в виде непрерывного потока данных следующему модулю.

Финальным этапом обработки является переход от комплексного представления спектра к вещественному. Модуль БПФ выдаёт комплексные отсчёты, в то время как для анализа, передачи или отображения необходим амплитудный спектр. Для этого вычисляется модуль каждого комплексного числа. Результатом этого этапа является массив действительных чисел, представляющий собой амплитудный спектр входного сигнала, готовый для дальнейшего использования. Структурная схема, поясняющая алгоритм работы, представлена на рисунке 1.

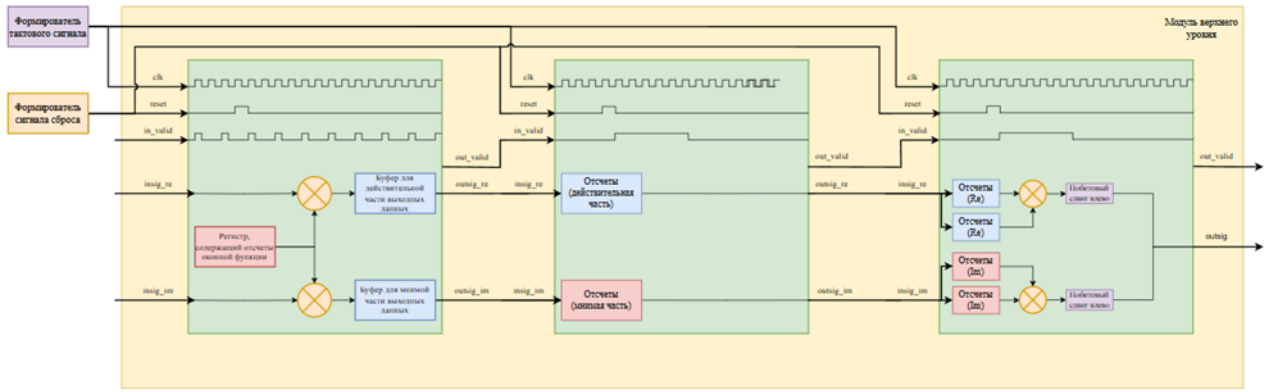


Рис. 1. Структурная схема алгоритма БПФ

Моделирование работы проекта с помощью гармонического сигнала, сформированного генератором

Для проверки корректности работы всей системы, включая реализованные на ПЛИС модули предобработки, БПФ и вычисления амплитудного спектра, было проведено моделирование с использованием эталонных гармонических сигналов. Тестовые сигналы формировались внешним генератором и подавались на аналоговый вход модуля FMC133V.

Особенность тестирования обусловлена целевым применением системы в качестве канала обработки сигналов радиолокационного измерителя дальности. В такой системе результат БПФ интерпретируется не как классический спектр частот, а как профиль дальности. Каждый выходной отсчёт БПФ соответствует своему каналу дальности, а амплитуда в этом канале – мощности сигнала, пришедшего с соответствующей дистанции.

В качестве первого и базового эксперимента на вход системы был подан чистый гармонический сигнал с известной частотой. В результате цель должна быть зафиксирована в каждом из каналов, а сдвиг спектра внутри канал покажет доплеровскую частоту, которая вызвана скоростью движения объекта. Результат обработки при нулевой доплеровской частоте представлен на рисунке 2.

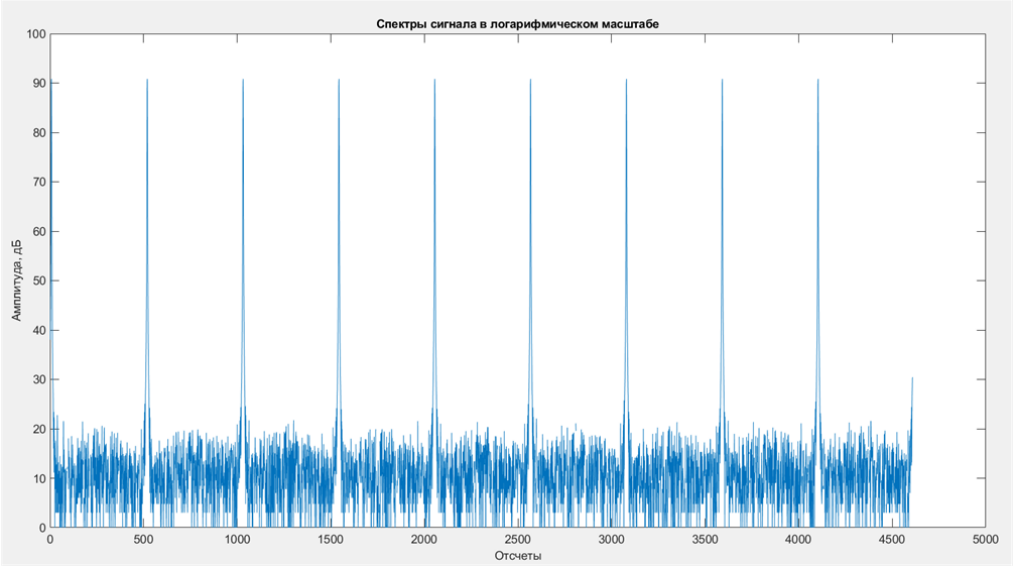


Рис. 2. Результат обработки гармонического сигнала с нулевой доплеровской частотой

Моделирование работы проекта при формировании цифровых сигналов в ЦАП

Следующим этапом работы стала интеграция в измерительный комплекс встроенного цифро-аналогового преобразователя (ЦАП) [2], который был использован в качестве программируемого источника тестовых сигналов. Переход на такой подход был обусловлен его существенными преимуществами в контексте разработки радиолокационной системы.

Основная целесообразность заключается в переходе от аналогового к цифровому синтезу сигналов. Вместо формирования сигнала во внешней аналоговой форме с последующей его передачей в тракт, он рассчитывается и синтезируется непосредственно в цифровом виде. Это позволяет единоразово рассчитать эталонный сигнал с требуемыми параметрами, после чего записать его отсчёты в буферную память ЦАП для последующего циклического воспроизведения.

Главными следствиями такого подхода являются гарантированная идентичность и высокая повторяемость формируемых сигналов, что критически важно для калибровки и точных измерений, а также значительное упрощение реализации испытательного стенда. Система становится более автономной, компактной и исключает неопределённости, вносимые внешним аналоговым оборудованием.

В качестве тестового сигнала для ЦАП был использован радиоимпульс, параметры которого соответствуют описанным в [1]. Сформированный цифровой сигнал был выведен на осциллограф. Полученный результат представлен на рисунке 3.

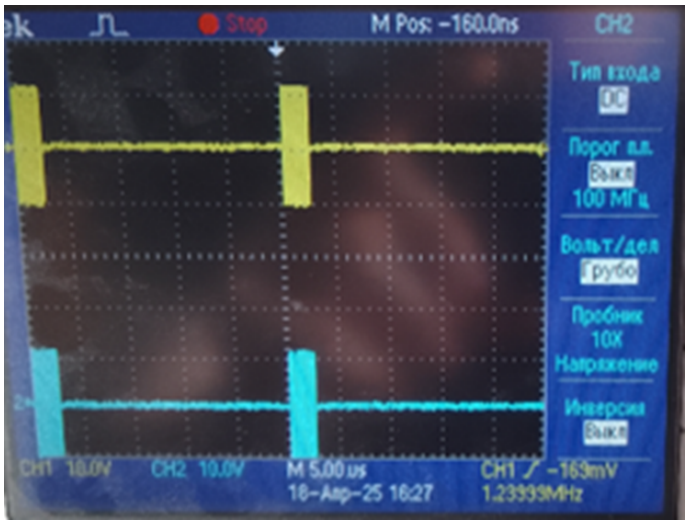


Рис. 3. Формирование радиоимпульса с помощью ЦАП

Сформированный импульс был передан по тракту «ЦАП → АЦП» и обработан описанным алгоритмом. Ожидаемым результатом является фиксация цели в канале дальности с возможным некоторым смещением внутри канала. Результат наблюдения представлен на рисунке 4.

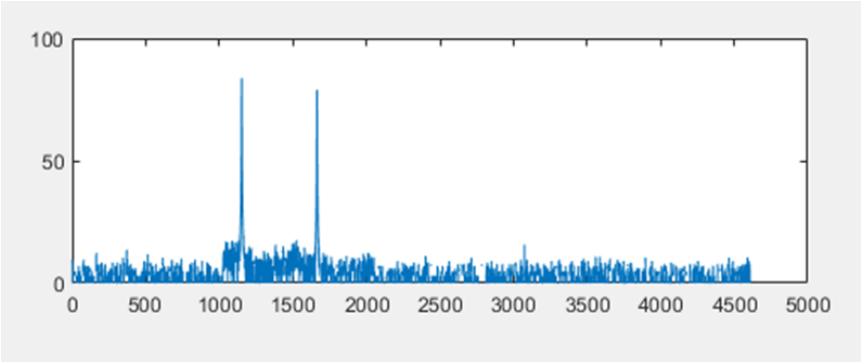


Рис. 4. Результат обработки сигнала, сформированного в АЦП

Заключение

Таким образом, в ходе разработки и исследований была создана работоспособная и универсальная система на ПЛИС. Её ключевым преимуществом является замкнутый цикл «генерация–обработка»: система способна как формировать сложные тестовые сигналы через ЦАП, так и выполнять их высокоскоростной приём и спектральный анализ через АЦП. Результаты всех экспериментов подтверждают корректность разработанных аппаратных и программных решений.

Библиографический список

1. Instrumental Systems Модуль FMC133V скую.467144.105рэ, 99 с.
2. Analog Devices AD9144 / Analog Devices [Электронный ресурс]. – 2015. – Режим доступа: https://www.farnell.com/datasheets/2333905.pdf. – Дата доступа: 11.02.2026.

УДК 004.94; ГРНТИ 28.17.19

МОДЕЛИРОВАНИЕ МНОГОСКОРОСТНЫХ СТРУКТУР УЗКОПОЛОСНЫХ КИХ-ФИЛЬТРОВ В СРЕДЕ SIMINTECH

А.А. Алексашин, В.А. Волченков

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, AleksashinAA2002@yandex.com

*Аннотация***.** В статье рассматривается задача проектирования узкополосных цифровых фильтров с конечной импульсной характеристикой (КИХ), характеризующихся высокой вычислительной сложностью при прямой реализации. В качестве эффективного подхода к снижению вычислительных затрат применяются методы многоскоростной обработки. Целью работы является исследование и сравнительный анализ двух методов синтеза многоступенчатых структур узкополосных КИХ-фильтров в отечественной среде моделирования SimInTech: на основе децимации и интерполяции преобразуемого сигнала и на основе децимации и интерполяции импульсной характеристики (с использованием гребенчатых фильтров). Представлены имитационные модели трёхступенчатых структур для обоих методов. Проведен анализ амплитудно-частотных и спектральных характеристик, временных диаграмм на различных этапах обработки. Показано, что применение многоскоростной обработки позволяет реализовать систему с требуемой избирательностью, при этом первый метод обеспечивает минимальные вычислительные затраты, а второй – упрощает процедуру проектирования. Полученные результаты подтверждают эффективность и корректность реализации данных алгоритмов в среде SimInTech.

Ключевые слова: SimInTech, КИХ-фильтр, многоскоростная обработка, узкополосный фильтр, децимация, интерполяция, гребенчатый фильтр.

MODELING OF MULTI-SPEED STRUCTURES OF NARROW-BAND FIR FILTERS IN THE SIMINTECH

A.A. Aleksashin, V.A. Volchenkov

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, AleksashinAA2002@yandex.com

The summary. The article discusses the problem of designing narrow-band digital filters with finite impulse response (FIR), characterized by high computational complexity in direct implementation. Multi-speed processing methods are used as an effective approach to reducing computational costs. The aim of the work is to study and compare two methods for synthesizing multi-stage structures of narrow-band FIR filters in the domestic SimInTech modeling environment: based on decimation and interpolation of the converted signal and based on decimation and interpolation of the impulse response (using comb filters). Simulation models of three-stage structures for both methods are presented. The analysis of amplitude-frequency and spectral characteristics, time diagrams at various stages of processing is carried out. It is shown that the use of multi–speed processing makes it possible to implement a system with the required selectivity, while the first method provides minimal computational costs, and the second simplifies the design procedure. The results obtained confirm the effectiveness and correctness of the implementation of these algorithms in the SimInTech environment.

Keywords: SimInTech, FIR filter, multi-speed processing, narrowband filter, decimation, interpolation, comb filter.

Прямая реализация узкополосных КИХ-фильтров требует высокого порядка N, что ведет к росту вычислительных затрат и объема памяти. Эффективным решением является многоскоростная обработка, основанная на децимации и интерполяции сигнала [1, 2].

В условиях импортозамещения актуально использование отечественной среды SimInTech [3]. Цель работы – исследование и сравнение в среде SimInTech двух методов синтеза трехступенчатых структур КИХ-фильтров: на основе децимации/интерполяции сигнала и на основе децимации/интерполяции импульсной характеристики.

Многоскоростная КИХ-фильтрация

Порядок N КИХ-фильтра, аппроксимирующего идеальную частотную характеристику, можно оценить с помощью эмпирического выражения (1):

$$N = \alpha\beta L(\varepsilon_1\varepsilon_2), \tag{1}$$

где α – показатель прямоугольности АЧХ;

β – показатель узкополосности АЧХ;

$L(\varepsilon_1, \varepsilon_2)$ –логарифмический показатель частотной избирательности, зависящий от допустимой неравномерности в полосе пропускания ε_1 и уровня подавления в полосе задерживания ε_2.

Для узкополосных фильтров $\beta >> 1$, что и определяет высокий порядок фильтра N. Многоскоростная обработка позволяет уменьшить зависимость вычислительных затрат от β.

Метод на основе децимации и интерполяции преобразуемого сигнала

Структура, построенная по этому методу, содержит два фильтра-дециматора (ЦФД-1, ЦФД-2), работающих на пониженной частоте дискретизации f_∂ в ν_1 и ν_2 раз соответственно, формирующий фильтр на самой низкой f_∂.

Общие вычислительные затраты R (операций умножения в секунду) и требуемый объем памяти данных S для такой структуры описываются выражениями (2, 3):

$$R = f_\partial\left(\frac{2N_1}{\nu_1} + \frac{2N_2}{\nu_1\nu_2} + \frac{N_0}{\nu_1\nu_2}\right), \tag{2}$$

$$S = \frac{\nu_1 + 1}{\nu_1}N_1 + \frac{\nu_2 + 1}{\nu_2}N_2 + N_3, \tag{3}$$

где ν_1, ν_2 – коэффициенты децимации на первой и второй ступенях;

N_1, N_2, N_3 – порядки соответствующих фильтров, рассчитываемые через исходные параметры α, β, ε_1, ε_2 и выбранные ν.

Метод на основе децимации и интерполяции импульсной характеристики

Этот метод, также называемый методом многокаскадной гребенчатой фильтрации, основан на «прореживании» по частоте. Входной каскад представляет собой гребенчатый фильтр (ЦГФ), импульсная характеристика которого получается путем вставки ($\nu - 1$) нулей между отсчетами импульсной характеристики базового НЧ-фильтра. Это эквивалентно сжатию его АЧХ по частоте, в результате чего она становится периодической с периодом $\frac{2\pi}{\nu}$.

Для выделения основного лепестка из этой периодической последовательности используются последующие каскады гребенчатых фильтров и оконечный сглаживающий фильтр (ЦСФ).

Для трёхкаскадной структуры вычислительные затраты и объём памяти данных оцениваются следующими выражениями (4, 5):

$$R = f_\partial\left(\frac{N_1}{\nu_1} + \frac{N_2}{\nu_2} + N_3\right), \tag{4}$$

$$S = N_{ЦГФ1} + N_{ЦГФ2} + N_{ЦСФ}, \quad (5)$$

где $N_{ЦГФ1}$, $N_{ЦГФ2}$, $N_{ЦСФ}$ – порядки ЦГФ-1, ЦГФ-2 и ЦСФ соответственно.

Ключевое отличие от первого метода заключается в способе получения фильтров децимации: здесь они не проектируются заново, а получаются из одного базового фильтра, что проще с точки зрения проектирования, но может давать иную эффективность.

Моделирование в среде SimInTech (SIT)

В среде SIT была реализована модель трёхступенчатой структуры узкополосных КИХ-фильтров на основе децимации сигнала (рис. 1).

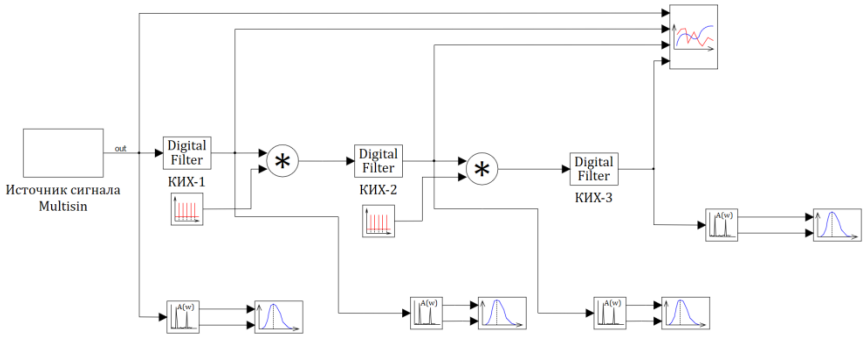


Рис. 1. Модель 3-х ступенчатой структуры узкополосных КИХ-фильтров

Для каждого каскада использовались цифровые КИХ-фильтры, а также умножитель на периодическую последовательность единичный импульсов (реализация процесса децимации).

Параметры фильтров: $f_{проп1}$ = 100 Гц, $f_{подавл1}$ = 650 Гц; $f_{проп2}$ = 100 Гц, $f_{подавл2}$ = 275 Гц; $f_{проп3}$ = 100 Гц, $f_{подавл3}$ = 135 Гц. Частоты дискретизации фильтров $f_д$: 4000 Гц, 2000 Гц, 1000 Гц соответственно. Допустимая неравномерность в полосе пропускания для каждого фильтра: $\varepsilon_1 = 10^{-2}/3$, уровень подавления $\varepsilon_2 = 10^{-3}$. В качестве тестового сигнала использовалась сумма пяти синусоид с частотами: 6, 250, 275, 375 и 700 Гц.

На рисунке 2 представлены временные диаграммы сигналов первой модели. Спектры сигналов на выходе каскадов модели и АЧХ каждого каскада представлены на рисунке 3.

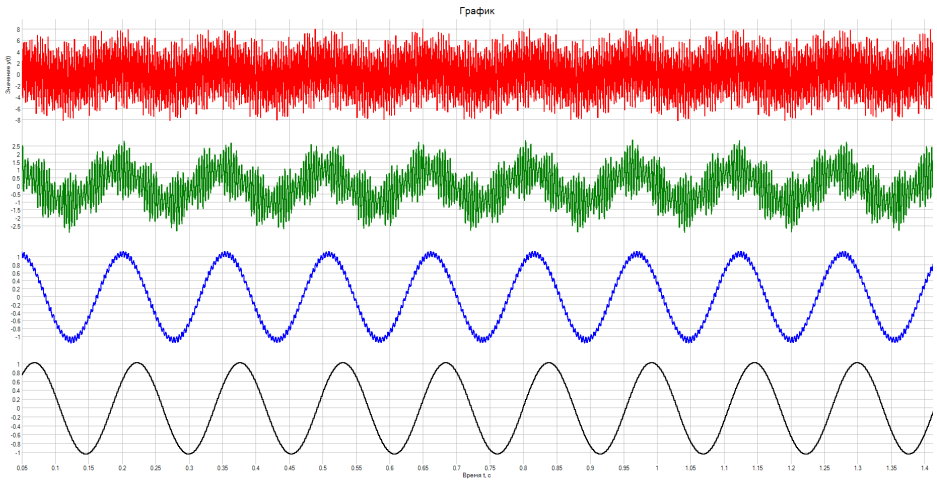


Рис. 2. Временные диаграммы исходного сигнала (красный), сигнала на выходе 1-го каскада (зеленый), на выходе 2-го каскада (синий), 3-го каскада (черный)

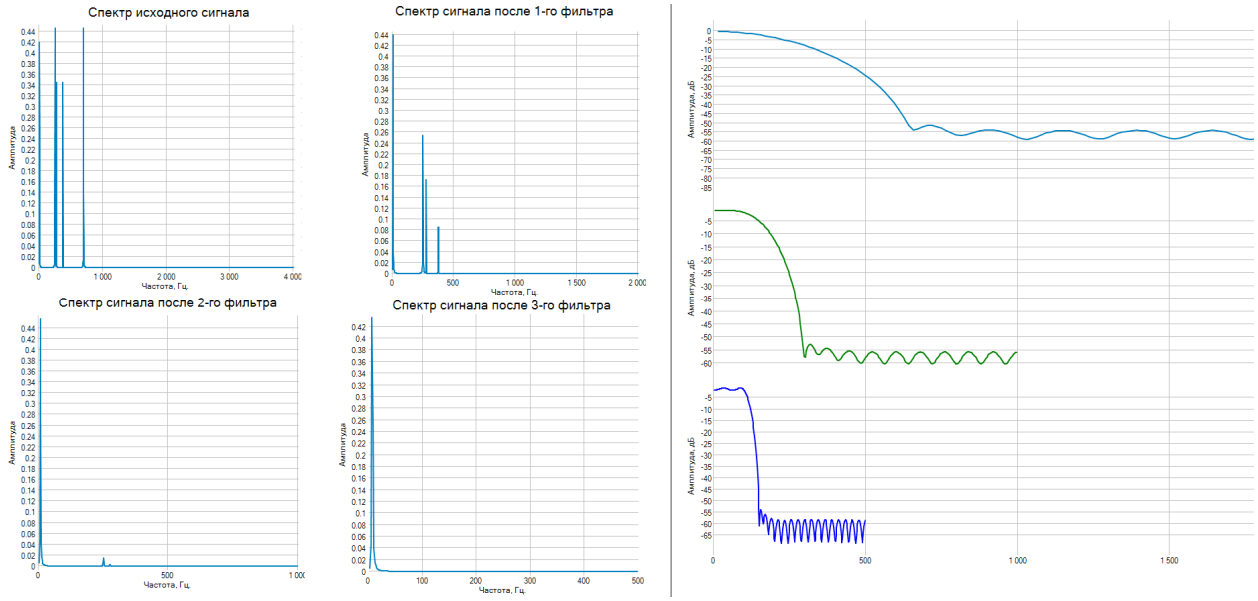


Рис. 3. Спектры исходного сигнала и сигналов на выходе каждого каскада (слева), АЧХ фильтров каждого каскада (справа)

Исходный сигнал содержит все пять гармоник. После первого каскада фильтрации и децимации высокочастотная составляющая (700 Гц) подавлена. На выходе второго каскада спектр дополнительно очищается от составляющей 375 Гц. Формирующий фильтр на пониженной частоте обеспечивает окончательное подавление помех (250 и 275 Гц, попавшие в переходную зону предыдущего каскада) и формирует требуемую полосу пропускания. Последующее восстановление частоты дискретизации (ЦФИ) не вносит искажений в спектр полезного сигнала.

Метод на основе гребенчатой фильтрации

Структурная схема модели SimInTech, реализующая метод децимации ИХ, представлена на рисунке 4.

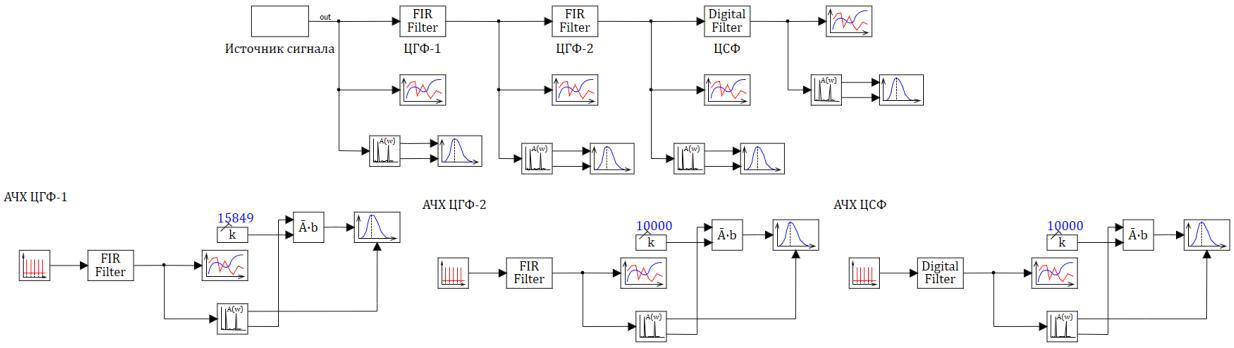


Рис. 4. Модель 3-х ступенчатой гребенчатой структуры КИХ-фильтров

Частоты базового фильтра: $f_{проп}$ = 100 Гц, $f_{подавл}$ = 150 Гц, $f_д$ = 4000 Гц. Частоты сглаживающего фильтра: $f_{проп_ЦСФ}$ = 100 Гц, $f_{подавл_ЦСФ}$ = 625 Гц, $f_д$ = 4000 Гц. Допустимая неравномерность в полосе пропускания для каждого фильтра: $\varepsilon_1 = 10^{-2}/3$, уровень подавления $\varepsilon_2 = 10^{-3}$. В качестве тестового сигнала использовалась сумма пяти синусоид с частотами: 10,

500, 1000, 1500 и 1990 Гц (подбирались таким образом, чтобы частоты сигнала попадали в разные полосы пропускания ЦГФ-1).

На рисунке 5 показаны АЧХ гребенчатых фильтров и ЦСФ. Видно, что АЧХ ЦГФ-1 (а) имеет периодический характер с периодом, определяемым коэффициентом $\nu_2 = 8$. ЦГФ-2 (б) с коэффициентом $\nu_2 = 4$ подавляет часть боковых лепестков. Оконечный ЦСФ (в) выделяет главный лепесток в районе нулевой частоты, формируя итоговую характеристику.

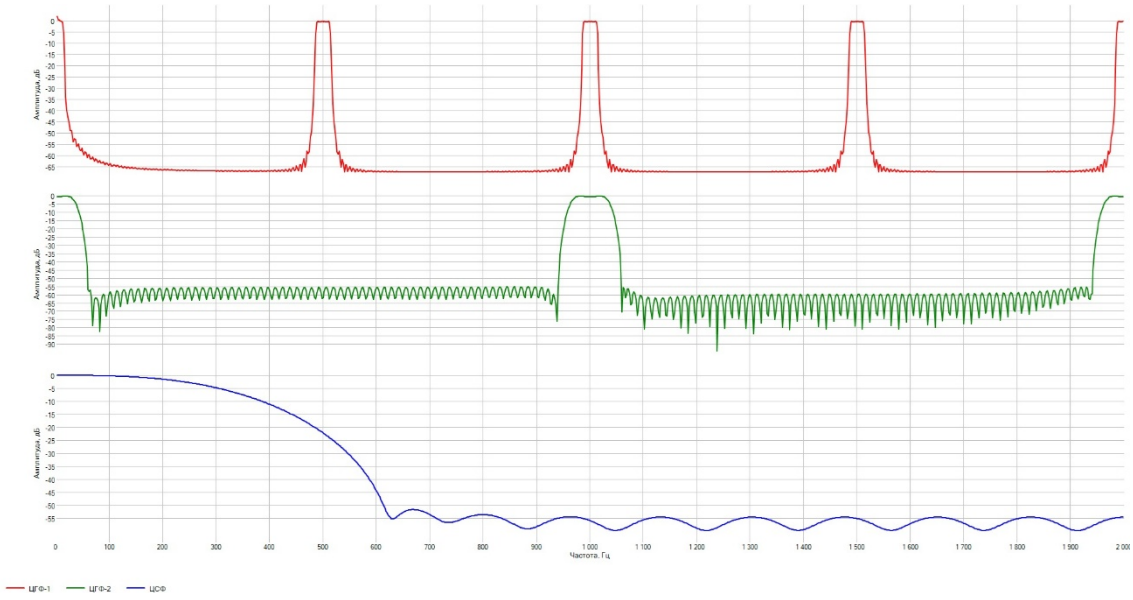


Рис. 5. АЧХ ЦГФ-1 (а), ЦГФ-2 (б) и ЦСФ (в)

На рисунке 6 представлены спектры сигналов для этой модели. Видно, что спектр после ЦГФ-1 практически не отличается от спектра исходного сигнала, поскольку все выбранные частоты попали в полосы пропускания его периодической АЧХ. Последующие каскады – ЦГФ-2 и ЦСФ – выделяют требуемую низкочастотную полосу, в результате чего на выходе ЦСФ наблюдается только сигнал частотой 10 Гц.

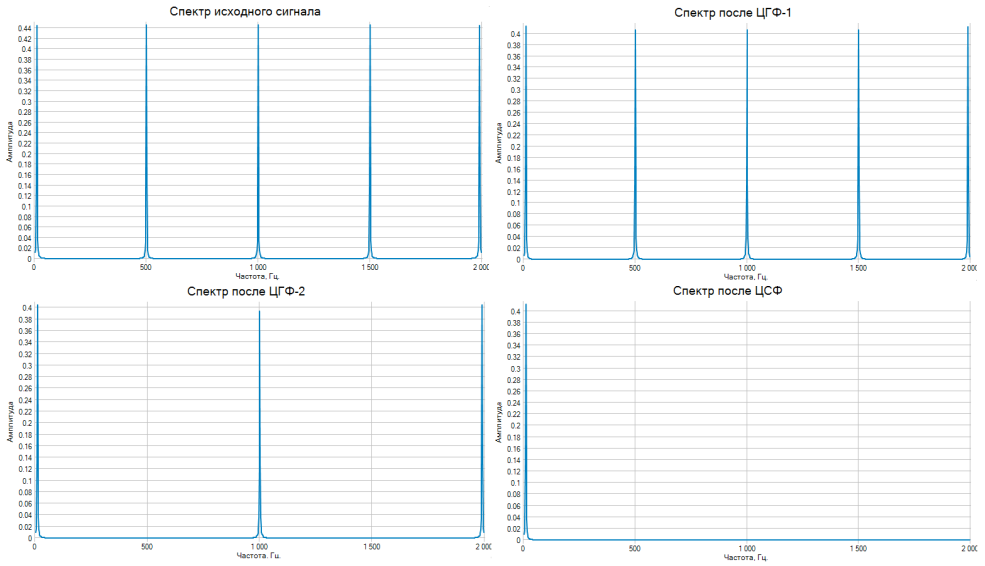


Рис. 6. Спектры исходного сигнала и сигналов на выходах ЦГФ-1, ЦГФ-2 и ЦСФ

В отличие от метода децимации сигнала, где каждый фильтр требует индивидуального расчета, здесь базовый фильтр повторяется в полифазной структуре υ раз, а его порядок составляет *N/υ*, что пропорционально снижает вычислительные затраты на его реализацию. Платой за это упрощение является увеличение требуемого объема памяти в (*υ* – 1) раз из-за наличия нулевых отсчетов в импульсных характеристиках гребенчатых фильтров.

Заключение

Результаты моделирования в среде SimInTech подтвердили корректность реализации обеих трехступенчатых структур узкополосных КИХ-фильтров. Анализ амплитудно-частотных и спектральных характеристик, а также временных диаграмм показал, что оба метода обеспечивают эффективное подавление нежелательных частот и выделение полезного сигнала в соответствии с заданными требованиями частотной избирательности. Среда SimInTech предоставляет удобные и наглядные средства визуализации, позволяющие в полном объеме анализировать временные и частотные характеристики разрабатываемых устройств непосредственно в процессе моделирования.

Таким образом, отечественная среда моделирования SimInTech обеспечивает широкие возможности для разработки и исследования алгоритмов цифровой обработки сигналов и может эффективно использоваться в учебных и научных задачах, связанных с синтезом сложных фильтровых структур.

Библиографический список

1. Витязев В.В. Цифровая частотная селекция сигналов. – М.: Радио и связь, 1993. – 240 с.;
2. Цифровые цепи и сигналы: учеб. Пособие / В.В. Витязев; РГРТУ. Рязань, 2012, 136с;
3. SimInTech: [сайт]. – URL: https://simintech.ru/ (дата обращения: 16.02.2026).

УДК 621.396; ГРНТИ 47.47

СРАВНЕНИЕ ИСПОЛЬЗОВАНИЯ АЛГОРИТМОВ OSD И ORBGRAND ДЛЯ ДЕКОДИРОВАНИЯ КОДОВ BCH

Н.С. Виноградов
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, nikita-vinogradov11@rambler.ru

Аннотация. В работе рассматривается использование алгоритмов OSD и ORBGRAND для декодирования БЧХ кодов. Рассматриваются особенности алгоритмов OSD и ORBGRAND.
Ключевые слова: коды Боуза-Чоудхури-Хоквингема (БЧХ), декодер OSD (Ordered Statistics Decoding), декодер ORBGRAND (Ordered Reliability Bits Guessing Random Additive Noise Decoding).

COMPARISON OF THE USE OF OSD AND ORBGRAND ALGORITHMS FOR DECODING BCH CODES

N.S. Vinogradov
Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, nikita-vinogradov11@rambler.ru

The summary. The paper considers the use of OSD and ORBGRAND algorithms for decoding BCH codes. The features of the OSD and ORBGRAND algorithms are considered.
Keywords: Bose-Chowdhury-Hockingham codes (BCH), ordered statistics decoding (OSD), ordered reliability bits guessing random additive noise decoding (ORBGRAND).

Коды БЧХ широко используются в современных приложениях, например, в системах хранения данных [1] и в спутниковых системах телевещания [2]. Одним из основных алгоритмов декодирования кодов БЧХ является алгоритм Берлекэмпа-Мэсси [3], [4]. Данный алгоритм предполагает использование жестких решений на входе декодера.

Для повышения эффективности использования кодов БЧХ переходят к мягким алгоритмам декодирования, которые принимают на вход мягкие решения, поступающие с выхода демаппера. Одними из таких известных алгоритмов являются алгоритм декодирования по порядковым статистикам OSD [5] и алгоритм ORBGRAND [6]. Данные алгоритмы способны декодировать любые блоковые коды. В данной работе рассматривается их применение для декодирования кодов БЧХ.

В алгоритме OSD выделяются две стадии: формирования новой систематической генераторной матрицы и перебор шаблонов ошибок заданного порядка. Структурная схема декодера OSD приведена на рисунке 1. На первом этапе в соответствии с наиболее достоверными мягкими решениями формируется новая генераторная матрица с использованием алгоритма Гауссового исключения (Gaussing Elimination) [5]. В заключении производится преобразование матрицы к систематическому виду. На выходе первого этапа фактически получается новое информационное сообщение, состоящее из наиболее достоверных мягких решений, а также новая генераторная матрица в систематическом виде.

Последующая стадия обработки заключается в последовательном переборе шаблонов ошибок для нового информационного сообщения с последующим получением нового кодового слова. Количество проверяемых шаблонов ошибок зависит от порядка **L**. Значение порядка **L** определяет максимальное количество единиц в шаблонах ошибок. Таким образом, при **L**, равном длине информационного сообщения, достигается декодирование по максимуму правдоподобия. Формирование выходного кодового слова состоит в выборе ближайшего полученного кодового слова к принятому. Для оценки расстояния используется метрика Евклида.

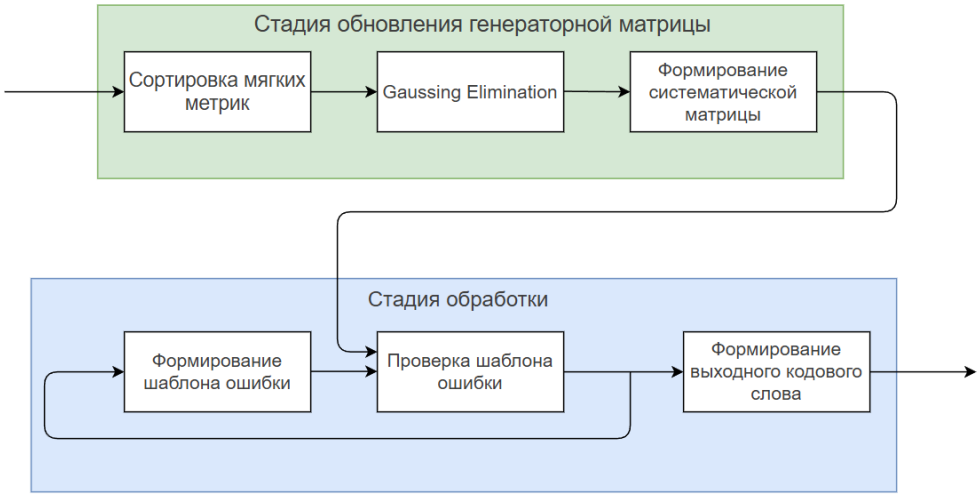


Рис. 1. Структурная схема декодера OSD

При увеличении порядка OSD декодера значительно увеличивается количество проверяемых шаблонов ошибок, а соответственно и увеличивается время работы декодера. Так, например, для кода BCH (128, 64, 22) для OSD(1) количество проверяемых шаблонов ошибок равно 64, для OSD(2) – 2080, а для OSD(3) – 43744.

Декодер ORBGRAND [6] основан на алгоритме GRAND, однако позволяет учитывать мягкость решений на входе декодера. Суть алгоритма состоит в том, чтобы формировать шаблоны ошибок с наименьшим весом Евклида и проверять является ли исправленное сообщение кодовым словом. Если после очередной проверки синдром сходится (становится рав-

ным нулю), то декодирование заканчивается и исправленное сообщение подается на выход декодера. Декодер ORNGRAND в соответствии с [6] имеет два параметра: количество проверяемых шаблонов ошибок **N** и порядок кусочно-линейной аппроксимации **M**.

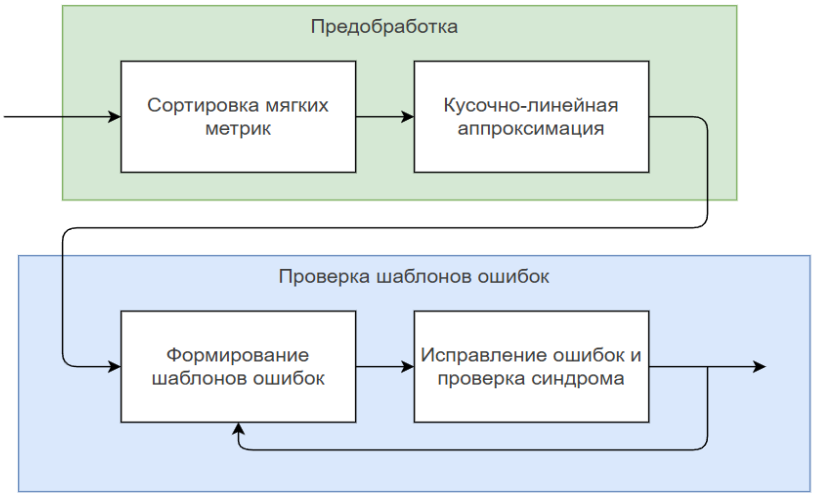


Рис. 2. Структурная схема декодера ORBGRAND

На рисунке 2 приведена структурная схема ORBGRAND декодера. По аналогии с OSD, здесь также можно выделить два этапа обработки. На первом этапе предобработки происходит построение кусочно-линейной аппроксимации для кривой, которая строится из отсортированных входных мягких решений. На втором этапе на основании полученной аппроксимации происходит генерация шаблонов ошибок и проверка синдрома.

В [6] в основном алгоритм используется для декодирования полярных кодов для 5G, однако также демонстрируется использование его для BCH кода (255,231).

Для сравнения декодеров OSD и ORBGRAND были выбраны два кода: (128,99,10) и (128,64,22). Моделирование проводилось на AWGN канале с использованием BPSK модуляции. На рисунках 3-4 представлены результаты моделирования для выбранных кодов. Для сравнения на графиках также приведены BER для BPSK без кодирования и BER для алгебраического декодера Берлекэмпа-Мэсси.

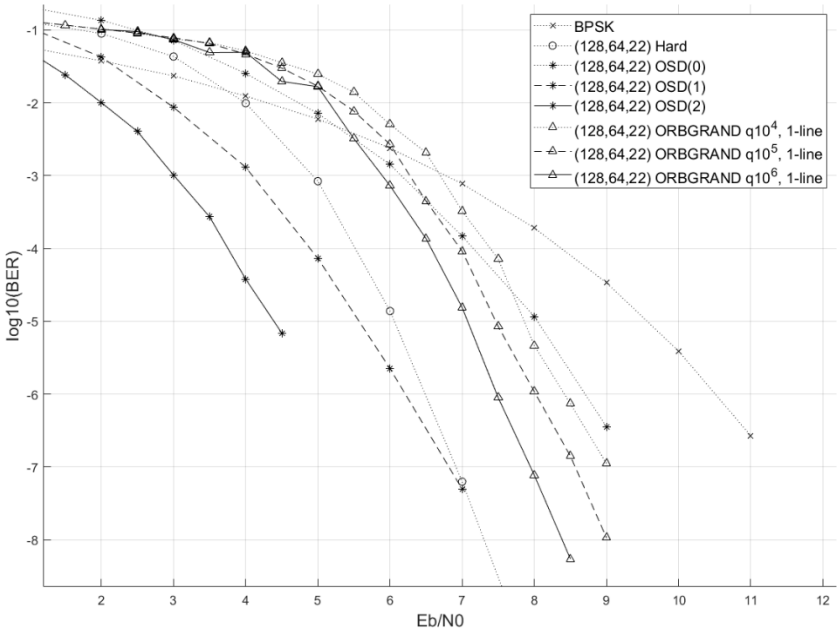


Рис. 3. Результаты моделирования BCH (128,64,22)

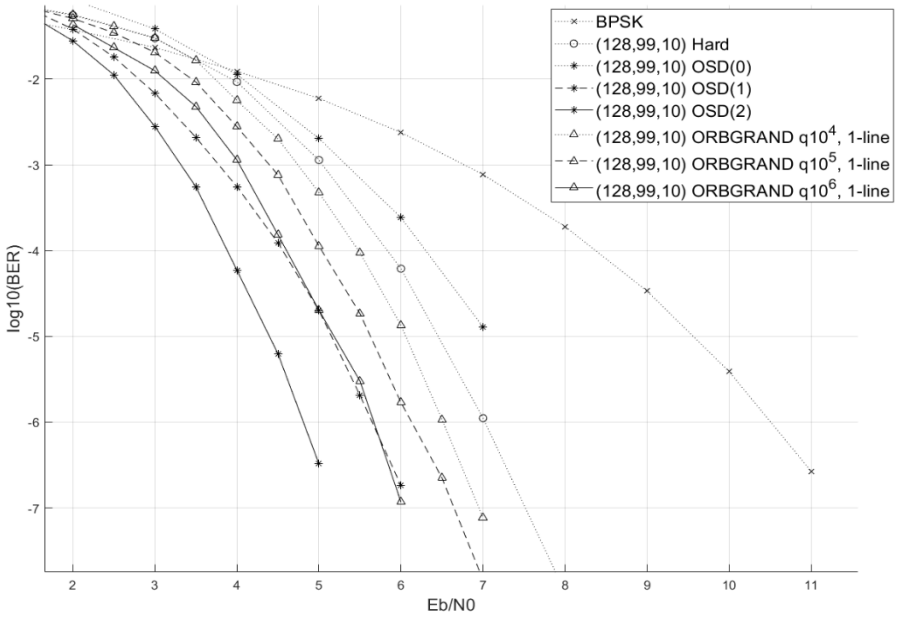


Рис. 4. Результаты моделирования BCH (128,99,10)

Для алгоритма OSD при моделировании порядок декодирования **L** менялся от 1 до 3. Для алгоритма ORBGRAND число проверяемых шаблонов ошибок **N** менялось от 10^4 до 10^6, а порядок кусочно-линейной аппроксимации **M** для всех результатов моделирования был приравнен к 1.

Для кода BCH (128,64,22) декодер ORBGRAND для количества шаблонов ошибок 10^6 показывает результаты хуже, чем OSD(1), для которого число проверяемых шаблонов ошибок равно 64. Также результаты моделирования для ORBGRAND хуже, чем результаты для алгебраического декодера на 1 дБ для BER 10^-7. При этом, увеличение количества проверяемых шаблонов ошибок для ORBGRAND на два порядка (с 10^4 до 10^6) позволяет получить выигрыш в 1 дБ при BER 10^-7. Потенциально, дальнейшее увеличение количества проверяемых шаблонов ошибок **N**, а также увеличение порядка кусочно-линейной аппроксимации **M** может позволить получить результаты лучше OSD(1), а возможно и приблизиться к ML, однако это требует значительной оптимизации текущей модели для ускорения вычислений.

Для кода BCH (128,99,10) ситуация лучше, так как ORBGRAND при количестве шаблонов ошибок до 10^6 превосходит алгебраический декодер и совпадает с OSD(1). Увеличение проверяемых шаблонов ошибок на два порядка (с 10^4 до 10^6) для ORBGRAND для BER 10^-7 также дает выигрыш в 1 дБ.

В соответствии с результатами моделирования, можно сделать вывод, что алгоритм ORBGRAND лучше себя проявляет для высокоскоростных кодов. Однако для обоих кодов (128,99,10) и (128,64,22) количество проверяемых шаблонов ошибок для OSD значительно меньше, чем для ORBGRAND. В результате, при использовании алгоритма OSD удается добиться большей пропускной способности, а также лучших характеристик BER при меньшем количестве проверяемых шаблонов ошибок. С другой стороны, для алгоритма OSD необходимо формирование новой генераторной матрицы, что является вычислительно сложной задачей, а также слабо распараллеливаемой.

В современных системах связи ставится ряд важных задач для алгоритмов декодирования помехоустойчивых кодов. Так, для систем 6G URLLC важно достижение требуемой характеристики BER при обеспечении минимальных задержек. Оба рассмотренных алгоритма декодирования могут быть удобно распараллелены на стадиях проверки шаблонов ошибок. Таким образом, становится актуальной задача исследования эффективности реализации алгоритмов OSD и ORBGRAND на ПЛИС.

По итогам проведенного исследования можно сделать вывод, что для алгоритма OSD узким местом является стадия формирования новой генераторной матрицы с использованием Гауссового исключения, а для алгоритма ORBGRAND узкое место – требуемое количество проверяемых шаблонов ошибок.

В дальнейшем также планируется исследование возможности использования других способов аппроксимации кривой для декодера ORBGRAND с целью уменьшения требуемого количества проверяемых шаблонов ошибок.

Библиографический список

1. Freudenberger, Juergen & Spinner, Jens. (2013). A CONFIGURABLE BOSE–CHAUDHURI–HOCQUENGHEM CODEC ARCHITECTURE FOR FLASH CONTROLLER APPLICATIONS. Journal of Circuits, Systems, and Computers. 23. 10.1142/S0218126614500194.

2. ETSI EN 302 307-1: "Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2"

3. E. R. Berlekamp, Algebraic Coding Theory., 1968.

4. J. Massey, Shift-register synthesis and BCH decoding, 1969, doi:10.1109/tit.1969.1054260

5. M. P. C. Fossorier and Shu Lin, "Soft decision decoding of linear block codes based on ordered statistics," Proceedings of 1994 IEEE International Symposium on Information Theory, 10.1109/ISIT.1994.394624.

6. K. R. Duffy, W. An and M. Médard, "Ordered Reliability Bits Guessing Random Additive Noise Decoding," in *IEEE Transactions on Signal Processing*, vol. 70, pp. 4528-4542, 2022, doi: 10.1109/TSP.2022.3203251.

УДК 621.3.01; ГРНТИ 45.01.45

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СРЕДЫ SIMINTECH ПО МОДЕЛИРОВАНИЮ ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ ПОСТОЯННОГО ТОКА

В.С. Литвинова, В.А. Волченков

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, varvara_lit@mail.ru

Аннотация. В работе рассматривается моделирование в среде SimInTech электрической цепи постоянного тока со смешанным соединением элементов. Проводится сравнение результатов теоретического расчета, измерений на реальном макете и в созданной имитационной модели цепи.

Ключевые слова: математическое моделирование, SimInTech, электрические цепи, постоянные ток и напряжение, смешанное соединение элементов, расчет электрической цепи, цифровое моделирование.

RESEARCH OF SIMINTECH ENVIRONMENT POSSIBILITIES FOR DIRECT CURRENT ELECTRIC CHAINS MODELLING

V.S. Litvinova, V.A. Volchenkov

Ryazan State Radio Engineering University named after V.F. Utkin, Russian Federation, Ryazan, varvara_lit@mail.ru

The summary. The paper considers the modeling in the SimInTech environment of direct current circuit with a mixed connection of elements. The results of theoretical calculation, measurements on a real layout and in the created simulation model of the circuit are compared.

Keywords: mathematical modeling, SimInTech, electrical circuits, constant current and voltage, mixed connection of elements, calculation of an electrical circuit, digital modeling.

Переход от выполнения лабораторных работ на физических макетах к математическому моделированию в специализированном программном обеспечении – это естественный шаг в развитии технического образования. Работа с реальными макетами, а, следовательно, и

их поддержание в работоспособном состоянии, требует значительных финансовых и материальных затрат. Виртуальное моделирование полностью решает эту проблему. Все элементы схемы представляются в цифровом виде, а студенты могут выполнять эксперименты на собственных компьютерах в любое время, что делает процесс обучения гораздо более доступным и гибким.

Расчетные математические модели в среде SimInTech создаются посредством функционально блочного программирования при помощи блоков [1], которые содержатся в различных библиотеках. SimInTech позволяет создавать модели с высокой степенью детализации, интегрировать различные этапы разработки и исследовать поведение цепи в динамике.

Модели в системе SimInTech создаются из стандартных блоков, помещенных в различных библиотеках. Для моделирования электрических цепей в настоящее время в SimInTech включены следующие библиотеки:

- электротехнического оборудования для анализа электрических цепей в действующих значениях «ЭЦ-Статика»;

- электротехнического оборудования для анализа электрических цепей в мгновенных значениях «ЭЦ-Динамика».

SimInTech обладает широкими возможностями по организации вычислений, связанных с решением алгебраических и обыкновенных дифференциальных уравнений, которые являются математическим аппаратом описания процессов, происходящих в электрических цепях.

В данной статье приводятся результаты моделирования в среде SimInTech лабораторной работы №1 «Исследование линейной электрической цепи со смешанным соединением элементов», которую выполняют студенты 2 курса в ходе изучения дисциплин «Основы теории цепей», «Теория электрических цепей» и «Электротехника» [2].

Для схемы, изображенной рисунке 1, методом свертывания [3] были рассчитаны токи в ветвях схемы и напряжения на участках цепи. Данные для расчета были взяты из таблицы 1 для бригады №5.

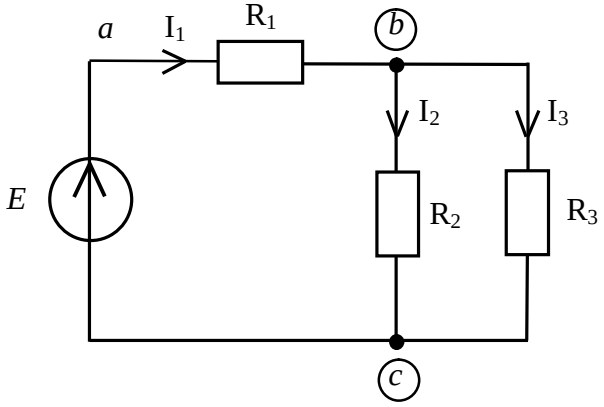


Рис. 1. Схема цепи, исследуемой в лабораторной работе №1

Таблица 1. Исходные значения параметров элементов схемы

Величина	Номер бригады							
	1	2	3	4	**5**	6	7	8
E, В	11	12	13	14	**11**	12	13	14
R_1, Ом	130	130	130	130	**130**	130	130	130
R_2, Ом	300	360	330	270	**390**	360	330	240
R_3, Ом	270	270	270	270	**330**	330	330	330

Работа в специализированной лаборатории выполнялась на универсальном стенде, на лицевой панели которого приведены изображения элементов и выведены гнезда и штыри, к которым они присоединены. Сама цепь почти полностью собрана. Небольшие дополнительные соединения в цепи, а также подключение измерительных приборов проводятся с помощью проводников. Недостающие перемычки втыкаются в специальные гнезда соответствующего диаметра. Измерительные приборы подключаются к штыревым контактам.

В данной лабораторной работе из всех измерительных приборов было достаточно использовать только мультиметр. Этот прибор совмещает в себе функции вольтметра и амперметра, то есть позволяет измерять напряжение на участке цепи и ток в ветви.

Моделирование в среде SimInTech

Для построения имитационной модели исследуемой цепи (рис. 2) из библиотеки «ЭЦ–Динамика» были выбраны следующие блоки:

- блок Источник напряжения из закладки Источники;
- три блока RLC-цепь из закладки Электротехнические элементы;
- блоки Вольтметр идеальный (2 штуки – для измерения напряжений U_{ab} и U_{bc}) и Амперметр идеальный из закладки Измерители (3 штуки – для измерения токов I_1, I_2 и I_3);
- пять блоков Порт выхода из библиотеки Субструктур.

Параметры расчета схемного окна проектов были заданы следующими:

- конечное время расчета в секундах равным 1;
- минимальный шаг и максимальный шаг интегрирования задать равным 0,01;
- метод интегрирования был установлен по умолчанию – метод Эйлера, который может использовать только фиксированный шаг, а все остальные методы могут использоваться как с фиксированным шагом, так и с автоматическим выбором шага.
- относительная ошибка 0.0001, абсолютная ошибка 1E-6;
- относительная ошибка сравнения времени для дискретных блоков и источников 1E-12.

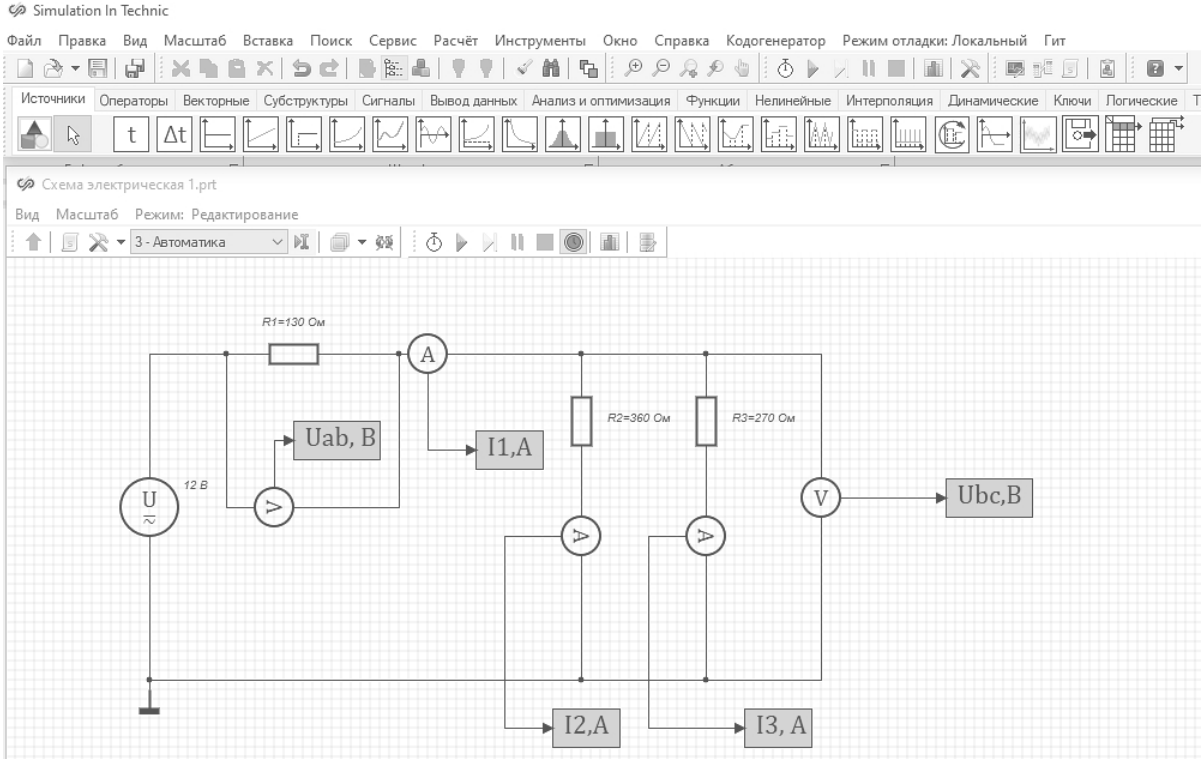


Рис. 2. Имитационная модель исследуемой цепи

На рисунке 3 приведены результаты моделирования.

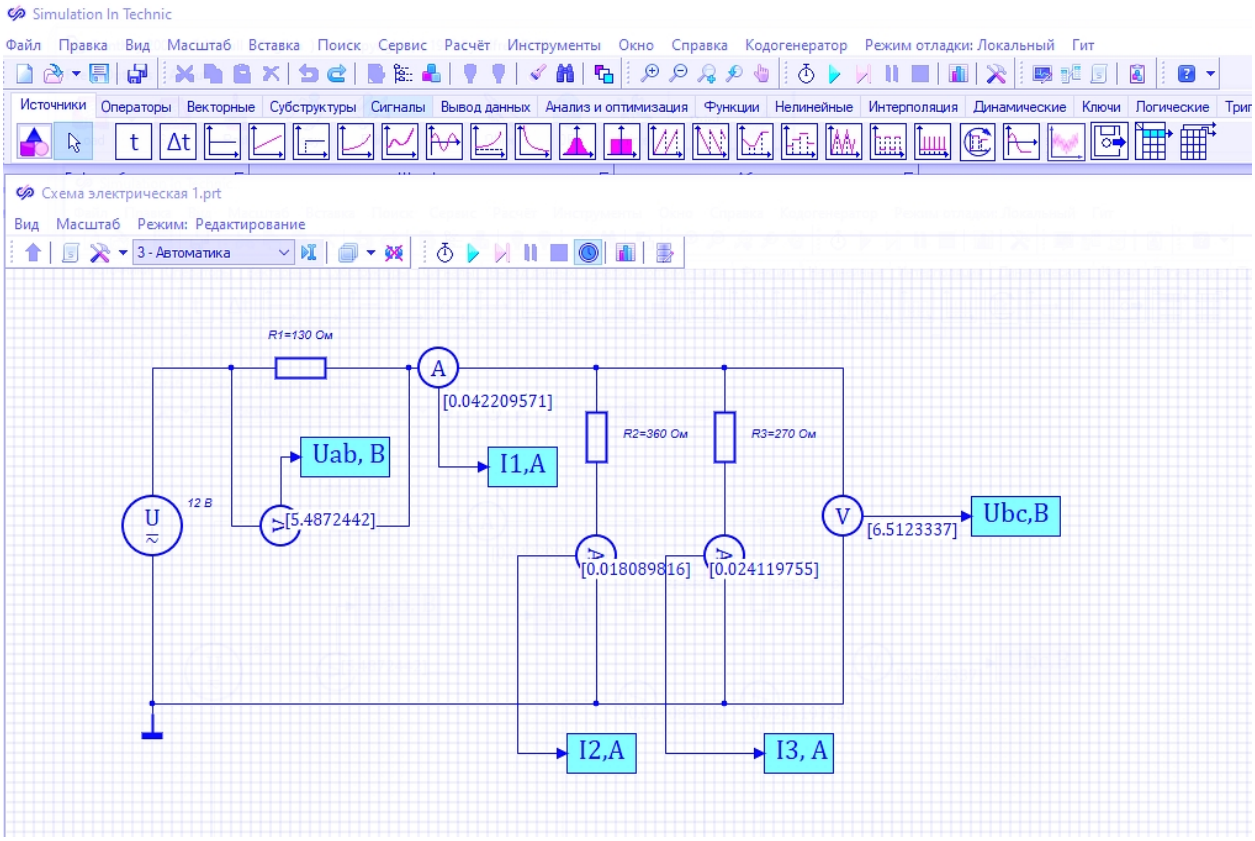


Рис. 3. Результаты моделирования

В таблице 2 представлены результаты расчета, измерений на макете и в созданной имтационной модели цепи в SimInTech.

Таблица 2.

Величина	U_{ab}, В	U_{bc}, В	U_{ac}, В	I_1, мА	I_2, мА	I_3, мА
Расчет	5,49	6,51	12	42,2	18,1	24,1
Натурный эксперимент	5,52	6,46	12	40,7	17,1	23,7
SimInTech	5,49	6,51	12	42,2	18,1	24,1

Значения токов и напряжений, полученных по расчетным формулам, и в среде математического моделирования SimInTech полностью совпали.

Таким образом, использование среды динамического моделирования технических систем SimInTech открывает широкие возможности для анализа и проектирования электрических цепей.

Библиографический список

1. Библиотеки блоков // Справочная система SimInTech (v12.11.2025)
URL: https://help.simintech.ru/#10_biblioteki_blokov/biblioteki_blokov.html (дата обращения: 17.02.2026).
2. Литвинова В.С., Милюков С.М. Теория электрических цепей. Основы теории цепей. Ч. 1: методические указания к лабораторным работам / Рязан. гос. радиотехн. ун-т.; – Рязань, 2020. – 24с.
3. Попов В. П. Основы теории цепей. – М.: Высшая школа, 2003. – 575 с.

УДК 621.376; ГРНТИ 47.47

РАЗРАБОТКА МОДЕЛИ ПРИЁМНИКА ЛЧМ-СИГНАЛОВ С АДАПТИВНОЙ КОМПЕНСАЦИЕЙ ПОМЕХ В СРЕДЕ MATLAB ДЛЯ ИЗУЧЕНИЯ АЛГОРИТМОВ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

М.В. Елисеев, А.Ю. Линович

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, kudimov.edu@yandex.ru AleksashinAA2002@yandex.com nikita-vinogradov11@rambler.ru varvara_lit@mail.ru maks-eliseev-97@mail.ru

Аннотация. В статье рассматривается разработка виртуальной модели приёмника сигналов с линейной частотной модуляцией (ЛЧМ), оснащённого системой адаптивной компенсации помех, в среде математического моделирования MATLAB. В работе представлены теоретические основы формирования ЛЧМ-сигналов, математическое описание алгоритма наименьших квадратов (LMS) и структура цифрового корреляционного приёмника. Описана программная реализация модели, включающая генерацию полезного сигнала, аддитивное наложение белого гауссовского и импульсного шума, адаптивную фильтрацию и последующее корреляционное обнаружение. На основе временных диаграмм и спектральных оценок проанализирована эффективность предложенного подхода. Результаты показывают, что применение LMS-фильтра повышает отношение сигнал/шум на 5–10 дБ и увеличивает вероятность корректного приёма на 15–20%. Разработанная модель может использоваться в образовательном процессе для наглядного изучения принципов адаптивной обработки сигналов и повышения компетенций обучающихся в области радиотехнических систем.

Ключевые слова: MATLAB, ЛЧМ-сигнал, адаптивная фильтрация, алгоритм LMS, компенсация помех, цифровая обработка сигналов, корреляционный приём.

DEVELOPMENT OF A MODEL OF AN LFM SIGNAL RECEIVER WITH ADAPTIVE INTERFERENCE COMPENSATION IN MATLAB FOR STUDYING SIGNAL PROCESSING ALGORITHMS

M.V. Eliseev, A.Yu. Linovich

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, maks-eliseev-97@mail.ru

The summary. The article discusses the development of a virtual model of a linear frequency modulated (LFM) signal receiver equipped with an adaptive interference compensation system in the MATLAB mathematical modeling environment. The paper presents the theoretical foundations of LFM signal generation, a mathematical description of the Least Mean Squares (LMS) algorithm, and the structure of a digital correlation receiver. The software implementation of the model is described, including useful signal generation, additive superposition of white Gaussian and impulse noise, adaptive filtering, and subsequent correlation detection. Based on time-domain plots and spectral estimates, the efficiency of the proposed approach is analyzed. The results show that the use of an LMS filter improves the signal-to-noise ratio by 5–10 dB and increases the correct reception probability by 15–20%. The developed model can be used in the educational process to visually study the principles of adaptive signal processing and to enhance student competencies in radio engineering systems.

Keywords: MATLAB, LFM signal, adaptive filtering, LMS algorithm, interference compensation, digital signal processing, correlation receiver.

Современные радиолокационные и телекоммуникационные системы активно используют сигналы с линейной частотной модуляцией (ЛЧМ) благодаря их высокой разрешающей способности, устойчивости к многолучевому распространению и возможности точного измерения дальности. Однако в условиях экспоненциального роста плотности радиоэлектронных средств и преднамеренного радиоэлектронного подавления эффективность традиционных приёмников существенно снижается. Адаптивные методы компенсации помех позволяют динамически корректировать параметры приёмного тракта, минимизируя влияние внешних и внутренних шумов без потери полезной информации.

В связи с этим актуальной задачей является разработка и исследование виртуальных моделей приёмников с адаптивной обработкой, которые могут быть использованы как в научных целях, так и в образовательном процессе. Целью настоящего исследования является создание модели ЛЧМ-приёмника с адаптивной компенсацией помех в среде MATLAB, позволяющей наглядно изучить работу алгоритмов цифровой фильтрации и оценить их эффективность при различных сценариях зашумления.

Теоретические основы ЛЧМ-сигналов и адаптивной фильтрации

ЛЧМ-сигнал представляет собой колебание, мгновенная частота которого линейно изменяется во времени. Его математическая модель имеет вид:

$$s(t) = Acos(2\pi\left(f_0 t + \frac{K}{2}t^2\right) + \varphi),$$

где A– амплитуда;

f_0 – начальная частота;

K – коэффициент линейной частотной модуляции (скорость изменения частоты);

φ – начальная фаза.

Благодаря свойству узкой автокорреляционной функции, ЛЧМ-сигналы эффективно выделяются из зашумленной среды при корреляционном обнаружении.

Для подавления помех в цифровой приёмной цепи широко применяются адаптивные фильтры. В данной работе был выбран алгоритм наименьших квадратов (LMS), обеспечивающий баланс между скоростью сходимости, вычислительной сложностью и устойчивостью. Обновление весовых коэффициентов фильтра происходит по рекуррентному правилу:

$$w(n+1) = w(n) + \mu e(n)x(n),$$

где $w(n)$ – вектор коэффициентов фильтра;

μ – шаг адаптации (скорость обучения);

$e(n)$ – ошибка фильтрации;

$x(n)$ – входной вектор отсчётов.

При корректном выборе параметра μ алгоритм обеспечивает стабильную сходимость в условиях нестационарных помех, что делает его предпочтительным для реализации в системах реального времени.

Разработка модели в среде MATLAB

Моделирование выполнено в программной среде MATLAB с использованием встроенных инструментов обработки сигналов и библиотеки dsp. Структурно модель состоит из четырёх последовательных этапов (рис. 1)

1. **Генерация ЛЧМ-сигнала.** Формируется опорный сигнал длительностью $T = 0.1$ мс с частотой дискретизации $Fs = 1$ МГц, начальной частотой $f0 = 100$ кГц и девиацией $B = 100$ кГц;
2. **Моделирование помеховой обстановки.** К полезному сигналу аддитивно подмешивается белый гауссовский шум (AWGN) с заданным отношением сигнал/шум (SNR = 10 дБ), а также импульсные помехи с вероятностью появления $Pimp = 0.01$ и амплитудным коэффициентом усиления;
3. **Адаптивная фильтрация.** Реализован LMS-фильтр порядка $N = 16$ с шагом адаптации $\mu = 0.01$. В качестве опорного (желаемого) сигнала на этапе обучения используется эталонный ЛЧМ-сигнал, что позволяет алгоритму минимизировать среднеквадратическую ошибку и выделить полезную составляющую;

4. **Корреляционное обнаружение и спектральный анализ.** Очищенный сигнал подаётся на корреляционный приёмник, вычисляющий взаимную корреляцию с эталонной ЛЧМ-последовательностью. Для оценки спектральных изменений используется метод Уэлча (pwelch).

Примечание: Визуализация результатов включает временные диаграммы исходного, зашумлённого и отфильтрованного сигналов, а также графики спектральной плотности мощности, аналогичные тем, что используются при изучении процессов дискретизации и фильтрации в учебном процессе.

Результаты моделирования и анализ

В ходе численного эксперимента были получены следующие результаты, представленные на рисунке 2:

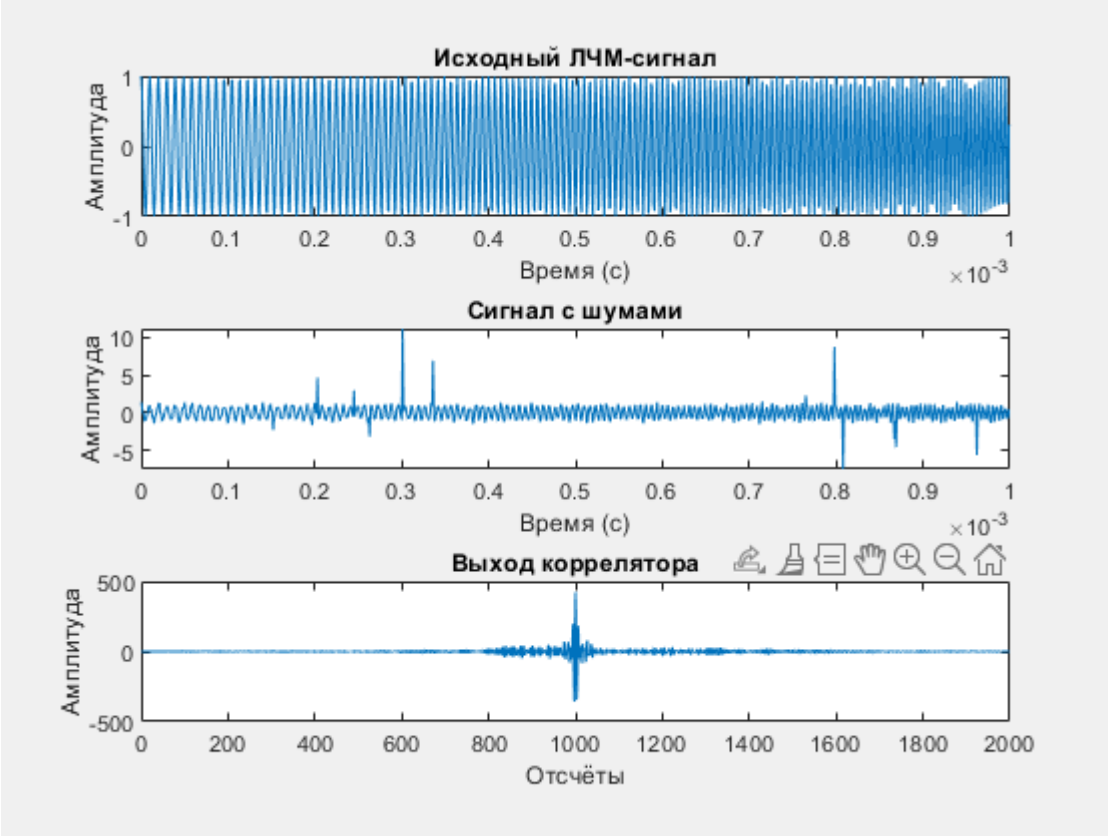


Рис. 2. Результаты моделирования обработки ЛЧМ-сигнала

- *Верхний график: исходный ЛЧМ-сигнал без помех.*
- *Средний график: сигнал с наложенными шумами (AWGN и импульсные выбросы).*
- *Нижний график: выход корреляционного приёмника после адаптивной обработки.*

Анализ графиков показывает следующее.

1. Исходный сигнал (верхний график). Демонстрируется классическая структура ЛЧМ-сигнала с линейно нарастающей частотой заполнения.

2. Зашумленный сигнал (средний график). Видно, что амплитуда полезного сигнала маскируется широкополосным шумом. Кроме того, присутствуют характерные вертикальные выбросы большой амплитуды, соответствующие моделируемым импульсным помехам. В таком виде прямое обнаружение сигнала затруднено.

3. Выход коррелятора (нижний график). После прохождения через адаптивный фильтр и корреляционную обработку наблюдается чёткий пик в районе 1000-го отсчёта. Это свидетельствует о том, что алгоритм LMS успешно подавил как широкополосный шум, так и импульсные помехи, позволив коррелятору выделить полезный сигнал на фоне остаточного шума.

Количественная оценка показала, что применение адаптивной фильтрации улучшает отношение сигнал/шум на 5–10 дБ и повышает вероятность корректного приёма на 15–20% по сравнению с приёмником без адаптации.

Заключение

Подводя итоги, можно выделить, что с использованием функционала среды MATLAB удалось разработать эффективную модель приёмника ЛЧМ-сигналов. В модель были интегрированы блоки генерации, имитации сложной помеховой обстановки и адаптивной фильтрации на базе алгоритма LMS.

Анализ результатов подтвердил, что адаптивная компенсация позволяет существенно улучшить качество приёма сигналов даже при наличии мощных импульсных помех. Наличие подобных виртуальных моделей способствует более наглядному и детальному изучению теоретических сведений в области цифровой обработки сигналов, что, в свою очередь, повышает уровень приобретаемых компетенций обучающимися. В перспективе планируется расширение модели за счёт внедрения более сложных алгоритмов (RLS, нейросети) и верификация на аппаратных прототипах.

Библиографический список

1. Проакис Дж. Г. Цифровая связь / Дж. Г. Проакис; пер. с англ. – 4-е изд. – М.: Радио и связь, 2000. – 800 с.
2. Хайкин С. Теория адаптивных фильтров / С. Хайкин; пер. с англ. – 5-е изд. – М.: Вильямс, 2009. – 1440 с.
3. Сколник М. И. Радиолокационный справочник / М. И. Сколник; пер. с англ. под ред. В. С. Кельина. – 3-е изд. – М.: Сов. радио, 1979. – 672 с.
4. IEEE Transactions on Signal Processing: научный журнал / IEEE. – New York: IEEE Press, 1993–н.в.
5. Гоноровский И. С. Радиотехнические цепи и сигналы: учебник для вузов / И. С. Гоноровский. – 4-е изд., перераб. и доп. – М.: Радио и связь, 1986. – 512 с.
6. Documentation: DSP System Toolbox – LMS Filter. The MathWorks, Inc. URL: https://www.mathworks.com/help/dsp/ref/dsp.lmsfilter.html (дата обращения: 15.04.2026).

УДК 621.396; ГРНТИ 49.33.35

ПРИМЕНЕНИЕ НЕЙРОСЕТЕВЫХ АРХИТЕКТУР ДЛЯ АДАПТАЦИИ РАДИОКАНАЛА К ПОМЕХОВОЙ ОБСТАНОВКЕ

В.С. Плющиков, А.В. Бакке

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, wladpluyschikov@mail.ru

Аннотация. В работе рассматривается применение искусственных нейронных сетей для решения задач систем адаптации к помеховой обстановке на этапе радиомониторинга. К таким задачам относятся мониторинг спектра, прогнозирование состояния его занятости и классификация сигналов. Проведен обзор основных архитектур нейросетей: полносвязных сетей прямого распространения, сверточных и рекуррентных сетей. Приведена сравнительная характеристика данных архитектур и рассмотрены примеры реализации для решения вышеперечисленных задач.

Ключевые слова: нейронные сети, мониторинг спектра, классификация сигналов, прогнозирование спектра, MLP, CNN, RNN, помеховая обстановка, когнитивное радио.

THE USE OF NEURAL NETWORK ARCHITECTURES TO ADAPT A RADIO CHANNEL TO AN INTERFERENCE ENVIRONMENT

V.S. Plushikov, A.V. Bakke
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, wladpluyschikov@mail.ru

The summary. The paper considers the use of artificial neural network to solve problems of systems adapting to interference environment at the stage of radio monitoring. Such tasks include monitoring the spectrum, predicting its occupancy status, and classifying signals. The main architectures of neural networks are reviewed: fully connected direct distribution networks, convolutional and recurrent networks. A comparative characteristic of these architectures is given and implementation examples for solving the above tasks are considered.
Keywords: neural networks, spectrum monitoring, signal classification, spectrum prediction, MLP, CNN, RNN, interference environment, cognitive radio.

В настоящее время в системах связи наблюдается стремительный рост количества устройств, что в конечном счете приводит к усложнению электромагнитной обстановки. Классические методы обработки сигналов, такие как согласованная фильтрация и энергетическое детектирование, являются оптимальными, однако в условиях сложной электромагнитной обстановки, высокой нестационарности канала связи и низкого отношения сигнал/шум (ОСШ) синтез оптимального решения может быть затруднителен. Трудность синтеза связана с высокими вычислительными затратами на оперативную оценку характеристик канала и исполнение алгоритма адаптации в реальном масштабе времени.

Все большее внимание привлекают искусственные нейронные сети (ИНС), которые заменяют классические алгоритмы обработки сигналов. Данные модели способны обучаться на наборах данных, выявляя сложные зависимости, которые не могут быть описаны строго аналитически. Отличительной способностью является перенос вычислительной сложности с этапа непосредственного применения на процесс обучения сети, что позволяет сократить время на решение целевой задачи.

Выбор архитектуры ИНС является фундаментальной задачей в разработке системы, который определяет ее способность эффективно обрабатывать радиотехнические данные. В работе рассмотрены три основных типа архитектур [1].

Полносвязные сети прямого распространения (MLP)

Данная архитектура является исторически первой и по-другому называется многослойным перцептроном. Каждый нейрон такой сети выполняет взвешенное суммирование входов с последующим нелинейным преобразованием (функцией активации). Результат преобразования отдельного нейрона можно записать в виде (1).

$$y(x_1, x_2, x_n) = f(w_1 x_1 + w_2 x_2 \ldots + \ldots w_n x_n), \quad (1)$$

где $x_1 \ldots x_2$ – входные значения нейрона;

$w_1 \ldots w_2$ – весовые коэффициенты входов нейрона;

$f(x)$ – функция активации.

Группа нейронов расположенных параллельно образует слой. Выходы нейронов каждого слоя, кроме последнего, соединены с каждым нейроном последующего слоя.

Процесс обучения сети заключается в минимизации функции потерь, которая может быть описана выражением (2).

$$L = \frac{1}{n}\sum_{k=0}^{n}\left(y_{true} - y_{pred}\right)^2, \quad (2)$$

где n – количество данных для обучения;

y_{true} - эталонное значение из таблицы;

y_{pred} – предсказанное нейросетью значение.

Выбор весовых коэффициентов на начальном этапе, как правило, делается произвольно, а далее известными методами (например, градиентными) происходит итеративно коррекция этих коэффициентов пока функция потерь не устремится заданной точности.

Многослойный перцептрон отлично справляется с задачами классификации и регрессии, однако недостатком является большое количество нейронов, что значительно усложняет процесс обучения такой сети.

Сверточные нейронные сети (CNN)

В основе сверточной нейронной сети лежит операция свертки, которая может быть описана выражением (3).

$$s(t) = \int x\,(a)w(t-a)da, \tag{3}$$

где $x(a)$ - входная функция;

$w(t)$ – ядро свертки.

Ядро свертки представляет собой матрицу весов, которая скользит с определенным шагом по всем входным данным. На каждой позиции вычисляется поэлементное произведение ядра на текущий участок входа и суммируется, формируя элемент выходной карты признаков, который рассчитывается по формуле 4.

$$v_{k,m} = \sum_{i=1}^{N}\sum_{j=1}^{M} x_{i+k,j+m} * w_{i,j} + b_0, \tag{4}$$

где N, M – определяют размер ядра свертки;

k, m – шаг сдвига ядра свертки по матрице данных;

$w_{i,j}$ – весовой коэффициент ядра;

b_0 – смещение.

Для обработки карт признаков используются масштабирующие слои (Pooling Layer), которые нужны для сокращения количества параметров путем выделения наиболее значащих признаков. После нескольких блоков свертки, активации и масштабирования в конце ставятся полносвязные слои многослойного перцептрона для нелинейной комбинации извлечённых признаков для решения целевой задачи – классификации, регрессии или детектирования.

Сверточные нейросети хорошо себя зарекомендовали при классификации изображений, что в радиотехнике может иметь место в качестве классификатора видов сигналов или занятости спектра по спектрограмме.

Рекуррентные нейронные сети (RNN)

Рекуррентные нейронные сети содержат в своем составе слои, которые имеют обратную связь, т.е. выходные значения слоя подаются на вход с некоторой задержкой. В каждый момент времени на нейроны подается входной вектор значений x_t и предыдущее значение $h_{t\text{-}1}$, вычисленное этим же нейроном на предыдущей итерации (рис.1). В общем случае выход нейрона слоя можно записать как $h_t = g(h_{t-1}, x_t)$. Благодаря механизму внутренней памяти, реализуемому через скрытое состояние, RNN способны моделировать временные и контекстуальные зависимости в последовательностях данных. Классические RNN страдают от проблемы затухающих градиентов, умножаясь на одну и ту же матрицу много раз они

экспоненциально стремятся к нулю. В то же время стоит проблема устойчивости нейросети, т.к. она теперь является нелинейной динамической системой. Модификации RNN такие как LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit) позволяют решить эту проблему, что делает их незаменимыми для задач долгосрочного прогнозирования.

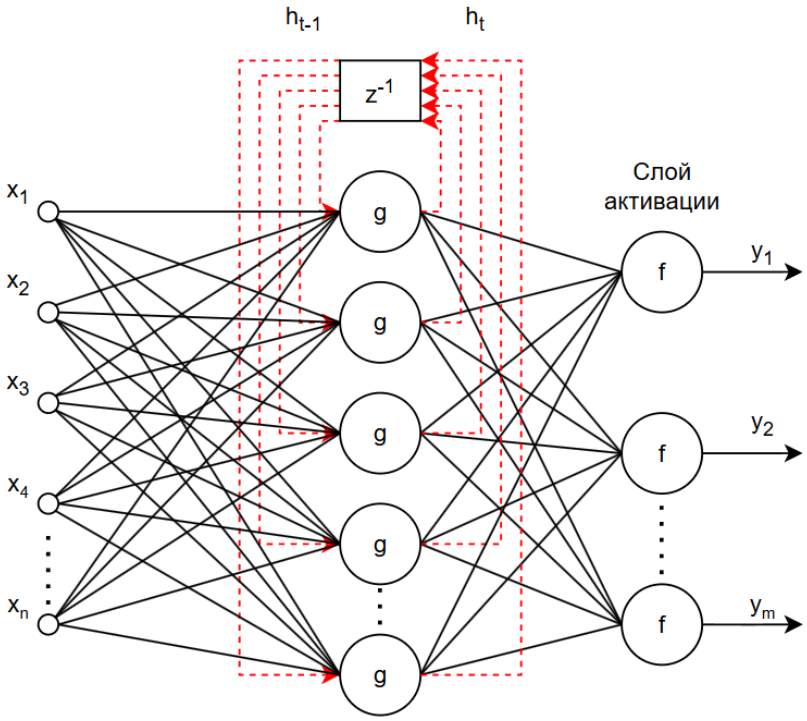


Рис. 1. Рекуррентный слой

Сравнительная характеристика архитектур

С точки зрения практической реализации системы на основе нейронной сети наиболее значимыми характеристиками будут являться вычислительная сложность обучения, тип и структура входных данных, а также специфичность решаемых задач. В таблице 1 представлен сравнительный анализ рассмотренных архитектур.

Таблица 1. Сравнительный анализ архитектур ИНС

Архитектура	Тип данных	Основные задачи в радиотехнике	Вычислительная сложность
MLP	Векторы признаков	Классификация по признакам	Высокая (большое число параметров)
CNN	I/Q-сигналы, спектрограммы	Мониторинг спектра, обнаружение сигналов и их классификация	Умеренная (отброс незначительных параметров)
RNN	Временные ряды	Прогнозирование занятости канала, моделирование долгосрочных зависимостей	Высокая (итеративные вычисления)

Проведенный анализ литературы позволили выделить 3 наиболее значимые задачи, решаемые с помощью ИНС для обеспечения адаптации радиоканала – мониторинг спектра, классификация сигналов и прогнозирование состояния спектра.

CNN являются наиболее эффективным инструментом для задач мониторинга и классификации сигналов. В работе [2] предложено использовать CNN для бинарной классификации занятости канала. Авторы сравнили несколько вариантов архитектур CNN, включая ба-

зовую модель, модель со слоями пакетной нормализации (Batch Normalization) и модель с глобальным усредняющим пулингом (GAP). Базовая CNN показала точность до 99,5%, однако она подвержена переобучению, что снижает точность до 80%. Применение слоев пакетной нормализации позволило устранить переобучение и сохранить точность в пределах 97,5%. Важным результатом стало то, что CNN способна обнаруживать сигналы, не участвовавшие в обучении, что свидетельствует о выделении общих признаков. В сравнении с традиционными методами (энергетический детектор, метод энтропии) CNN показала преимущество при низких значениях ОСШ (менее - 8 дБ).

Наиболее популярной задачей, решаемой с помощью ИНС, является классификация сигналов по виду модуляции. В работе [3] была применена CNN для анализа I/Q-представления сигнала как двумерного изображения, что позволило достичь точности 93% при ОСШ выше 10 дБ. Однако у модели возникли проблемы с классификацией амплитудных и широкополосных частотных сигналов, чьи характеристики менее выражены во временной области. В исследовании [4] рассматривается более сложный случай классификации сигналов, когда на вход ИНС поступает сигнал с неизвестным типом. Предложенный подход позволяет не только классифицировать известные сигналы, но и относить неизвестные к определенным группам. При этом достигается точность порядка 83%.

Прогнозирование состояния спектра относится к задаче анализа временных рядов, что определяет выбор рекуррентной архитектуры сети. В работе [5] применяется гибридная архитектура, сочетающая CNN и RNN, что обусловлено корреляционными связями не только во временной области, но и в спектральной. Предложенная гибридная архитектура позволила на 39% снизить среднеквадратическую ошибку по сравнению с базовым методом (скрытая марковская модель). В работе [6] продемонстрирована практическая реализация системы мониторинга и прогнозирования спектра на базе IoT- устройства. Сверточная нейронная сеть анализирует временные ряды и предсказывает занятость спектра на интервале до 150 мс, что подтверждает возможность внедрения подобных решений в устройства с ограниченными вычислительными ресурсами.

Библиографический список

1. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с анг. А. А. Слинкина. – 2-е изд., испр. – М.: ДМК Пресс, 2018. – 652 с.: цв. ил.

2. Abdelbaset S. E., Kasem H. M., Khalaf A. A., Hussein A. H., Kabeel A. A. Deep Learning-Based Spectrum Sensing for Cognitive Radio Applications / Sensors 2024, 24, 7907, p. 22.

3. O'shea T. J., Corgan J., Clancy T. C., Convolutional Radio Modulation Recognition Networks / International Conference on Engineering Application of Neural Networks, 2016, P. 213-226.

4. Shi Y., Davaslioglu K., Sagduyu Y. E., Headley W. C., Fowler M., Green G. Deep Learning for RF signal Classification in Unknown and Dynamic Spectrum Environments / IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN). 2019. P. 1-10

5. Pan G., Yau D. K. Y., Zhou B., Wu Q. Deep Learning for spectrum Prediction in Cognitive Radio Networks: State-of-the-Art, New Opportunities, and Challenges / IEEE network, vol. 40(1), 2026, pp. 192-200.

6. Rojas A., Follet G., Jovanovic-Dolecek G., De La Rosa J. M., Linan-Cembrano G. Predicted-Based Spectrum Sensing Framework for Cognitive Radio / IEEE Open Journal of Circuits and Systems, 6, 2025, pp. 313-328.

УДК 004.94; ГРНТИ 28.17.19

РАЗРАБОТКА МОДЕЛИ СИНХРОНИЗАЦИИ СРЕДСТВ СВЯЗИ В ОТЕЧЕСТВЕННОЙ СРЕДЕ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ SIMINTECH

Н.Д. Сивов, В.А. Волченков

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, sivovnik@gmail.com

Аннотация. В работе рассматривается моделирование системы фазовой автоподстройки частоты в средах Simulink пакета MATLAB и SimInTech. Исследуется реализация генератора, управляемого напряжением (VCO), цифрового КИХ-фильтра и контура обратной связи, обеспечивающих компенсацию фазового и частотного рассогласования. Проводится анализ полученных результатов и сравнение возможностей обеих сред математического моделирования.

Ключевые слова: MATLAB, Simulink, SimInTech, VCO, фазовая автоподстройка, PLL, моделирование, синхронизация, фазовое рассогласование, КИХ-фильтр.

DEVELOPMENT OF A COMMUNICATION SYSTEM SYNCHRONIZATION MODEL IN THE DOMESTIC MATHEMATICAL MODELING ENVIRONMENT SIMINTECH

N.D. Sivov, V.A. Volchenkov

Ryazan State Radio Engineering University named after V.F. Utkin, Russian Federation, Ryazan, sivovnik@gmail.com

Abstract. The paper considers the modeling of a phase-locked loop (PLL) system in the Simulink environment of the MATLAB package and in SimInTech. The implementation of a voltage-controlled oscillator (VCO), a digital FIR filter, and a feedback loop that ensures compensation of phase and frequency mismatch is studied. An analysis of the obtained results is carried out, along with a comparison of the capabilities of both mathematical modeling environments.

Keywords: MATLAB, Simulink, SimInTech, VCO, phase-locked loop, PLL, modeling, synchronization, phase error, FIR filter.

Введение

Моделирование – ключевой этап в разработке современных телекоммуникационных систем связи. Существует необходимость протестировать и проанализировать разрабатываемую схему в различных условиях. Поскольку разработка и внедрение новых систем требует значительных денежных средств, для расчета и моделирования на первых этапах используют среды математического моделирования. Это позволяют дать теоретическую оценку, разработанной системе в различных условиях и выявить её уязвимые стороны.

Обеспечение синхронизации приемника и передатчика является одним из важнейших этапов в проектировании систем связи, из-за чего моделирование и тестирование подобных систем играет важную роль. Фазовая автоподстройка частоты (ФАПЧ) является одним из важнейших примеров подобной системы.

Для проектирования и анализа модулей связи применяются различные среды блочного и математического моделирования. Одной из таких сред является модуль Simulink [1] среды MATLAB. Данный модуль позволяет собирать различные системы за счет внутренних заранее созданных блоков. Наряду с Simulink в России широко используется SimInTech - среда разработки математических моделей, алгоритмов управления, интерфейсов управления и автоматической генерации кода для контроллеров управления и графических дисплеев [2].

В настоящей работе проводится моделирование системы фазовой автоподстройки частоты в указанных средах и анализ полученных результатов.

MATLAB

MATLAB [1] является одной из самых широко используемых сред для моделирования систем связи. Благодаря многолетнему развитию, MATLAB предоставляет большой набор инструментов для работы с цифровой обработкой сигналов, модуляцией, демодуляцией, кодированием и анализом помехоустойчивости.

Одним из ключевых преимуществ MATLAB является наличие специализированных библиотек. Например, Communications Toolbox [3] позволяет моделировать различные схемы модуляции (QAM, PSK, FSK), а также исследовать влияние каналов распространения, включая AWGN, Райса и Релея. Кроме того, в MATLAB интегрирована среда Simulink, что облегчает разработку сложных моделей за счет использования блоков.

Однако, начиная с 5 марта 2022 года нельзя официально приобрести лицензию, поскольку компания The MathWorks приостановила свою деятельность на территории РФ.

Моделирование в MATLAB Simulink

Как было упомянуто ранее MATLAB Simulink [1] обладает обширным функционалом. На рисунке 1 представлена схема синхронизации при изменении несущей частоты и фазы.

Схема состоит из двух основных подсистем. Первая изображена на рисунке 2. В данной подсистеме генерируется несущая частота, а также вносятся сдвиг по частоте и скачки фазы. На рисунке 3 представлена схема внесения частотных искажений.

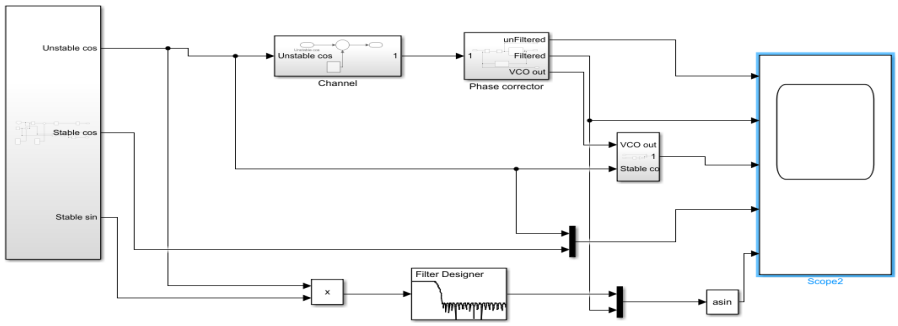


Рис. 1. Схема системы синхронизации в Simulink

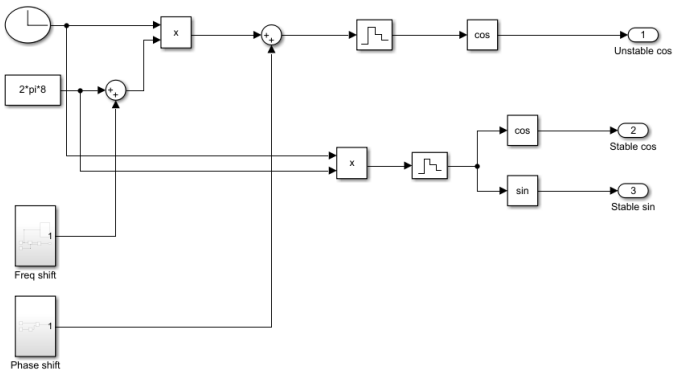


Рис. 2. Подсистема генерации исходного сигнала

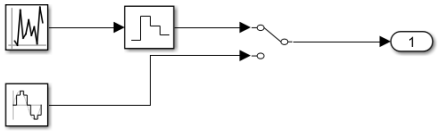


Рис. 3. Подсистема генерации частного и фазового сдвига

Вторая подсистема – блок фазовой коррекции (рисунок 4). Ключевые компоненты здесь – цифровой рекурсивный фильтр и генератор, управляемый напряжением.

Рекурсивный фильтр сглаживает сигнал фазовой ошибки и формирует управляющий сигнал для генератора. Это помогает снизить влияние высокочастотных составляющих ошибки и стабилизировать систему.

Генератор, управляемый напряжением, создает гармонический сигнал, частота которого зависит от входного управляющего сигнала. Его задача – корректировать частоту и фазу выходного сигнала для минимизации фазовой ошибки относительно опорного сигнала.

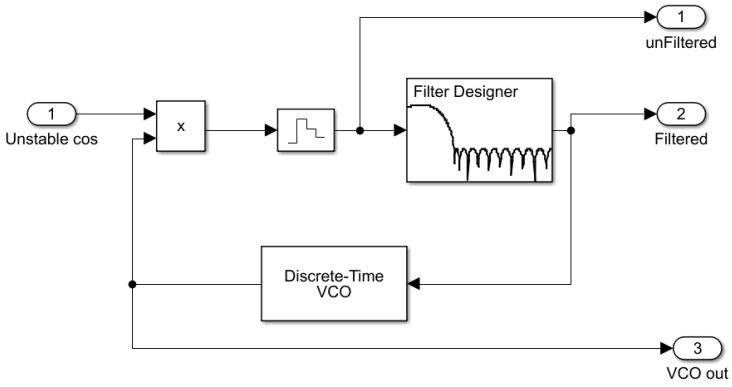


Рис. 4. Подсистема компенсации фазового сдвигов

После прохождения фазового детектора, сигнал ошибки содержит как низкочастотную составляющую, связанную с разностью фаз, так и дополнительные высокочастотные элементы, возникающие при перемножении гармоник.

Цифровой КИХ-фильтр нужен для удаления высокочастотной части сигнала и сохранения полезной низкочастотной составляющей, соответствующей средней фазовой ошибке.

Отфильтрованный сигнал ошибки – это сглаженное управляющее воздействие для VCO. Его амплитуда и знак показывают, как и насколько нужно скорректировать частоту генератора.

Во время захвата синхронизации ошибка постепенно становится меньше. В стабильном состоянии сигнал ошибки приближается к постоянному значению (или к нулю), что говорит о совпадении частот и фиксации фазового рассогласования, что можно пронаблюдать на рисунках 5 и 6. На рисунке 5 представлен график фазового рассогласования. Периодические всплески, возникающие каждые 10 секунд, обусловлены заданными параметрами блоков внесения частотного и фазового сдвига. Эти возмущения искусственно нарушают синхронизацию системы.

После каждого возмущения система фазовой автоподстройки компенсирует возникшее рассогласование. На рисунке 6 видно, что после всплеска начинается переходный процесс, в ходе которого величина фазовой ошибки постепенно уменьшается. Это свидетельствует о корректной работе контура синхронизации и его способности восстанавливать фазовое равновесие.

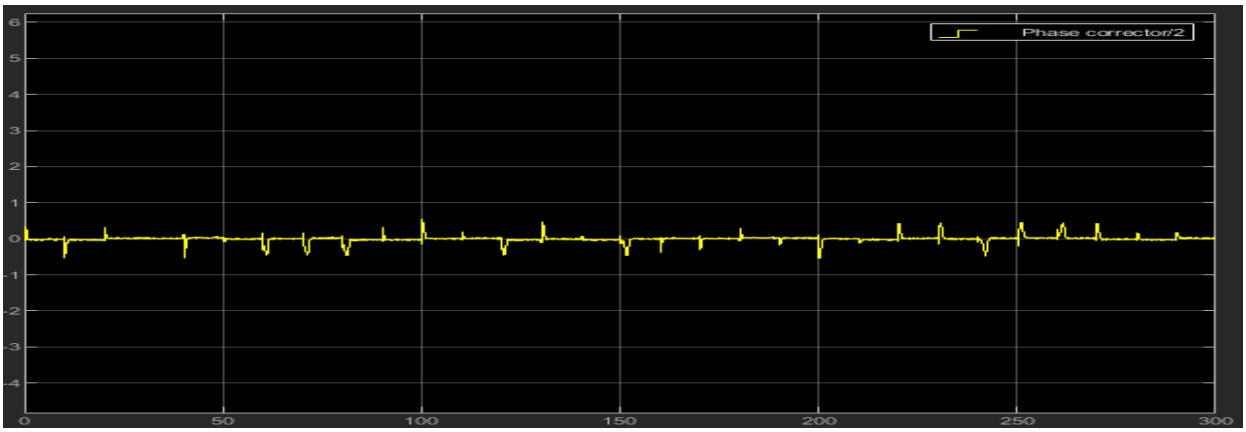


Рис. 5. График фазового рассогласования

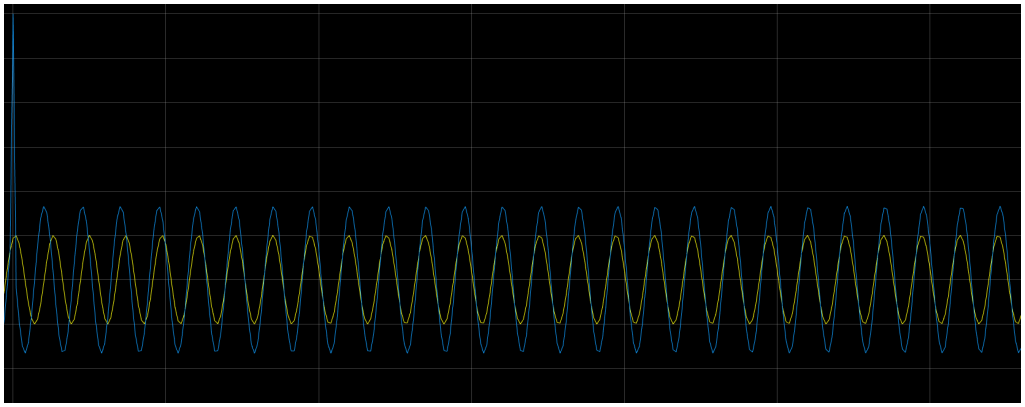


Рис. 6. График синхронизации колебания.

Моделирование в SimInTech

SimInTech – это интегрированная среда моделирования, схожая по принципам работы с Simulink, предназначенная для моделирования различных физических процессов [2]. В ней также используется блочный подход, что позволяет пользователям создавать сложные модели, комбинируя стандартные компоненты. В SimInTech также, как и в Engee и Simulink есть библиотека блоков «Цифровая связь» для создания моделей систем связи.

На рисунке 7 представлена система синхронизации. Аналогично Simulink, в SimInTech система состоит из двух основных подсистем. На рисунке 8 изображен генератор исходного сигнала с подсистемами внесения частотных и фазовых искажений.

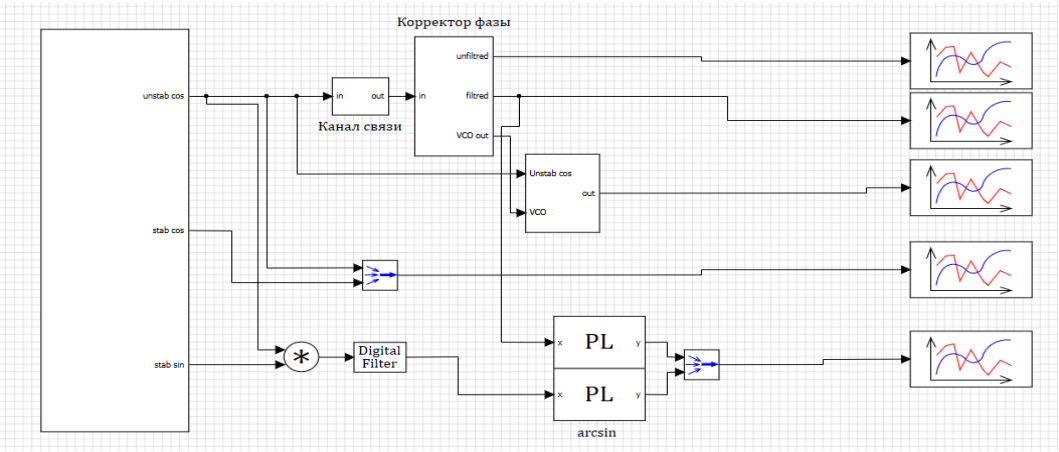


Рис. 7. Схема системы синхронизации в SimInTech

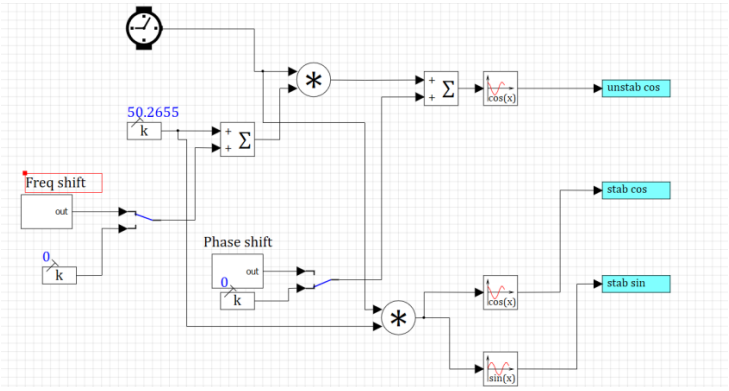


Рис. 8. Подсистема генерации исходного сигнала

На рисунке 9 изображена схема компенсации фазового сдвига.

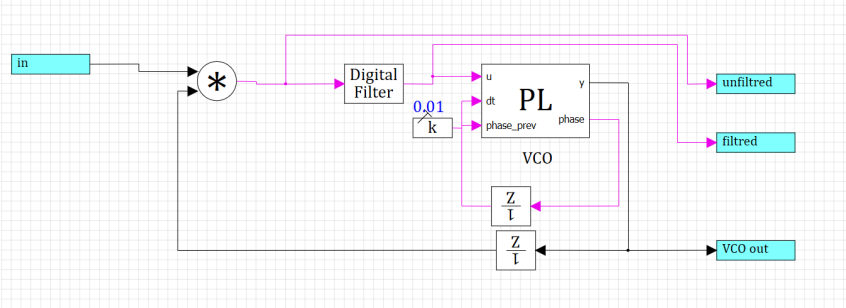


Рис. 9. Подсистема компенсации фазового сдвига

В среде SimInTech отсутствует аналог блока VCO, поэтому для его реализации используется программируемый блок “PL”. На схеме присутствуют 2 петли обратной связи.

Первая петля обратной связи необходимая для накопления изменения фазы. Возможности программируемого блока сильно ограничены и поэтому необходимо неявное накопление изменения фазы.

Вторая петля – это стандартная петля обратной связи для VCO, аналогичная Simulink. Она компенсирует возникающие фазовые искажения.

На рисунке 10 представлен код реализации блока VCO в SimInTech. Команда “input” создаёт входные порты для соответствующих переменных. В данной реализации используются три входных порта: управляющее напряжение “u”, шаг дискретизации “dt” и предыдущее значение фазы “phase_prev”.

Команда “output” формирует выходные порты. Переменная “y” – это выходной сигнал, вычисленный как косинус от фазы, а “phase” – это текущее значение фазы, которое используется для накопления фазового приращения через цепь обратной связи. Параметр “F” задаёт опорную (центральную) частоту генератора, а коэффициент “KV” определяет чувствительность VCO к управляющему сигналу.

```
input u;
input dt;
input phase_prev;
output y;
output phase;

F = 8;
KV = 1;

delta_phi = 2.0 * pi * dt * (F + KV * u);
phase = phase_prev + delta_phi;

y = cos(phase);
```

Рис. 10. Код реализации блока VCO

Процесс автоподстройки в SimInTech идентичен Simulink MATLAB. Сигнал ошибки также содержит полезную низкочастотную часть, и высокочастотный шум. Для его подавления используется низкочастотный цифровой КИХ-фильтр. Далее, отфильтрованный сигнал поступает на VCO в роли управляющего напряжения.

При рассогласовании, величина ошибки постепенно снижается, стремясь к постоянному значению или нулю. Достижение данного значения, является признаком успешно восстановленной синхронизации.

Возмущения возникают периодически каждые 10 секунд в виде всплесков, что можно пронаблюдать на рисунке 11. С течением времени, данный всплеск стремится к нулю, что свидетельствует о постепенном восстановлении синхронизации.

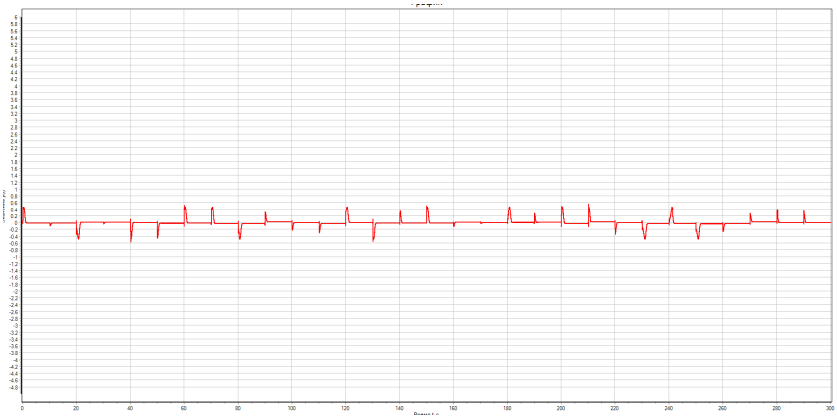


Рис. 11. График фазового рассогласования

На рисунке 12 изображены графики косинусоид. Из данного рисунка видно, что на 20 секунде возникает рассогласование между двумя косинусами. Однако, постепенно они синхронизируются, и на 21.3 секунде сигналы вновь совпадают, что свидетельствует о корректной работе ФАПЧ в среде SimInTech.

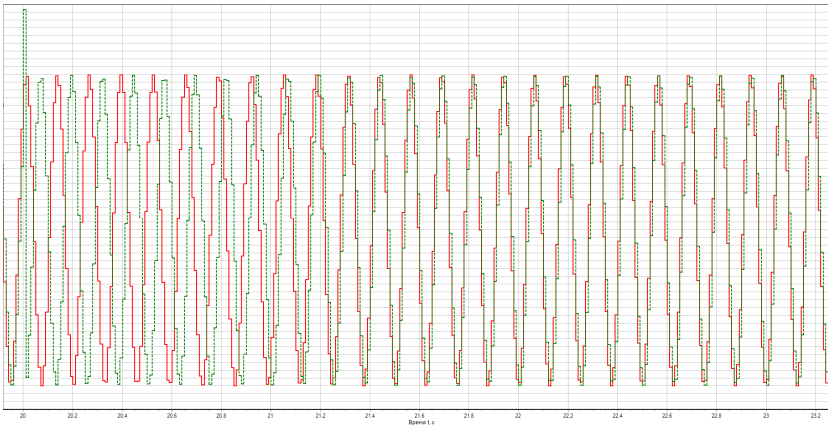


Рис. 12. График синхронизации колебания.

Вывод

В ходе работы была реализована и сравнена идентичная система ФАПЧ в двух различных средах проектирования. В среде Simulink уже присутствуют все необходимые блоки, в том числе и VCO. В результате, система корректно обнаружила и скорректировала периодически вносимое фазовое искажение.

В среде SimInTech отсутствует отдельно блок VCO. Его получилось реализовать на основе программируемого блока “PL” и набора присутствующих в нем команд. Однако, ввви-

ду внутренних ограничений блока, связанных с работой циклов, накопление фазы пришлось реализовать неявно в виде дополнительной петли обратной связи.

Результаты, полученные в обеих средах, идентичны и корректны, из чего можно сделать вывод, что SimInTech подходит на роль аналога Simulink при разработке и тестировании ФАПЧ.

Библиографический список

1. MATLAB: [сайт]. – URL: https://www.mathworks.com/ (дата обращения: 15.02.2026).
2. SimInTech: [сайт]. – URL: https://simintech.ru/ (дата обращения: 15.02.2026).
3. Сергиенко А.Б. Цифровая обработка сигналов: учеб. пособие. — 3-е изд. — СПб.: БХВ-Петербург, 2011. — 768 с.

УДК 004.94; ГРНТИ 28.17.19

РАЗРАБОТКА МОДЕЛИ ФОРМИРОВАНИЯ АНАЛОГОВОГО И ДИСКРЕТНОГО СИГНАЛОВ В СРЕДЕ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ SIMINTECH ДЛЯ ИЗУЧЕНИЯ ИХ ХАРАКТЕРИСТИК ОБУЧАЮЩИМИСЯ

Л.А. Фетисова, В.А. Волченков
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, lidia.fetisovaa@gmail.com

Аннотация. В статье рассматривается разработка моделей формирования аналоговых и дискретных сигналов в среде математического моделирования SimInTech для изучения их характеристик обучающимися. В начале работы представлены краткие теоретические сведения о классификации сигналов по признакам непрерывности, математическое описание гармонических колебаний и теоретические основы дискретизации сигналов. Далее приведено описание математических моделей, которые реализуют формирование аналоговых и дискретных сигналов, соответственно. Для вывода результатов моделирования используются временные диаграммы, благодаря которым можно наглядно проследить процесс дискретизации сигналов. Исходя из результатов проделанной работы, можно сделать выводы, что подобные виртуальные математические модели способствуют более наглядному и детальному изучению теоретических сведений в области радиотехнических цепей и сигналов, что, в свою очередь, повышает уровень приобретаемых компетенций обучающимися.
Ключевые слова: SimInTech, математическое моделирование, аналоговый сигнал, дискретный сигнал, дискретизация, цифровой сигнал, гармонические колебания.

DEVELOPMENT OF A MODEL OF FORMATION OF ANALOG AND DISCRETE SIGNALS IN THE ENVIRONMENT OF MATHEMATICAL MODELING SIMINTECH FOR THE STUDY OF THEIR CHARACTERISTICS BY STUDENTS

L.A. Fetisova, V.A. Volchenkov
Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, lidia.fetisovaa@gmail.com

The summary. The article discusses the development of models for generating analog and discrete signals in the SimInTech mathematical modeling environment to study their characteristics by students. At the beginning of the work, brief theoretical information on the classification of signals by continuity features, a mathematical description of harmonic oscillations, and the theoretical foundations of signal discretization are presented. Next, a description of mathematical models that implement the generation of analog and discrete signals, respectively, is provided. To output the simulation results, time diagrams are used, which make it possible to visually trace the signal discretization process. Based on the results of the work performed, it can be concluded that such virtual mathematical models contribute to a more visual and detailed study of theoretical information in

the field of radio engineering circuits and signals, which, in turn, increases the level of competencies acquired by students.
Keywords: SimInTech, mathematical modeling, analog signal, discrete signal, sampling, digital signal, harmonic oscillations.

В настоящее время всё бóльшая часть образовательных процессов осуществляется с использованием цифровых технологий. Особенно актуальна тема цифровизации становится для подготовки студентов с техническим уклоном, например, при изучении процессов происходящих в радиотехнических системах. С помощью специализированных сред математического моделирования можно разрабатывать и собирать модели формирования различных видов сигналов, что, в свою очередь, будет способствовать более наглядному изучению процессов, происходящих внутри системы на различных этапах прохождения сигнала, так и во всей в целом.

Сейчас лабораторные работы по дисциплине «Радиотехнические цепи и сигналы» проводятся на реальных физических макетах в лабораторных аудиториях, что сопровождается рядом технических сложностей. В первую очередь, работа с реальными макетами требует особой аккуратности при работе с ними. В ином случае, макеты быстро приходят в негодность, а поддерживать их работоспособность бывает сложно и порой слишком дорого. Во-вторых, студентам не всегда очевидно, что происходит внутри многофункционального лабораторного макета, так как им доступен лишь функционал выставления определенных параметров сигнала в генератор и визуальный вывод результата на экран осциллографа. В-третьих, что не маловажно, работа с установками подключенными к сети, сопровождается определенными рисками при работе.

Работа с виртуальными макетами лишена всех перечисленных недостатков. Позволяет гибко работать с собранными моделями, анализировать что меняется в работе системы при вводе того или иного блока из библиотеки. Помимо этого, можно варьировать параметры исследуемых сигналов и наблюдать эти изменения на экране компьютера в считанные секунды.

Среда SimInTech представляет собой отечественную среду математического моделирования технических систем, разработанную компанией «ЗВ Сервис» и предназначенную для создания виртуальных моделей динамических систем различной физической природы [1]. Плюсами работы в данной программе являются: интуитивно понятный графический интерфейс; большая библиотека готовых функциональных блоков; возможность расширения функциональности за счёт создания недостающих блоков на основе внутреннего языка программирования.

Целью настоящего исследования является разработка моделей формирования аналоговых и дискретных сигналов в среде SimInTech, которые можно будет использовать в образовательном процессе для формирования у обучающихся более структурированных представлений о процессах преобразования сигналов.

Классификация сигналов по признакам непрерывности

С точки зрения теории под сигналом подразумевается физический процесс, который изменяется с течением времени и, при этом, несет информацию о состоянии или характеристиках некоторого объекта [2]. Если рассматривать сигнал в виде математической функции, то это функция одной или нескольких независимых переменных, наиболее часто – функция времени $s(t)$.

Радиотехнические сигналы можно классифицировать по двум независимым признакам: характере изменения независимой переменной (времени) и характере изменения зависимой переменной (амплитуды). По каждому из этих двух признаков радиотехнический сиг-

нал может быть либо непрерывным, то есть принимающим любые значения из некоторого интервала, либо дискретным, то есть принимающим значения только из счётного множества.

Аналоговый сигнал $s(t)$ определён для любого момента времени t из некоторого интервала и может принимать любые значения амплитуды из допустимого диапазона. К примеру, напряжение на выходе микрофона, температура объекта, измеряемая термопарой, освещённость, регистрируемая фотоэлементом, всё это является аналоговыми сигналами.

Дискретный сигнал $s(n) = s(nT)$, где T – период дискретизации, $n \in Z$, представляет собой последовательность отсчётов аналогового сигнала, взятых в равноотстоящие моменты времени. При этом значения амплитуды сохраняют непрерывный характер.

Математическое описание гармонических колебаний

Одним из самых распространённых периодических сигналов является гармоническое колебание. Такой сигнал математически может быть описан синусоидальной или косинусоидальной функцией времени. Математическая модель гармонического колебания имеет вид [3]:

$$s(t) = A_m \sin(\omega_0 t + \varphi_0), \tag{1}$$

где A_m – амплитуда колебания, определяющая максимальное отклонение колебания от нулевого уровня;

$\omega_0 = 2\pi f_0$ — циклическая частота;

φ_0 – начальная фаза, определяющая значение сигнала в момент времени $t = 0$.

В соответствии с теоремой Фурье, периодический сигнал может быть представлен в виде суммы гармонических составляющих с кратными частотами (ряд Фурье), а непериодический сигнал – в виде интеграла по непрерывному спектру частот (интеграл Фурье). Используя данные понятия мы можем переносить анализ сигнала из временной в частотную область и работать уже со спектрами сигналов.

Теоретические основы дискретизации сигналов

Процесс дискретизации заключается в преобразовании непрерывного по времени сигнала $s(t)$ в последовательность дискретных отсчётов $s(n)$, взятых с периодом дисретизации T_d.

Математическая модель дискретизации основана на представлении выходного сигнала как произведения входного сигнала на периодическую последовательность дельта-функций Дирака:

$$s_d(t) = s(t) \cdot \sum_{n=-\infty}^{+\infty} \delta(t - nT_d) = \sum_{n=-\infty}^{+\infty} s(nT_d) \cdot \delta(t - nT_d). \tag{2}$$

Существует теорема Котельникова, которая устанавливает условие, при котором дискретизация не приводит к потере информации [1]:

$$f_d \geq 2f_{max}$$

где $f_{\max}$ — максимальная частота спектра сигнала.

Согласно этому условию, для того, чтобы в точности восстановить входной сигнал необходимо, чтобы частота дискретизации была равна или, что предпочтительнее, больше удвоенной максимальной частоте в спектре сигнала.

И наоборот, частота Найквиста $f_N = f_d / 2$ определяет верхнюю границу полосы частот, которая может быть корректно представлена дискретным сигналом.

Если данные условия нарушаются, то происходит наложение спектров, что в конечном итоге искажает восстановленный входного сигнала.

Модель формирования аналоговых сигналов

Для исследования будем использовать модулированный сигнал, представляющий собой произведение трёх гармонических составляющих [2]:

$$s(t) = A_1 \cos(2\pi f_1 t) \cdot A_2 \cos(2\pi f_2 t) \cdot A_3 \cos(2\pi f_3 t),$$

где $A_1 = 2$ В, $A_2 = 4$ В, $A_3 = 1$В, $f_1 = 25$Гц, $f_2 = 70$ Гц, $f_3 = 190$Гц.

На рисунке 1 представлена структурная схема модели, разработанная в среде SimInTech, предназначенная для генерации трёх гармонических составляющих исследуемого полигармонического сигнала.

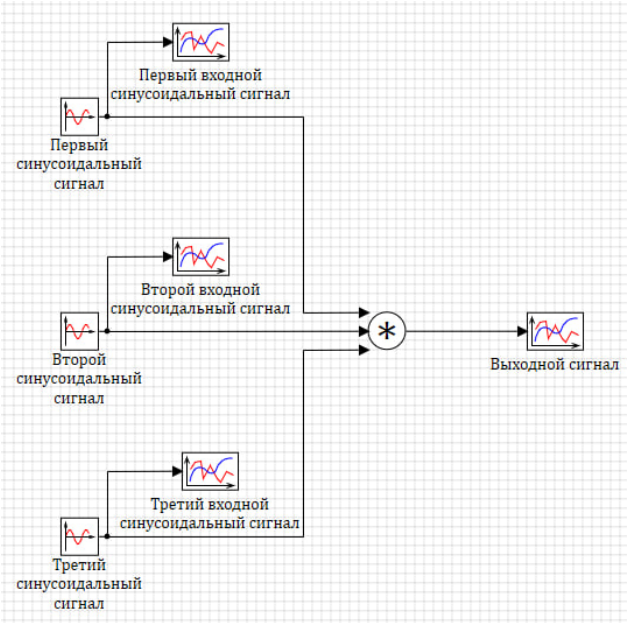


Рис. 1. Схема для формирования аналогового сигнала

Схема, представленная на рисунке 1 включает три идентичных по структуре канала, каждый из которых содержит блок-источник «Синусоида» [1], формирующий гармоническое колебание с индивидуальными параметрами частоты, амплитуды и начальной фазы, а также подключённый к его выходу блок «Временной график», предназначенный для поэтапного визуального представления формируемых сигналов. Затем выходные сигналы всех трёх источников алгебраически перемножаются с целью получения результирующего сигнала $s(t)$.

На выходе генераторов синусоидальные сигналы будут иметь вид в соответствии с рисунком 2.

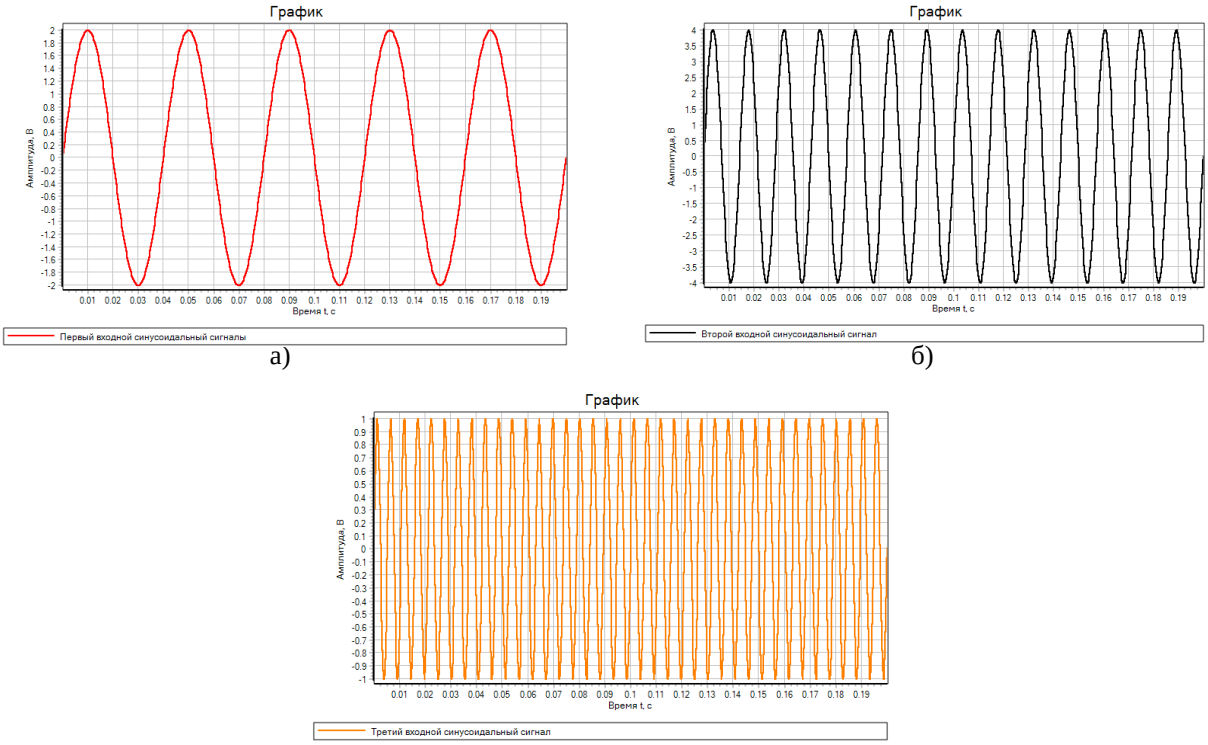


Рис. 2. Сигналы на выходе генератора: а) первый входной синусоидальный сигнал с $f_1 = 25$ Гц,
б) второй входной синусоидальный сигнал с $f_2 = 70$ Гц,
в) третий входной синусоидальный сигнал с $f_3 = 190$ Гц.

После перемножения получаем аналоговый сигнал, представленный на рисунке 3.

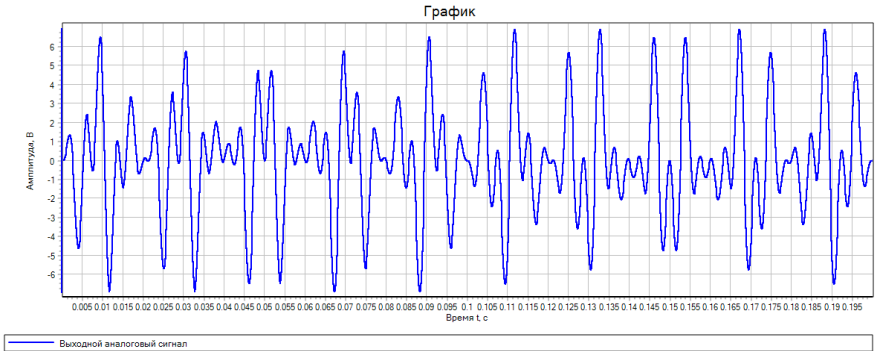


Рис. 3. Выходной аналоговой сигнал

В ходе экспериментального исследования было выполнено перемножение трёх гармонических сигналов с различными частотами. Анализ выходного аналогового сигнала подтверждает формирование сложного полигармонического колебания. Форма сигнала характеризуется многоуровневой амплитудной модуляцией, что обусловлено интерференцией комбинационных частот, возникающих в результате нелинейного преобразования. На осциллограмме отчетливо наблюдается сложная структура огибающей, которая не сводится к простым биениям, свойственным двухчастотному взаимодействию, а представляет собой результат суперпозиции нескольких низкочастотных составляющих.

Модель формирования дискретных сигналов

Теперь соберем модель формирования дискретных сигналов. Для этого в схему добавим блок генерации единичных импульсов и еще один перемножитель. Схема для формирования дискретного сигнала представлена на рисунке 4.

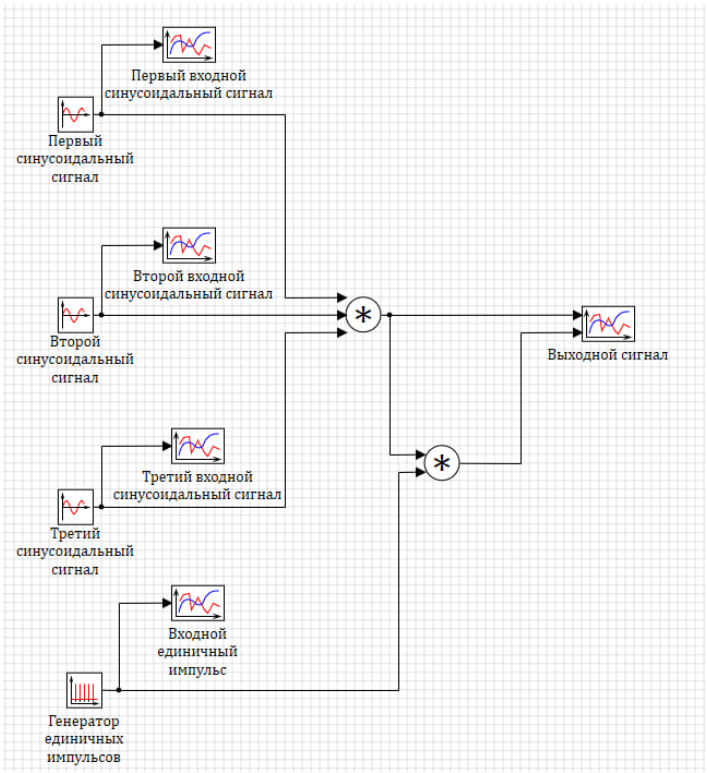


Рис. 4. Схема для формирования дискретного сигнала

Проанализируем влияние частоты дискретизации на точность восстановления исходного сигнала.

Зададим частоту дискретизации 285 Гц, которая точно совпадает с максимальной частотой спектра выходного сигнала, и на выходе получим следующий сигнал, представленный на рисунке 5:

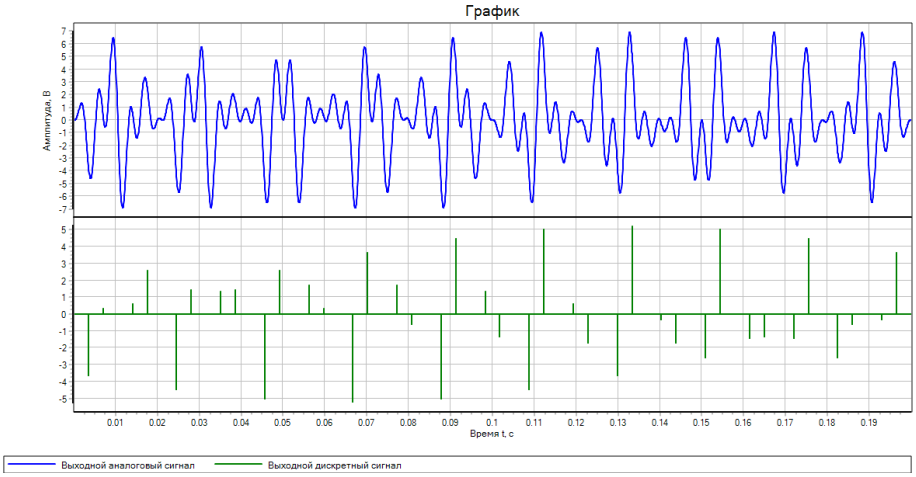


Рис. 5. Выходной аналоговый и дискретный сигналы при частоте дискретизации 285 Гц

Анализируя полученные графики, можно сделать вывод, что при использовании частоты дискретизации, равной максимальной частоте, в спектре сигнала точно восстановить исходный сигнал невозможно. Из-за того, что спектры сигналов накладываются друг на друга, на выход поступают лишь редкие импульсы, по которым можно проследить лишь отдалённые очертания формы входного сигнала.

Исходя из того, что в соответствии с теоремой Котельникова, частота дискретизации должна быть больше или равна удвоенной максимальной частоте спектра сигнала, зададим частоту дискретизации 615 Гц и на выходе получим сигнал, представленный на рисунке 6:

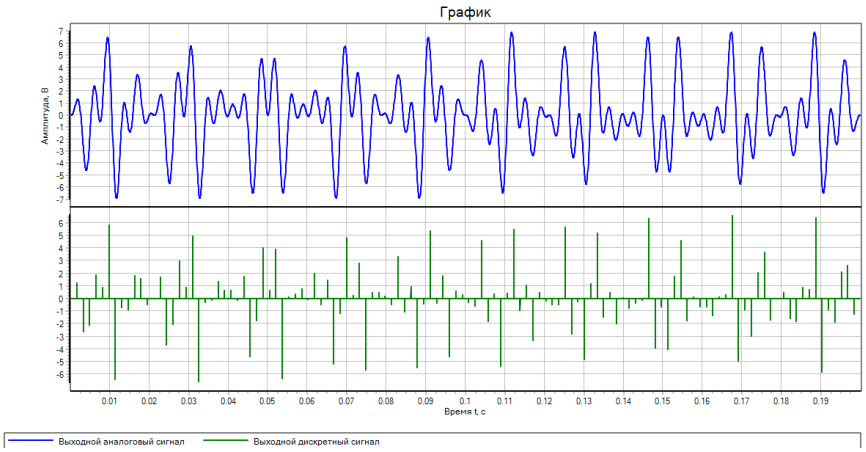


Рис. 6. Выходной аналоговый и дискретный сигналы при частоте дискретизации 615 Гц

Теперь выбор частоты дискретизации отвечает условию теоремы Котельникова. В таком случае, теоретически, сигнал может быть восстановлен без потерь, но на практике выбор режима, при котором частота дискретизации близка к граничной по условию, является неустойчивым и чувствительным к погрешностям радиотехнической аппаратуры. Рекомендуют частоту выбирать хотя бы в несколько раз выше максимальной в спектре [3].

Зададим частоту дискретизации 1230 Гц и на выходе получим следующий сигнал, представленный на рисунке 7:

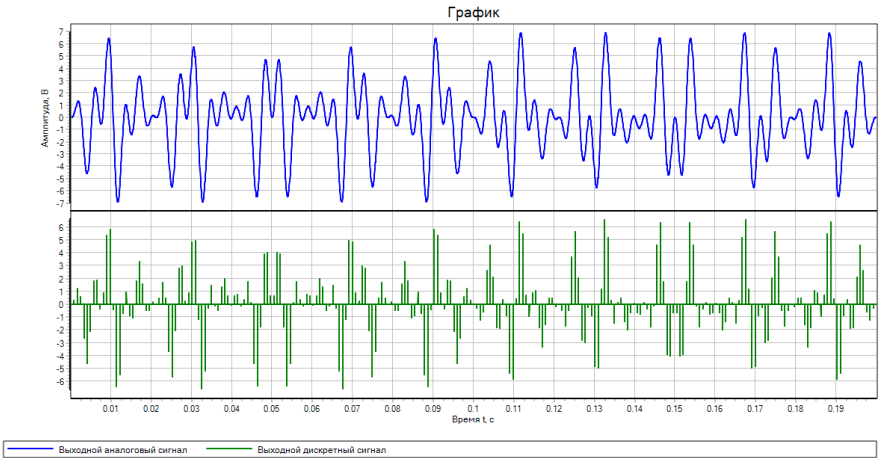


Рис. 7. Выходной аналоговый и дискретный сигналы при частоте дискретизации 1230 Гц

Выбор частоты дискретизации, в четыре раза превышающий максимальную частоту в спектре сигнала, обеспечивает точное выполнение условия теоремы Котельникова. Можно наглядно видеть, что с высокой вероятностью возможно восстановление входного сигнала и передать максимальное количество информации без потерь.

Подводя итоги, можно выделить, что с использованием функционала отечественной среды математического моделирования SimInTech получилось разработать модели формирования аналоговых и дискретных сигналов. Из имеющихся блоков сначала была собрана модель формирования аналоговых сигналов, а на промежуточном этапе добавлены блоки для визуализации трёх входных гармонических колебаний. В модель формирования дискретных сигналов дополнительно был добавлен блок из другой библиотеки, имеющейся в среде SimInTech, что позволило реализовать переход от непрерывного сигнала в его дискретное представление.

Анализ показал, что для высокого уровня восстановления исходного сигнала частоту дискретизации необходимо выбирать в несколько раз больше максимальной частоты в спектре. В нашем случае, высокий уровень сходства исходного и восстановленного сигналов удалось достичь при выставлении частоты дискретизации в чуть более чем 4 раза превышающей максимальную частоту в спектре. При таком выборе полностью отсутствует эффект наложения спектров.

Наличие подобных виртуальных моделей способствуют более наглядному и детальному изучению теоретических сведений в области радиотехнических цепей и сигналов, что, в свою очередь, повышает уровень приобретаемых компетенций обучающимися.

Библиографический список

1. Библиотеки блоков // Справочная система SimInTech URL: https://help.simintech.ru/#10_biblioteki_blokov/biblioteki_blokov.html (дата обращения: 28.01.2026).
2. Радиотехнические цепи и сигналы: методические указания к лабораторным работам. Часть I / Рязан. гос. радиотехн. ун-т; сост.: В.В. Авдеев, А.Ю. Линович, С.Л. Соколов, Б.И. Филимонов; под ред. Б.И. Филимонова. — Рязань, 2017. — 48 с.
3. Гоноровский И.С. Радиотехнические цепи и сигналы: Учебник для вузов. – 4-е изд., перераб. и доп. – М.: Радио и связь, 1986. – 512 с.

УДК 004.94; ГРНТИ 28.17.19

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРОЕКТИРОВАНИЯ КОМПОНЕНТОВ ТЕЛЕКОММУНИКАЦИОННЫХ УСТРОЙСТВ В РАЗЛИЧНЫХ СРЕДАХ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

А.С. Заря, В.А. Волченков
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, anton.zarya001@mail.ru

Аннотация. В рамках научно-исследовательской работы был создан полосовой вокодер в среде MATLAB/Simulink, охватывающий полный цикл обработки речевого сигнала – от анализа до синтеза. Основные усилия были направлены на оптимизацию параметров фильтрации и усовершенствование алгоритмов определения ключевых речевых характеристик. Было произведено построение детектора огибающей, детектора «тон-шум», а также реализация выделителя основного тона.
Ключевые слова: полосовой вокодер, речевой сигнал, полосовой фильтр, разделение спектра сигнала

INVESTIGATION OF THE POSSIBILITIES OF DESIGNING COMPONENTS OF TELECOMMUNICATION DEVICES IN VARIOUS MATHEMATICAL MODELING ENVIRONMENTS

A.S. Zarya, V.A. Volchenkov
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, anton.zarya001@mail.ru

The summary. As part of the research work, a band-pass vocoder was created in the MATLAB/Simulink environment, covering the full cycle of speech signal processing — from analysis to synthesis. The main efforts were aimed at optimizing filtering parameters and improving algorithms for determining key speech characteristics. The construction of a "tone-noise" detector, the calculation of the compression ratio, as well as the implementation of basic tone filtering were carried out.
Keywords: band-pass vocoder, speech signal, band-pass filter, signal spectrum separation.

В связи с ростом, развитием и увеличением объемов передаваемой речевой информации, в частности, со скорейшим внедрением систем связи пятого и шестого поколения (5G и 6G), усовершенствованием беспроводных сенсорных сетей и развитием Интернета вещей, возникает проблема эффективного кодирования и сжатия речевого сигнала. В настоящее время методы цифрового кодирования речи, основывающиеся на импульсно-кодовой модуляции (ИКМ), становятся малоэффективны и малорезультативны. Это связано в большей мере с тем, что условия ограничения пропускной способности каналов связи ужесточаются, а также возрастают энергопотребление и задержки. Поэтому на фоне вышеперечисленных проблем даже такие популярные кодеки речевых сигналов, как AMR (Adaptive Multi-Rate) или Opus, могут передавать речь с искажениями и «металлическим» призвуком.

В этой области интерес представляют полосовые вокодеры с параметрическими методами кодирования, позволяющие решать ряд проблем. В отличие от современных кодеков CELP, которые базируются на точном воспроизведении сигнала ошибки, полосовые вокодеры используют минимальный набор параметров, описывающих огибающую сигнала, частоту основного тона и характер звука (звонкий/глухой). Благодаря такому подходу полосовые вокодеры обеспечивают низкий битрейт (1,2–2,4 кбит/с). Однако ради достижения низкого битрейта приходится жертвовать разборчивостью речи и натуральностью звучания.

Создание, улучшение и внедрение полосовых вокодеров остается актуальной проблемой по ряду технических, экономических и социальных причин. Ниже приведены основные аргументы, доказывающие их значимость.

1. Эффективное кодирование речи при ограниченной пропускной способности. Полосовые вокодеры (bandwidth vocoders) позволяют передавать речь с очень низким битрейтом – от 1 до 8 кбит/с и даже ниже. Это особенно важно в условиях:

– спутниковой связи, где пропускная способность и энергопотребление критичны;

– военных и экстренных систем связи, где устойчивость канала важнее качества звука;

– развивающихся регионов с ограниченной телекоммуникационной инфраструктурой.

2. Устойчивость к шумам и потерям пакетов. Многие современные вокодеры (например, MELP, AMBE, Codec 2) используют параметрическое представление речи – описывают её через набор параметров (форманты, тональность, энергия и т.д.), а не через аудиоволну. Это делает их:

– менее чувствительными к шуму;

– более устойчивыми к потерям данных в сетях с низким качеством (VoIP, радиосвязь, IoT-устройства).

3. Интеграция с современными технологиями ИИ и машинного обучения. Современные вокодеры всё чаще используют глубокое обучение (например, WaveNet, LPCNet, Neural Vocoder). Однако даже классические полосовые вокодеры служат:

– базой для обучения нейросетей (например, для синтеза речи, voice conversion, TTS);

– инструментом для сжатия данных в голосовых ассистентах, где важно минимизировать задержку и объём передаваемых данных.

4. Приватность и безопасность. Поскольку вокодеры передают не исходный звук, а параметры, это:

– снижает риск идентификации личности по голосу (в определённых режимах);

– позволяет использовать криптографически защищённые каналы с минимальной нагрузкой;

– используется в защищённых военных и правительственных системах связи.

Вокодеры представляют собой устройства, осуществляющие параметрическое сжатие речевых сигналов. Компрессия речевых сигналов на передающей стороне производится в анализаторе, выделяющем из речевого сигнала медленно меняющиеся составляющие, которые передаются по каналу связи в виде кодовых посылок [1].

Вокодеры можно разделить на 2 класса:

1) речеэлементные (РЭ);
2) параметрические.

В речеэлементных вокодерах при передаче распознаются произнесенные элементы речи (например, фонемы) и передаются только их номера. На приеме эти элементы создаются по правилам речеобразования или берутся из памяти устройства. Область применения фонемных вокодеров – линии командной связи, речевое управление и говорящие автоматы информационно-справочной службы. Практически в таких вокодерах происходит автоматическое распознавание слуховых образов, а не определение параметров речи [1].

В параметрических вокодерах из речевого сигнала выделяют два типа параметров:

– параметры, характеризующие огибающую спектра речевого сигнала, (фильтровую функцию);

– параметры, характеризующие источник речевых колебаний (генераторную функцию), - частота основного тона, ее изменение во времени, моменты появления и исчезновения основного тона, шумового сигнала.

По этим параметрам на приеме синтезируют речь [1].

В полосных вокодерах спектр речи делится на 7-20 полос (каналов) аналоговыми или цифровыми полосовыми фильтрами. Большее число каналов в вокодере дает большую натуральность и разборчивость. С каждого полосового фильтра сигнал поступает на детектор и фильтр низких частот с частотой среза F_{CP}. Таким образом, сигналы на выходе каждого канала изменяются с частотой менее F_{CP}. Их передача возможна в аналоговом или цифровом виде [1].

На приемной стороне с помощью местных источников сигнала, управляемых принятыми параметрами, синтезируется речевой сигнал. Работа вокодера основана на моделировании человеческой речи с учетом ее характерных особенностей. При вычислении непосредственного изменения амплитуды сигнала вокодера получают параметры модели речеобразования для получения другого сигнала, максимально схожего с исходным. Таким образом осуществляется анализ для последующего синтеза речи [2].

Полосовой вокодер представляет собой совокупность двух основных частей – анализирующей (передающая сторона) и синтезирующей (приемная), которые содержат идентичные наборы (гребенки) полосовых фильтров, перекрывающих определенный частотный интервал. Структура полосового вокодера представлена на рисунке 1 [2].

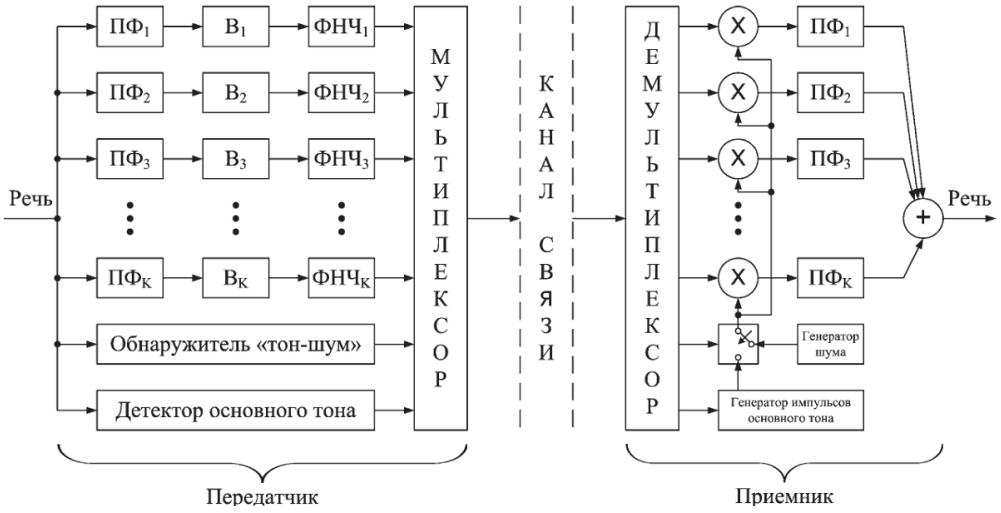


Рис. 1. Структурная схема полосового вокодера

Фильтры блока анализа обеспечивают тональное разделение спектра сигнала. Для перекрытия всей полосы звуковых частот, наряду с полосовыми, в гребенке можно использовать фильтры НЧ и ВЧ (в самых низкочастотном и высокочастотном каналах). Детектор и фильтр НЧ в каждом канале выделяют огибающую сигнала данного канала, и каждая из них характеризует энергию речевого спектра в соответствующей полосе частот для фрагмента речи (длина фрагмента 5-30 мс). Для более компактной передачи выходы каждого из каналов могут логарифмироваться и кодироваться с помощью дифференциальной импульсно-кодовой модуляции (ДИКМ). От числа частотных полос зависит разборчивость синтезированной речи. Хорошие результаты получаются при числе каналов 15-16 (полоса 100 Гц...4 кГц). Для улучшения качества восстановленной речи при выборе центральных частот и ширины полос пропускания канальных фильтров целесообразно использовать критические полосы слуха [2].

При выборе типа фильтров необходимо иметь в виду, что спектральные составляющие сигнала вблизи центральной частоты резонансных фильтров подвергаются существенным фазовым сдвигам, а это приводит к изменению тембра, даже если амплитудные соотношения сохранены. Причем при увеличении порядка фильтров фазовый сдвиг увеличивается, являясь причиной характерной для вокодера неестественности речи.

Практическое моделирование в среде MATLAB/Simulink

Исходные данные для расчета и дальнейшего моделирования:

– тип фильтр –: КИХ;

– длина кадра Т – 25 мс;

– уровень пропускания $\varepsilon_{1ДОП}$ – 0,75 дБ;

– уровень подавления $\varepsilon_{2ДОП}$ – 52 дБ;

– число частотных каналов I – 14;

– показатель прямоугольности АЧХ – 1,09;

– частота дискретизации $f_Д$ – 8 кГц;

– разрядность АЦП – n = 8 бит.

При выборе метода проектирования фильтра необходимо, чтобы соблюдались заданные параметры частотной избирательности с минимально возможным порядком. Проектирование будет осуществляться в Filter Designer – графическом пользовательском интерфейсе (GUI) в Signal Processing Toolbox. На рисунке 2 приведена АЧХ фильтра № 7, спроектиро-

ванного по методу Паркса-Мак-Клеллана с равноволновой аппроксимацией. Уровень неравномерности в полосе пропускания составляет 1,12 дБ, а в зоне непрозрачности 48,2 дБ. При этом порядок фильтра *N* равен 107.

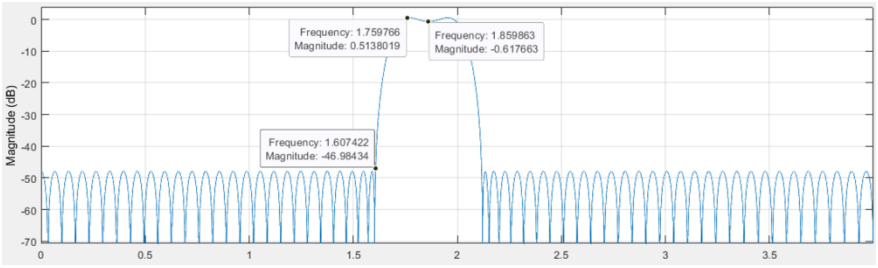


Рис. 2. АЧХ фильтра с порядком 107

Соберем детектор огибающей для первого полосового канала. Детектор состоит из полосового фильтра, выпрямителя и НЧ фильтра и приведен на рисунке 3. Выпрямитель осуществляется с помощью возведения в квадрат. Частота среза НЧ фильтра устанавливается в 10 раз меньше центральной частоты полосового фильтра. На рисунке 4 приведены диаграммы с выхода каждого блока детектора огибающей.

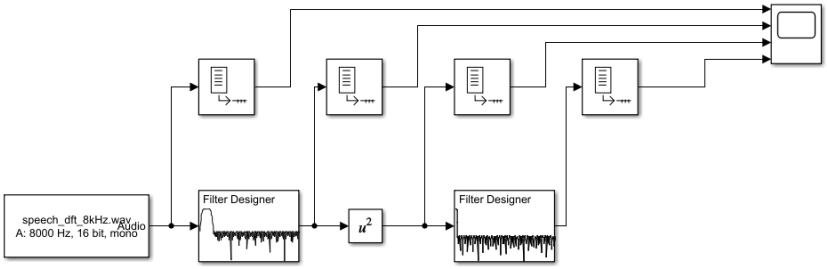


Рис. 3. Детектор огибающей

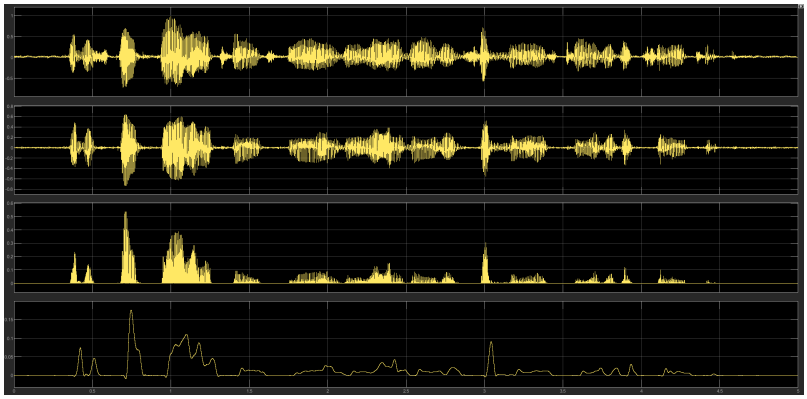


Рис. 4. Временные диаграммы с выхода каждого блока детектора первого канала

Полная схема полосового вокодера приведена на рисунке 5. Она содержит детектор огибающей, детектор «тон-шум», выделитель основного тона и ключ, который в зависимости от решения первого включает сигнал с выделителя основного тона либо с генератора шума. К схеме дополнительно в полосовых каналах добавляются блоки кодирования/декодирования. На рисунках 6 и 7 изображены результаты работы полосового канала передатчика и приемника соответственно, а на рисунке 8 изображен общий результат работы вокодера.

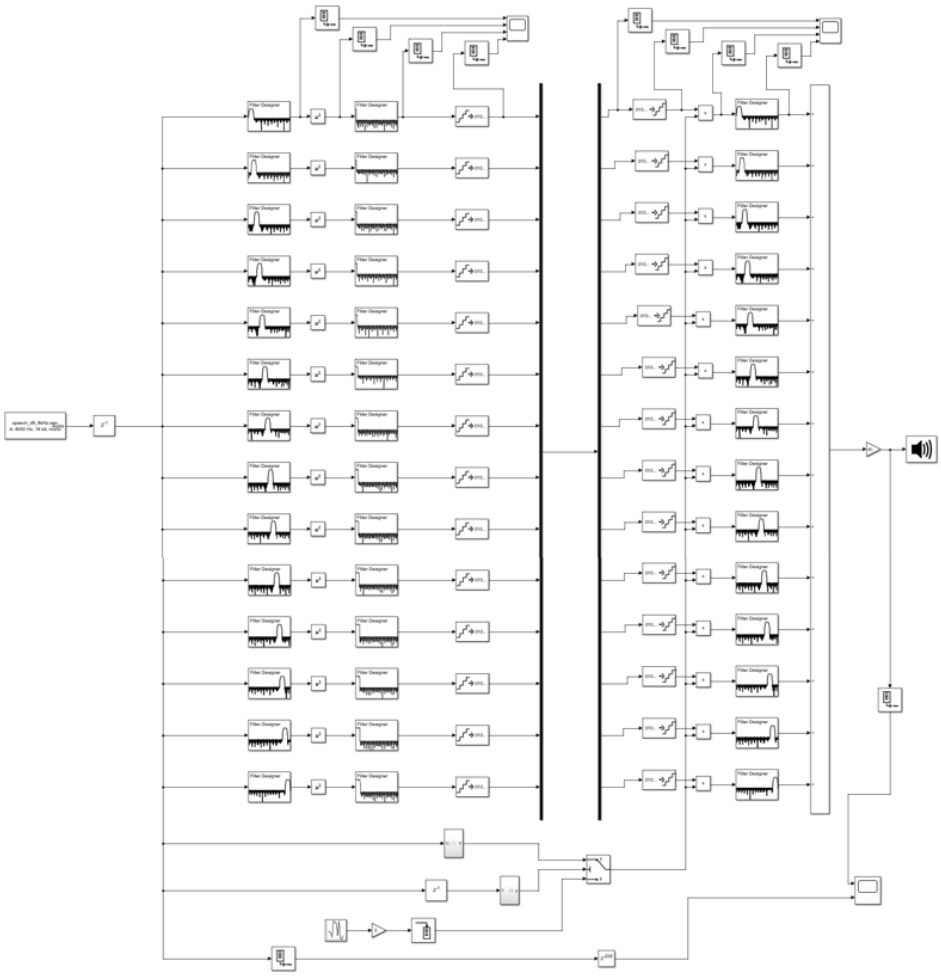


Рис. 5. Собранная полная схема полосового вокодера

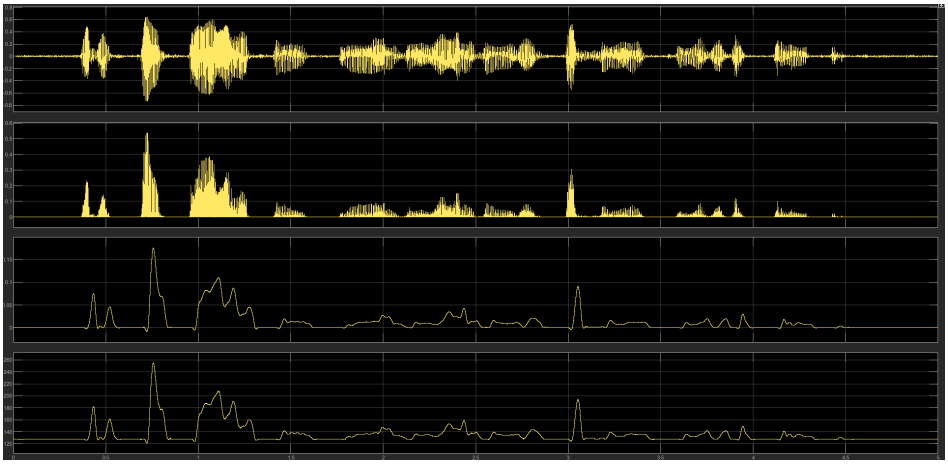


Рис. 6. Результат работы полосового канала передатчика

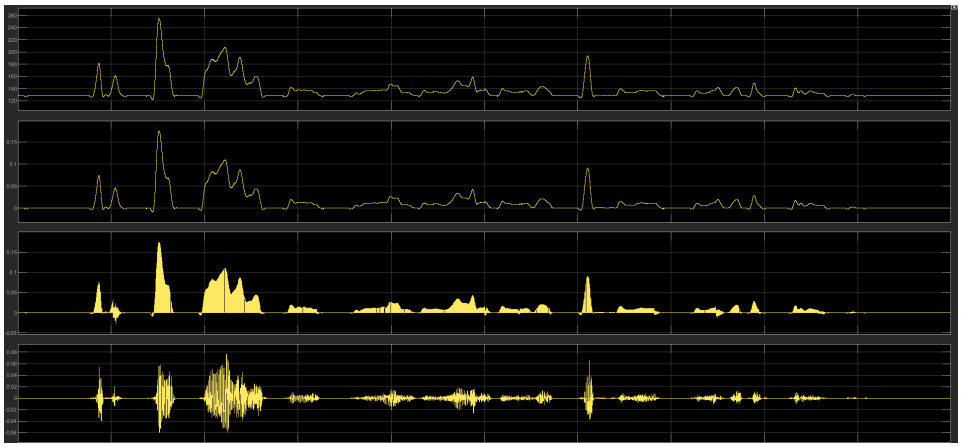


Рис. 7. Результат работы полосового канала приемника

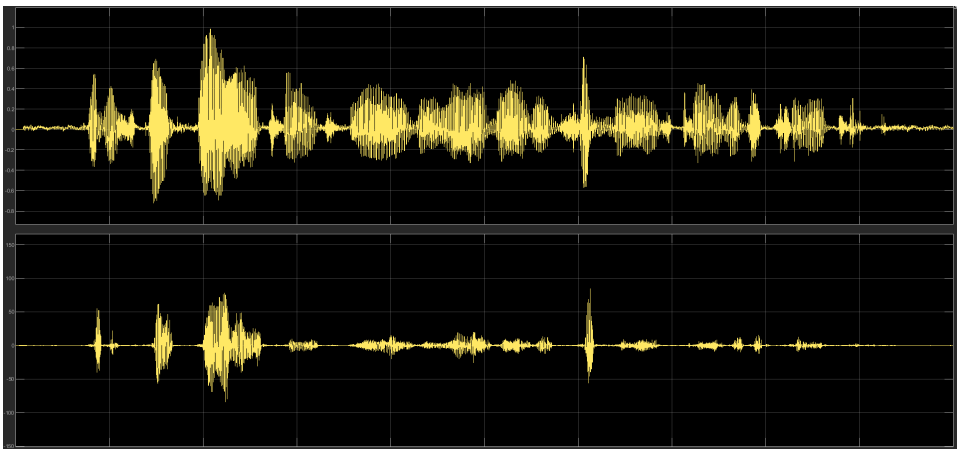


Рис. 8. Результат работы вокодера

Моделирование полосового вокодера показало, что восстановленный сигнал заметно отличается от исходного. Речь остается слышимой, но разобрать слова становится трудно. Это связано с тем, что в каждом частотном канале сигнал сильно сжимается, из-за чего теряются мелкие временные детали, важные для понимания речи.

Вывод

В ходе выполнения работы были систематизированы теоретические знания о принципах функционирования полосовых вокодеров. Разработанная в среде MATLAB/Simulink имитационная модель подтвердила базовые принципы работы устройства: результирующий речевой сигнал характеризуется наличием искажений спектра, однако сохраняет удовлетворительную разборчивость, что является характерным компромиссом для данного класса систем анализа-синтеза речи.

Библиографический список

1. Разработка полосового вокодера на основе модификации алгоритма Хургина – Яковлева [Электронный ресурс] // - URL: https://cyberleninka.ru/article/n/razrabotka-polosovogo-vokodera-na-osnove-modifikatsii-algoritma-hurgina-yakovleva/viewer

2. Устройства преобразования и обработки информации в системах подвижной радиосвязи: методические указания к курсовой работе / сост. В.А. Волченков; Рязан. гос. радиотехн. ун-т. — Рязань, 2021. 40 с. С. 2.

3. Полосное кодирование. Вокодеры [Электронный ресурс] // - URL: https://studfile.net/preview/4330340/page:4/

4. Что такое вокодер и липредер? [Электронный ресурс] // - URL: http://www.bnti.ru/showart.asp?aid=720&lvl=01.02.09.

УДК 004.934; ГРНТИ 28.23.37

ОБЗОР И АНАЛИЗ СПОСОБОВ РАСПОЗНАВАНИЯ РЕЧЕВЫХ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕЙ

Д.С. Королев, В.А. Волченков

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, dmit.korolev2016@yandex.ru

Аннотация. В работе рассматриваются современные методы распознавания речевых сигналов на основе нейросетевых технологий. Проведен анализ этапов обработки речевого сигнала, особенностей обучения моделей автоматического распознавания речи и проблемы дикторонезависимости. Представлен сравнительный анализ классических статистических методов HMM и современных нейросетевых архитектур, включая рекуррентные, сверточные и трансформерные модели. Рассмотрены архитектуры Deep Speech, Wav2Letter, wav2vec 2.0, Transformer, Conformer и Whisper. Выявлены их преимущества и ограничения с точки зрения точности, вычислительной сложности и устойчивости к шумам. Сделан вывод о том, что наиболее перспективными являются end-to-end и архитектуры, обучающиеся на неразмеченных данных, обеспечивающие высокое качество распознавания при масштабировании на большие объемы данных.

Ключевые слова: распознавание речи, нейронные сети, дикторонезависимость, Transformer, Conformer, wav2vec, Whisper, обработка сигналов.

OVERVIEW AND ANALYSYS OF METHODS FOR RECOGNIZING SPEECH SIGNALS USING NEURAL NETWORKS

D.S. Korolev, V.A. Volchenkov

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, dmit.korolev2016@yandex.ru

The summary. The paper discusses modern methods of speech signal recognition based on neural network technologies. It analyzes the stages of speech signal processing, the features of training automatic speech recognition models, and the problem of dictation independence. The paper presents a comparative analysis of classical statistical methods HMM and modern neural network architectures, including recurrent, convolutional, and transformer models. The paper discusses the architectures of Deep Speech, Wav2Letter, wav2vec 2.0, Transformer, Conformer, and Whisper. Their advantages and limitations in terms of accuracy, computational complexity, and noise resistance have been identified. It has been concluded that end-to-end and unsupervised learning architectures are the most promising, providing high-quality recognition while scaling to large datasets.

Keywords: speech recognition, neural networks, speaker independence, Transformer, Conformer, wav2vec, Whisper, signal processing.

Автоматическое распознавание речи является одной из ключевых задач современной цифровой обработки сигналов и искусственного интеллекта. Речь представляет собой естественный и наиболее удобный способ коммуникации человека, поэтому создание эффективных систем автоматического преобразования речевого сигнала в текст имеет важное практическое значение. Подобные технологии активно применяются в голосовых ассистентах, системах транскрибирования аудио- и видеоматериалов, интеллектуальных информационных системах, колл-центрах, системах управления «умным домом» и средствах повышения доступности информации для людей с ограниченными возможностями.

Речевой сигнал отличается высокой вариативностью и нестационарностью. Его характеристики изменяются во времени и зависят от множества факторов: индивидуальных особенностей диктора, темпа речи, фонетического состава высказывания, условий записи и наличия шумов. Эти особенности существенно усложняют задачу построения универсальной модели распознавания.

Особенности обработки речевого сигнала

Современные системы распознавания речи реализуют многоуровневую схему обработки сигнала. На первом этапе осуществляется предварительная фильтрация и подавление шумов, частотный спектр которых выходит за пределы диапазона человеческой речи. Затем сигнал разбивается на короткие временные фреймы, из которых извлекаются информативные акустические признаки, например мел-частотные кепстральные коэффициенты или логмел спектрограммы.

Далее происходит последовательный анализ фонем, морфем и слов, после чего формируется итоговая текстовая гипотеза. Общая схема анализа и обработки речи представлена на рисунке 1 [1].

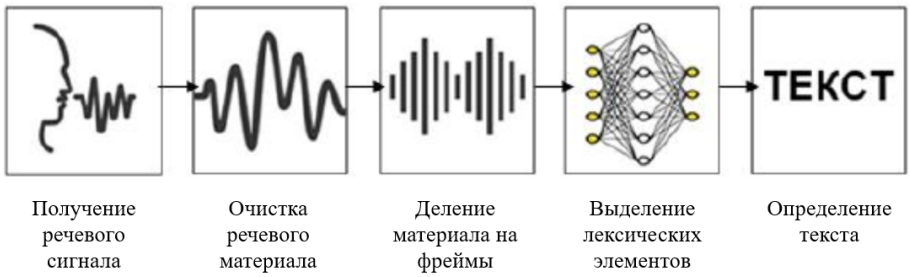


Рис. 2. Схема анализа и обработки речи

Одной из наиболее сложных задач является обеспечение дикторонезависимости системы [2], то есть способности корректно распознавать речь различных пользователей без предварительной настройки под конкретного человека. Для решения этой проблемы используются крупные и разнообразные обучающие датасеты, включающие записи множества дикторов с различными темпами, акцентами и условиями записи. Пример организации баз данных для дикторонезависимого распознавания представлен на рисунке 2 [3].

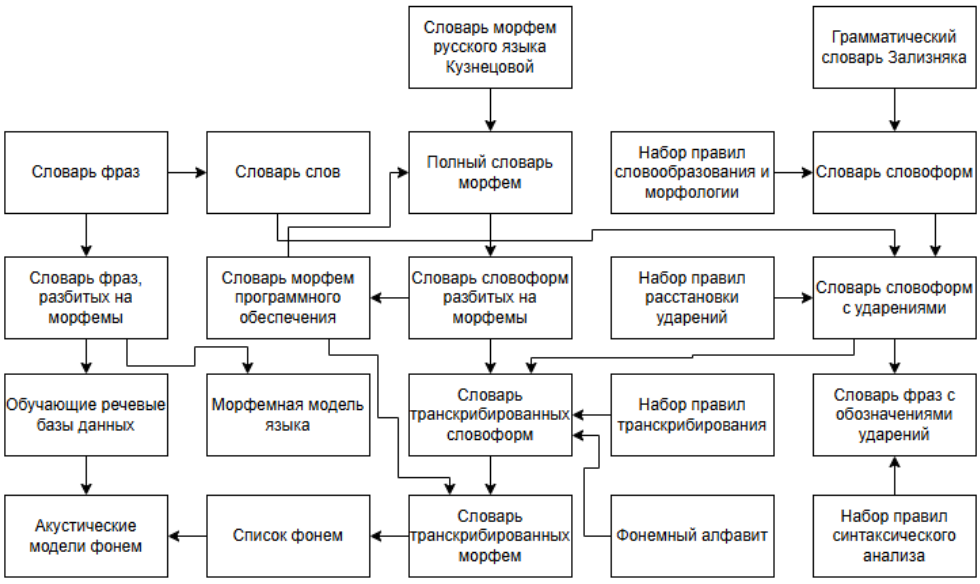


Рис. 3. Базы данных модели SIRIUS для распознавания русской речи

Классические методы распознавания речи

До широкого распространения нейросетевых методов стандартом в области распознавания речи являлись скрытые марковские модели HMM. Эти методы основываются на вероятностном описании переходов между скрытыми акустическими состояниями и генерации наблюдаемых признаков.

Архитектура такой системы представлена на рисунке 3.

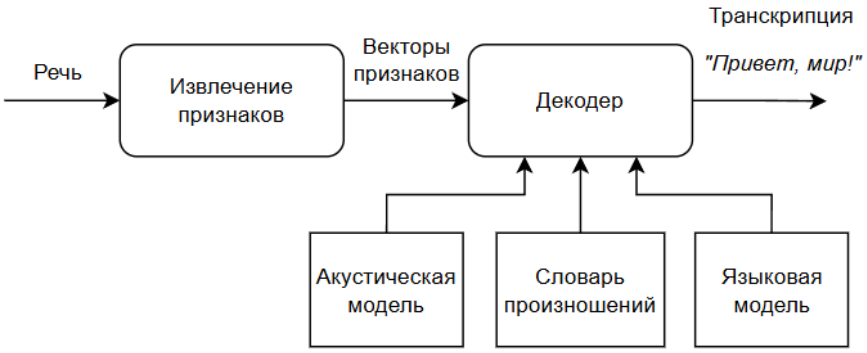


Рис. 4. Архитектура модели на базе HMM

Данные методы обладают строгим математическим аппаратом и интерпретируемостью, однако имеют существенные ограничения. Они требуют предварительного извлечения признаков, слабо моделируют нелинейные зависимости и демонстрируют ограниченную устойчивость к шумам и вариативности речи.

Рекуррентные нейронные сети и архитектура Deep Speech

Существенный прогресс в области распознавания речи связан с применением глубоких нейронных сетей. Одним из первых успешных end-to-end решений стала архитектура Deep Speech, основанная на рекуррентных нейронных сетях. В данной модели используется механизм рекуррентных связей, обеспечивающий учет временного контекста. Структура рекуррентной сети в системе Deep Speech показана на рисунке 4 [4].

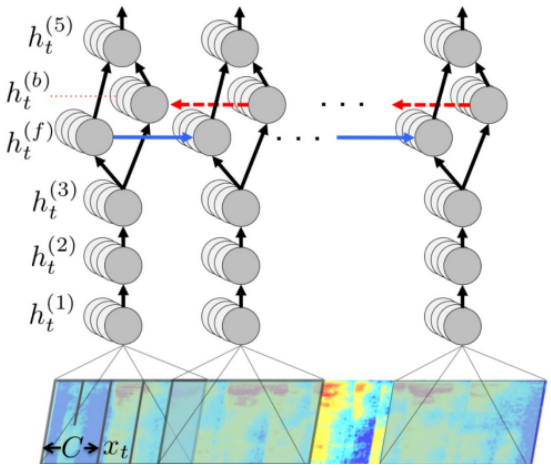


Рис. 5. Структура RNN в Deep Speech

Рекуррентные сети позволяют учитывать длительные временные зависимости, что особенно важно при обработке речевых последовательностей. Однако их обучение требует

значительных вычислительных ресурсов, а последовательная природа обработки ограничивает возможности параллелизации.

Сверточные нейронные сети и архитектура Wav2Letter

Сверточные нейронные сети рассматривают спектрограмму как двумерное представление сигнала и извлекают локальные временно-частотные признаки. Примером такого подхода является архитектура Wav2Letter, представленная на рисунке 5 [5].

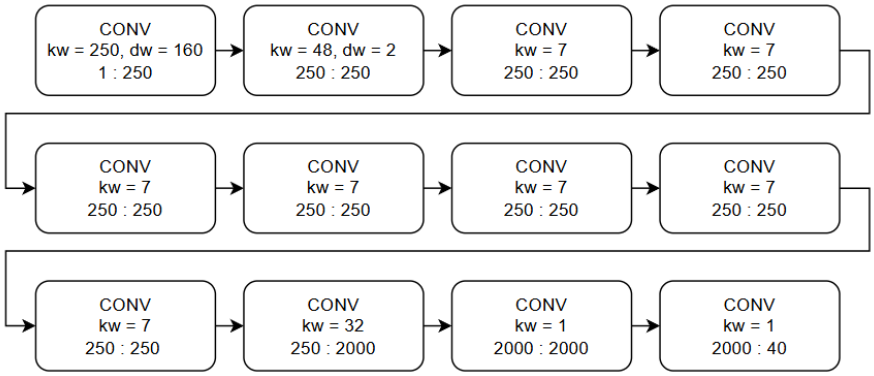


Рис. 5. Архитектура Wav2Letter

Преимуществом сверточных моделей является высокая скорость обучения и эффективная параллельная обработка данных. Они демонстрируют стабильность обучения и лучше масштабируются по сравнению с рекуррентными сетями.

Обучение на неразмеченных данных: Wav2Vec

Значительный шаг вперед связан с появлением “неразмеченных” моделей, таких как wav2vec 2.0. Данная архитектура предварительно обучается на больших объемах неразмеченных аудиоданных, что позволяет формировать информативные представления сигнала без использования текстовых транскрипций.

Архитектура модели представлена на рисунке 6.

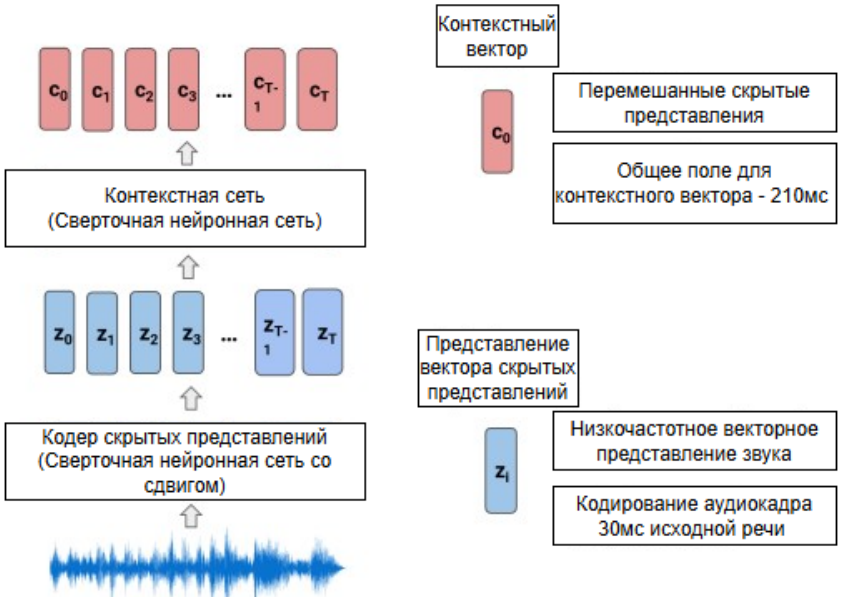


Рис. 6. Архитектура Wav2Vec

После этапа предварительного обучения модель обучается на размеченных данных. Такой подход существенно снижает требования к объему размеченных корпусов и повышает качество распознавания.

Transformer и Conformer

Архитектура Transformer основана на механизме самовнимания, который позволяет учитывать зависимости между любыми элементами последовательности независимо от их расстояния. Это обеспечивает эффективное моделирование долгосрочного контекста.

Общая схема Transformer приведена на рисунке 7 [6].

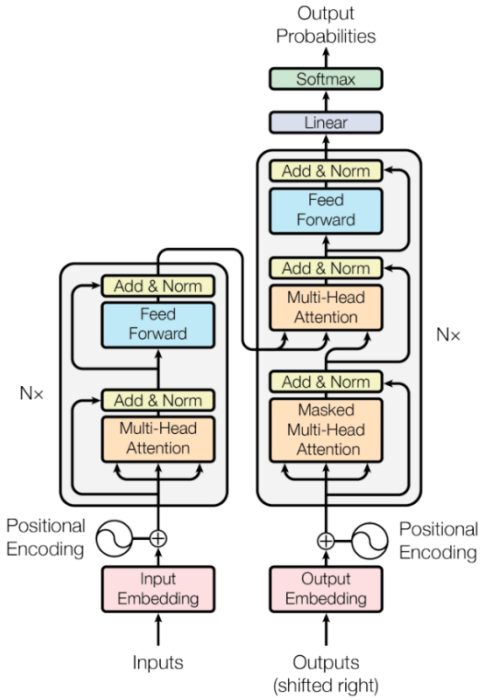


Рис. 7. Архитектура кодер Transformer

Однако для более эффективного учета локальных акустических особенностей была разработана архитектура Conformer, сочетающая механизмы внимания и сверточные операции. Структура кодера Conformer представлена на рисунке 8 [7].

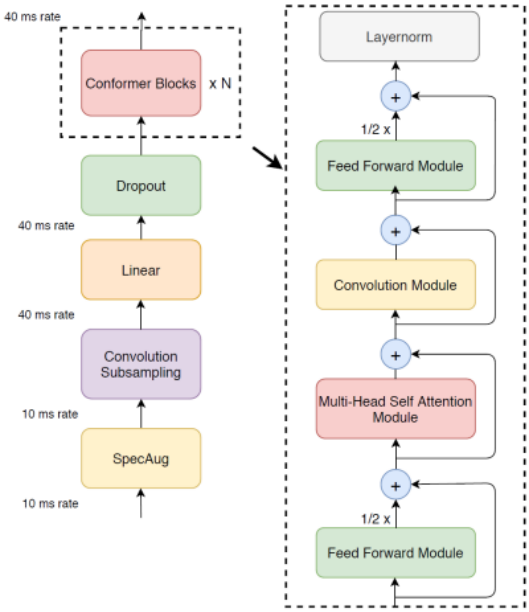


Рис. 8. Архитектура кодера Conformer

Conformer объединяет преимущества глобального контекстного моделирования и локального анализа спектральных признаков, что делает его одной из наиболее эффективных архитектур в современных системах распознавания речи.

Крупные многоязычные модели: Whisper

Одной из наиболее универсальных современных моделей является Whisper. Она построена по архитектуре «кодер–декодер» на основе Transformer и обучена на чрезвычайно большом объеме аудиоданных.

Архитектура модели представлена на рисунке 9 [8].

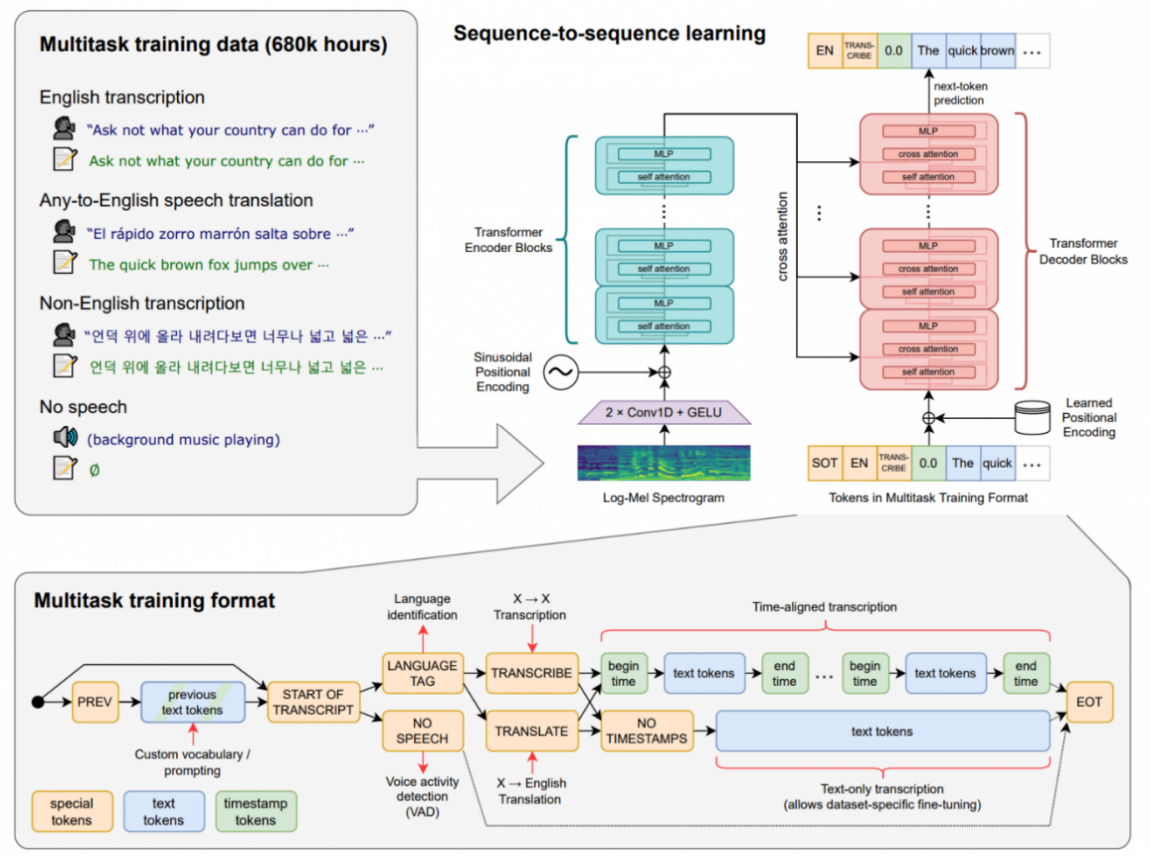


Рис. 9. Архитектура Whisper

Whisper поддерживает множество языков, демонстрирует устойчивость к шумам и способна работать в режиме zero-shot без дополнительного обучения. Основным ограничением является высокая вычислительная сложность, что затрудняет использование модели во встраиваемых системах.

Выводы

Распознавание речевых сигналов представляет собой сложную задачу цифровой обработки сигналов, поскольку речь характеризуется высокой вариативностью и зависит от множества факторов, таких как особенности диктора, темп речи и условия записи. Это требует применения эффективных методов обработки и обучения моделей, способных работать с различными типами данных и обеспечивать устойчивость к шумам.

Проведённый анализ показал, что классические методы, основанные на скрытых марковских моделях, обладают рядом ограничений и постепенно уступают место современным нейросетевым подходам. Использование рекуррентных, сверточных и архитектур трансформеров позволяет более точно учитывать временные зависимости, эффективно обрабатывать большие объёмы данных и повышать качество распознавания речи.

Наиболее перспективными являются end-to-end модели и архитектуры, использующие предварительное обучение на больших массивах неразмеченных данных. Такие подходы позволяют улучшить точность распознавания, повысить устойчивость систем к различным условиям и обеспечить их дальнейшее развитие и масштабирование.

Библиографический список

1. Ахметшин А.Ф. “Применение нейросетевых технологий для анализа речевой информации” / Электрон. научн. журн. КиберЛенинка. – 2020. – https://cyberleninka.ru/article/n/primenenie-neyrosetevyh-tehnologiy-dlya-analiza-rechevoy-informatsii
2. В.В. Дубровский, А.И. Егоров “О проблеме дикторонезависимости при распознавании речи на фонемном уровне”. – 5 с.
3. А.А. Карпов, А.Л. Ронжин, И.В. Ли “SIRIUS – Система дикторонезависимого распознавания слитной русской речи”, – 10 с.
4. Ханнун А., Кейс К., Каспер Дж., Катанзаро Б., Диамос Г., Элсен Э., Пренгер Р., Сатхииш С., Сенгупта Ш., Коатс А., Нг Э. Ю. Deep Speech: Scaling up end to end speech recognition – https://arxiv.org/abs/1412.5567
5. Ronan Collobert, Christian Puhrsch, Gabriel Synnaeve “WAV2LETTER: AN END-TO-END CONVNET-BASED SPEECH RECOGNITION SYSTEM”, 2017. – 9 с.
6. Рябинин М. “Трансформеры” / Учебник по машинному обучению: Yandex Education. – https://education.yandex.ru/handbook/ml/article/transformery
7. Gulati A., Qin J., Chiu C.-C., Parmar N., Zhang Y., Yu J., Han W., Wang S., Zhang Z., Wu Y., Wu Y., Pang R. Conformer: Convolution augmented Transformer for Speech Recognition / arXiv preprint. – 2020. – arXiv:2005.08100. – https://arxiv.org/pdf/2005.08100.pdf
8. Радфорд А., Ким Дж. В., Сю Т., Брокман Г., Макливей К., Сутскевер И. Robust Speech Recognition via Large-Scale Weak Supervision – https://arxiv.org/pdf/2212.04356

УДК 004.383.5; ГРНТИ 28.23.37

ОЦЕНКА ВЫЧИСЛИТЕЛЬНОЙ ЭФФЕКТИВНОСТИ ГРАФИЧЕСКОГО ПРОЦЕССОРА В РЕАЛИЗАЦИИ ОБУЧЕННОЙ НЕЙРОСЕТИ ПРИ АНАЛИЗЕ GPR-ИЗОБРАЖЕНИЙ

М.О. Филимонова, С.В. Витязев

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, maryrsl777@yandex.ru, vityazev.s.v@tor.rsreu.ru

Аннотация. Рассматривается проблема реализации нейросетевых алгоритмов на встраиваемых системах в условиях жёстких ограничений по времени обработки. Цель работы — анализ вычислительной эффективности графического процессора (GPU) и технологии CUDA при решении задачи бинарной классификации GPR-изображений. Описаны основные математические операции на этапе применения обученной модели двухслойной нейросети и аппаратные особенности GPU. Приведены результаты эксперимента в среде MATLAB на видеокарте NVIDIA GeForce GTX 1050 Ti. Показана связь между структурой нейросети, архитектурой процессора и временем выполнения. Сделаны выводы о достаточности производительности GPU среднего класса для практических задач анализа георадарных данных без потери точности классификации.

Ключевые слова: графический процессор (GPU); CUDA; нейронная сеть; георадар (GPR); обработка изображений; цифровая обработка сигналов; MATLAB; вычислительная эффективность; параллельные вычисления.

EVALUATION OF THE COMPUTATIONAL EFFICIENCY OF A GPU IN THE IMPLEMENTATION OF A TRAINED NEURAL NETWORK IN THE ANALYSIS OF GPR-IMAGES

M.O. Filimonova, S.V. Vityazev

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, maryrsl777@yndex.ru, vityazev.s.v@tor.rsreu.ru

The summary. The problem of implementing neural network algorithms on embedded systems in conditions of severe processing time constraints is considered. The purpose of the work is to analyze the computational efficiency of a graphics processor (GPU) and CUDA technology in solving the problem of binary classification of GPR images. The main mathematical operations of the two-layer neural network inference and GPU hardware features are described. The results of an experiment in the MATLAB environment on an NVIDIA GeForce GTX 1050 Ti graphics card are presented. The relationship between the neural network structure, processor architecture, and execu-

tion time is shown. Conclusions are drawn about the sufficiency of the GPU performance of the middle class for practical tasks of analyzing GPR data without loss of classification accuracy.
Keywords: graphics processing unit (GPU); CUDA; neural network; ground penetrating radar (GPR); image processing; digital signal processing; MATLAB; computational efficiency; parallel computing.

Введение

В современных системах цифровой обработки сигналов (ЦОС) всё чаще применяются методы машинного обучения, в частности, нейронные сети, для решения задач классификации, детектирования и распознавания образов в сигналах и изображениях. Однако внедрение таких алгоритмов во встраиваемые системы обработки сталкивается с проблемой ограниченных вычислительных ресурсов и жестких требований к времени обработки.

Традиционные CPU (Central Processing Unit) плохо приспособлены для массовых параллельных вычислений, характерных для нейросетей. Альтернативой выступают GPU (Graphics Processing Unit), способные выполнять тысячи операций одновременно.

Постановка задачи

Цель данной работы – проанализировать вычислительную эффективность GPU и технологии CUDA (Compute Unified Device Architecture) при решении типовой задачи нейросетевой классификации GPR-изображений (рис. 1), выявить узкие места и определить пути повышения производительности. GPR-изображения (радарограммы) представляют собой результаты георадиолокационного зондирования, где по горизонтали отложено положение антенны, а по вертикали — время прихода отраженного сигнала (глубина).

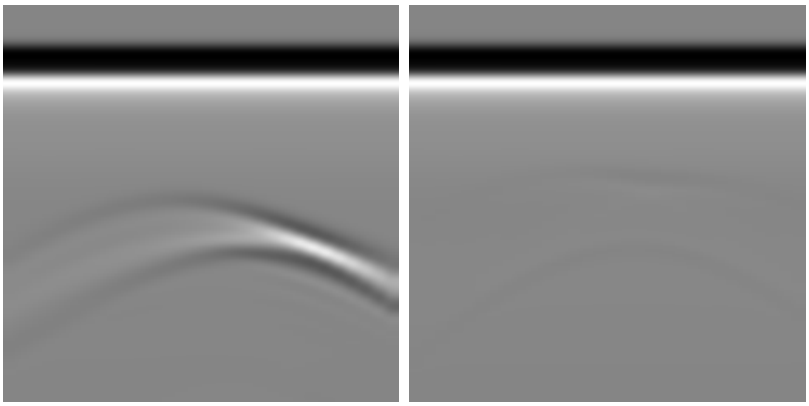


Рис. 1. Примеры GPR-изображений с объектом и без

Основные математические операции

Любая обученная нейросеть на этапе применения (инференс, inference) сводится к последовательности математических операций над входными данными [1]. В контексте данной работы используется двухслойная модель, которая после обучения выполняет нижеперечисленные действия.

1. Умножение матриц. Это основная операция. Входной вектор признаков умножается на матрицу весов скрытого слоя. Эта операция требует большого количества операций умножения и сложения с плавающей точкой.

2. Функция активации. В данной работе используется Leaky ReLU:

$$f(x) = \max(x, \alpha x) \quad (1)$$

3. Сигмоида. Для финальной бинарной классификации применяется сигмоида, преобразующая выход в диапазон от 0 до 1:

$$\sigma(x) = \frac{1}{1+e^{-x}}. \quad (2)$$

4. Сравнение с порогом. Логическая операция, формирующая итоговый бинарный ответ.

Таким образом, функционирование нейросети сводится к комбинации двух типов операций: ресурсоёмких матричных умножений и менее затратных поэлементных преобразований.

Аппаратная база

Для выполнения описанных операций существуют разные классы микропроцессоров.

• CPU (Central Processing Unit): оптимизирован для последовательных вычислений с минимальными задержками. Имеет мало ядер, но развитую иерархию кэш-памяти и сложный блок управления, что обеспечивает низкую задержку при обработке одного потока команд.

• DSP (Digital Signal Processor): оптимизирован для типовых задач ЦОС (БПФ, фильтрация). Эффективное использование DSP может потребовать трудоёмкой оптимизации кода с учётом его архитектурных особенностей.

• GPU (Graphics Processing Unit): изначально создан для параллельной обработки пикселей. Архитектура GPU подразумевает сотни простых ядер, объединенных в потоковые мультипроцессоры (Streaming Multiprocessor, SM). Это делает его идеальным для матричных операций.

CUDA (Compute Unified Device Architecture) – это программно-аппаратная архитектура от NVIDIA, позволяющая использовать GPU для общих вычислений. Она предоставляет абстракции ("решётки", "блоки", "нити") для распараллеливания кода. В контексте данной работы CUDA используется неявно через MATLAB, который транслирует команды в ядра CUDA. GPU выступает в роли ускорителя – "сопроцессора", выполняющего матричные вычисления.

Задача анализа GPR-изображений

Георадар (Ground-penetrating Radar, GPR) формирует изображения (радарограммы), где каждый столбец – это отражённый сигнал (трасса), а строка – глубина (или время прихода). Анализ таких изображений требует обнаружения характерных гиперболических образов (паттернов, patterns), указывающих на наличие объекта [2].

В рамках эксперимента входными данными являются фрагменты GPR-изображений, развернутые в векторы размерностью 65536 (256x256) пикселей. Задача нейросети – бинарная классификация – есть объект на изображении (класс 1) или нет (класс 0).

Описание эксперимента

Для оценки производительности GPU при решении задачи классификации GPR-изображений был проведен эксперимент в среде MATLAB. В качестве аппаратной платформы использовался графический процессор NVIDIA GeForce GTX 1050 Ti.

Входные данные для эксперимента представляли собой тестовую выборку *testData*, организованную в виде матрицы. Первые 65536 столбцов этой матрицы содержали значения пикселей GPR-изображений, развернутых в одномерные векторы, а последний, 65537-й столбец, хранил истинные метки классов. Для выполнения инференса использовались предварительно обученные веса: матрица WH для скрытого слоя и матрица WO для выходного слоя.

Программная реализация была построена таким образом, чтобы максимально задействовать вычислительный потенциал GPU. На первом этапе все массивы данных и весов бы-

ли приведены к формату single (рис. 2), что позволило сократить объем памяти, занимаемый числами с плавающей точкой, без существенной потери точности классификации.

```
testData = single(testData);
WH = single(WH);
WO = single(WO);
```

Рис. 2. Конвертация в single для ускорения на GPU

Затем с помощью функции *gpuArray* эти массивы были перенесены из оперативной памяти компьютера в видеопамять GPU (рис.3). Далее запускался таймер *tic*, после чего выполнялся сам инференс (рис. 4).

```
%Перенос всех данных на GPU
X_gpu = gpuArray(testData(:, 1:65536));
% Перенос весов на GPU
WH_weights_gpu = gpuArray(WH(:, 1:65536));
WH_bias_gpu = gpuArray(WH(:, 65537));
WO_gpu = gpuArray(WO);
```

Рис. 3. Перенос массивов на GPU

```
% Прямое распространение
hidden = max(X_gpu * WH_weights_gpu' + WH_bias_gpu', alpha * (X_gpu * WH_weights_gpu' + WH_bias_gpu'));

% Выходной слой с сигмоидой
output = 1 ./ (1 + exp(-[hidden, ones(numImages, 1, 'gpuArray')] * WO_gpu'));
```

Рис. 4. Инференс

Ключевой особенностью реализации являлось использование векторизованных операций: вместо обработки изображений по одному в цикле, все вычисления производились сразу над всем пакетом данных. Такой подход позволяет эффективнее загрузить GPU по двум причинам. Во-первых, запуск ядер CUDA имеет фиксированные накладные расходы, обработка одного пакета требует лишь одного запуска. Во-вторых, при обработке одного изображения объем вычислений может оказаться недостаточным для полной загрузки всех потоковых мультипроцессоров (SM). После завершения вычислений результирующий массив предсказаний извлекался обратно в оперативную память командой *gather*, а таймер останавливался, фиксируя общее время обработки. Минимальное зафиксированное время выполнения полного цикла обработки тестового набора изображений составило 0,3644 секунды.

Связь времени обработки, структуры нейросети и архитектуры процессора

Чтобы понять, как именно сложилось полученное время 0,3644 секунды, необходимо разобрать вычислительную сложность алгоритма и сопоставить её с архитектурными особенностями GTX 1050 Ti.

Используемая нейросеть в режиме инференса выполняет два основных этапа. Первый и самый ресурсоемкий этап – это работа скрытого слоя. Берётся матрица, содержащая исходные данные – в ней N строк (каждая соответствует одному изображению) и 65536 столбцов. Эта матрица умножается на транспонированную матрицу весов WH (у нее H строк, где H – число нейронов в скрытом слое, и 65536 столбцов). Для этой операции нам требуется

примерно N * 65536 * H операций умножения и сложения с плавающей точкой. Если подставить наши значения (N = 143, H = 200), получается около 1,87 миллиарда таких операций.

Графический процессор GTX 1050 Ti располагает 768 ядрами CUDA, работающими на частоте 1,3 ГГц. Теоретически это даёт ему возможность обрабатывать около 10^{12} операций в секунду. Исходя из этого, чистое время на матричное умножение (исключая любые задержки с памятью) заняло бы примерно 0,00187 секунды.

Второй этап – выходной слой, состоящий из одного нейрона с сигмоидой, его вклад в общее время значительно меньше.

Однако экспериментально полученное время (0,3644 с) более чем на два порядка превышает теоретическую оценку, поскольку дело не только в вычислительной мощи ядер GPU. Огромную роль играют задержки при доступе к основной памяти видеокарты, накладные расходы на запуск самих вычислений, а также необходимость постоянно пересылать данные туда-сюда между разными уровнями её памяти.

Проще говоря, даже при наличии 768 ядер CUDA на GTX 1050 Ti, которые, казалось бы, должны позволять выполнить до 768 операций умножения и сложения с плавающей точкой за такт, достичь этой пиковой производительности на практике мешает множество нюансов, связанных с устройством памяти и самой организацией вычислений. Когда мы запускаем умножение матриц в MATLAB, это транслируется в специальные команды для CUDA. Эти команды разбивают большую задачу на множество мелких. Вместо того чтобы работать с исходными большими матрицами целиком, их делят на маленькие блоки. Эти блоки загружаются в сверхбыструю разделяемую память (shared memory), доступную каждому потоковому мультипроцессору. И уже внутри этих блоков множество параллельных нитей (threads) одновременно считают свои части результирующей матрицы, постоянно подгружая новые порции данных из основной памяти GPU.

Таким образом, зафиксированные 0,3644 секунды — это сумма нескольких составляющих: времени на пересылку данных из глобальной памяти GPU в разделяемую память и регистры, времени на выполнение самих математических операций над этими данными, времени на запись вычисленных результатов обратно в глобальную память, а также времени на выполнение последующих, менее затратных ядер, реализующих функции Leaky ReLU и сигмоиды.

Понимание этих механизмов напрямую подводит нас к вопросу о возможных путях сокращения времени обработки. Несмотря на то, что используемый код на MATLAB уже является весьма эффективным, есть ряд архитектурно-обусловленных методов оптимизации. Первый способ – снижение разрядности вычислений. Использование типа half (fp16) вместо single позволило бы сократить объем перемещаемых данных вдвое, что автоматически уменьшило бы время на операции с памятью, но снизило бы точность. Ещё более агрессивный метод – квантование, то есть снижение точности весов до целочисленных форматов, например, int8. Это позволяет задействовать целочисленные вычислительные блоки и еще сильнее сжать данные, однако требует тщательной калибровки, чтобы не потерять в точности классификации.

Другой важный фактор – сама стратегия обработки данных. В данном эксперименте обрабатывались все изображения сразу, что обеспечило максимальную загрузку GPU. Если бы подавались изображения по одному, время каждого инференса было бы значительно больше из-за накладных расходов на инициализацию и запуск каждого ядра CUDA.

Заключение

В итоге, проведенный анализ позволяет сделать следующие выводы из эксперимента. Измеренное время обработки 143 изображений составило 0,3644 с, что соответствует 2,55 мс на один классифицируемый кадр. Достигнутая производительность обусловлена применением пакетной векторизованной обработки, позволившей эффективно загрузить вычислитель-

ные ресурсы GPU. Результат наглядно демонстрирует, что даже относительно скромная по современным меркам видеокарта способна выполнять сложные матричные вычисления со скоростью, достаточной для многих практических задач. Архитектура GPU, изначально ориентированная на массовый параллелизм, позволила эффективно выполнить большой объем матричных операций, лежащих в основе инференса нейросети. С точки зрения цифровой обработки сигналов, данный эксперимент показывает, что GPU является зрелым и надежным инструментом для задач классификации, способным работать с высокой скоростью без необходимости снижения разрядности и, как следствие, без риска потери точности детектирования подповерхностных объектов.

Библиографический список

1. Хайкин, С. Нейронные сети: полный курс, 2-е издание. / Пер. с англ. – М. / Изда-тельский дом «Вильямс», 2006. – 1104 с. / ил. – Парал. тит. англ. – ISBN 5-8459-0890-6

2. Travassos X. L., Avila S. L., Ida N. Artificial Neural Networks and Machine Learning techniques applied to Ground Penetrating Radar: A review / Applied Computing and Informatics. — 2018. — P. 1–8. — DOI: 10.1016/j.aci.2018.10.001.

СЕКЦИЯ «АКТУАЛЬНЫЕ ЗАДАЧИ ХИМИЧЕСКИХ ТЕХНОЛОГИЙ»

УДК 621.396; ГРНТИ 31.21

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СОДЕРЖАНИЯ ОКСИДА АКТИВНЫХ МЕТАЛЛОВ В КАТАЛИЗАТОРЕ НА ЭФФЕКТИВНОСТЬ ПРОЦЕССА ОКИСЛЕНИЯ БИОДИЗЕЛЬНОГО ТОПЛИВА

С.А. Юдаев, Е.В. Алтабаев
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, evaltabaev@gmail.com

Аннотация. В работе изучено влияние содержания оксида активного металла – меди в используемом катализаторе на эффективность процесса окисления биодизельного топлива. Проанализирована эффективность окисления сырья в целевой продукт при различном содержании активного металла – меди (Cu/Al2O3) в катализаторе, нанесенном на Al2O3 в качестве носителя методом пропитки.
Ключевые слова: окисление, биодизельное топливо, каталитические процессы, катализаторы прямого окисления, каталитические системы, оксид меди.

STUDY OF EFFECT OF CATALYST ACTIVE METAL CONTENT ON EFFICIENCY OF BIODIESEL FUEL OXIDATION PROCESS

S.A. Yudaev, E.V. Altabaev
Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, evaltabaev@gmail.com

Summary. The paper covers studies of impact of active metal oxide content in the used catalyst on efficiency of biodiesel fuel oxidation. Efficiency of target product oxidation under various active metal content has been analyzed. Copper was the active metal used in the catalyst (Cu/Al2O3). The copper oxide was applied via impregnation on the Al2O3 carrier.
Keywords: oxidation, biodiesel, catalytic processes, direct oxidation catalysts, catalytic systems, copper oxide.

Исследовали эффективность окисления биодизельного топлива при различных концентрациях активного компонента в катализаторе в равных условиях проведения реакции.

Использовались оксиды металла в трёх различных концентрациях:

1) исходное, которое было использовано в первоначальном исследовании;
2) концентрация ниже исходного значения;
3) концентрация выше исходного значения.

Остальные характеристики катализатора оставались неизменными. Рисунок 1 позволяет получить представление о том, как выглядит исследуемый катализатор.

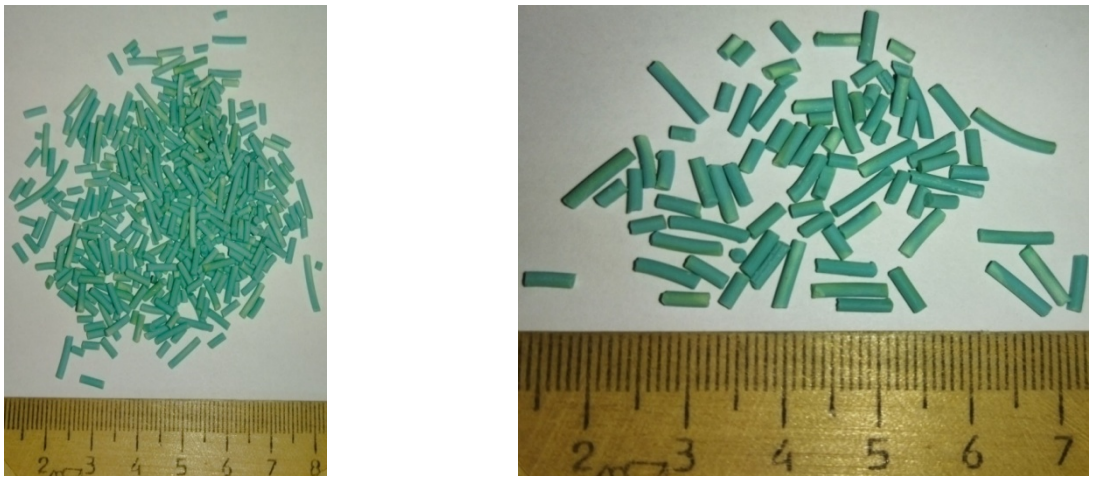


Рис. 1. Внешний вид катализатора Cu/Al_2O_3 (4,82%)

Основные характеристики исходного катализатора представлены в таблице 1.

Таблица 1. Основные характеристики исходного катализатора

Оксид активного металла	Концентрация оксида активного металла % масс.	Общий объем пор, $см^3/г$	Удельная поверхность, $м^2/г$	Насыпной вес, $г/см^3$	Прочность, Н/гранула
CuO	4,82	0,67	165	0,85	15,2
CuO	3,66	0,69	173	0,83	15,0
CuO	2,03	0,67	175	0,83	14,8
CuO	0,89	0,69	182	0,82	15,3
CuO	6,25	0,66	160	0,86	15,2
CuO	6,84	0,66	160	0,86	15,3
CuO	7,56	0,65	161	0,88	15,1

Исследования проводили в несколько стадий. Для проведения экспериментов были отмерены навески катализатора с различным содержанием активного металла одинаковой массы (15 г) для загрузки реактора. Далее в реактор было залито 100 мл окисляемого сырья – биодизельного топлива, установлена подача окислителя с постоянным расходом 26 л/ч. В качестве окислителя использовали атмосферный осушенный воздух. Для контроля расхода воздуха использовался ротаметр. Реакция проходила при температуре 120°С. Поддержание необходимого значения температуры обеспечивалось ПИД-регулятором. После того, как была достигнута требуемая температура, каждые 60 минут производился отбор проб отработанного воздуха для анализа степени эффективности окисления исходного сырья. Эффективность оценивали путём замера содержания кислорода в атмосферном воздухе на входе в реактор и с последующим замером содержания кислорода на выходе из реактора. В целом, продолжительность каждого эксперимента, включая фазу окисления, составляла 6 часов. Результаты замеров фиксировались для последующей обработки.

Вышеописанный эксперимент проводили с одинаковыми условиями процесса для каждой партии катализатора с различной концентрацией активного компонента.

Результаты замера содержания кислорода в атмосферном воздухе до поступления в реактор и после реактора для каждого значения содержания активного металла приведены в таблице 2.

Таблица 2. Содержание кислорода в окислителе для различных значений концентрации активного металла

Катализатор	**Концентрация активного компонента % масс.**	**Концентрация кислорода на входе в реактор, %об.**	**Концентрация кислорода после реактора, %об.**	**Относительная активность катализатора, %**
-		20,1	19,7	0
Cu/Al_2O_3	4,82	20,1	18,2	83,3
Cu/Al_2O_3	3,66	20,1	18,4	72,2
Cu/Al_2O_3	2,03	20,1	19,0	38,9
Cu/Al_2O_3	0,89	20,1	19,1	33,3
Cu/Al_2O_3	6,25	20,1	18,0	94,4
Cu/Al_2O_3	6,84	20,1	18,0	94,4
Cu/Al_2O_3	7,56	20,1	17,9	100,0

Обсуждая результаты, можно сделать следующий вывод о влиянии концентрации активного компонента в катализаторе на основе оксида меди: увеличение концентрации оксида меди приводит к увеличению относительной каталитической активности катализатора. Но данное увеличение не является линейным так как с увеличением концентрации присутствуют ряд факторов, влияющих на каталитическую активность. Первый фактор диффузионные затруднения – так как масса загрузки катализатора неизменна от эксперимента к экспери-

менту, стоит предположить, что область протекания процесса переходная и лимитирующей стадией будет при низких концентрациях активного компонента кинетическая, а при высоких концентрациях диффузионная (рис. 2).

Второй фактор структура активного компонента на поверхности катализатора. Часть активных центров на поверхности катализатора при высоких концентрациях оксида меди может быть недоступна для атаки субстрата. Подтвердить влияние второго фактора можно после проведения рентгеноструктурного анализа.

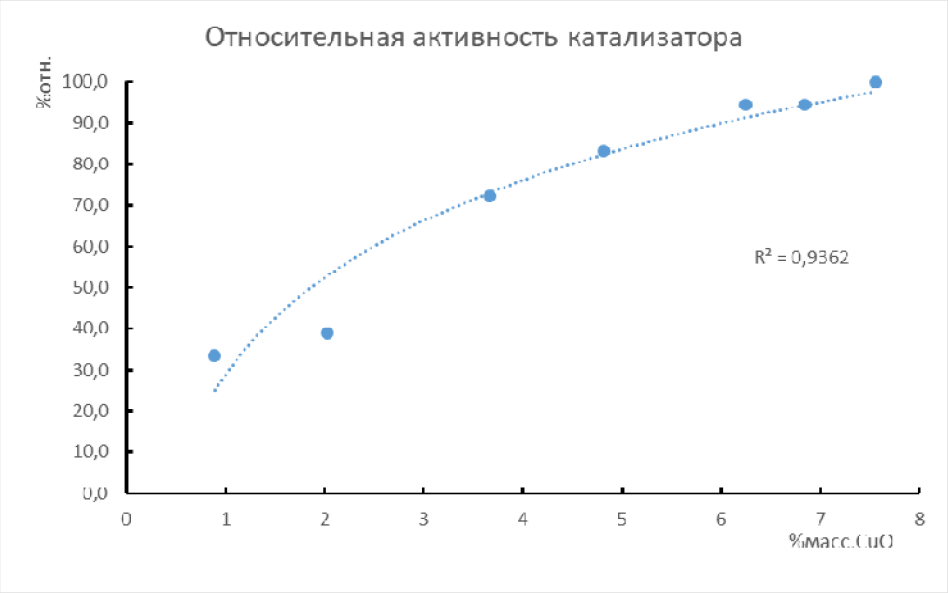


Рис. 2. Показатели относительной активности катализатора в зависимости от концентрации оксида меди

Таким образом, можно прийти к следующему заключению: концентрация активного металла в катализаторе непосредственно связана с эффективностью процесса окисления. Для конкретных условий каталитической реакции следует подбирать оптимальное содержание оксида меди, которое обеспечит максимальную активность и выход целевого продукта с учётом того, что концентрация может быть увеличена лишь до определённых значений, ввиду действующих ограничений, описанных выше.

В ходе описанного эксперимента, на ставилась задача проведения анализа продуктов окисления с целью определения их состава, а также подробно не рассматривался механизм реакции. При последующих исследованиях будет расширена аппаратная база, в частности, в состав оборудования будет включён ИК-Фурье Спектрометр ФСМ 2202 производства компании «Инфраспек». Планируется проведение анализа компонентного состава продуктов окисления, будет определён состав окисленного биодизельного топлива при использовании катализатора на основе оксида меди, будут сравниваться основные характеристики исходного и окисленного продукта, анализироваться их качественные показатели.

Расширенный набор исходных данных поможет понять сущность реакций, протекающих в процессе рассматриваемого процесса окисления в присутствии катализатора, позволит получить представление о возможных способах использования продуктов окисления, а также сделать выводы о том, какие дополнительные компоненты либо параметры могли бы способствовать дальнейшему повышению эффективности процесса.

Библиографический список

1. Юдаев С.А., Шуварикова О.В., Ветшев К.А., Рубцова А.Д. Синтез и свойства гетерогенных катализаторов эпоксидирования МЭЖК / Журнал Сибирского федерального университета. Серия: Химия. 2022. Т. 15. № 2. С. 214-225.

2. Сапунов В.Н., Юдаев С.А., Черепанова А.Д., Ивашкина Е.Н., Воронов М.С., Козловский Р.А. Особенности процесса эпоксидирования метиловых эфиров жирных кислот в барботажном реакторе / Журнал прикладной химии. 2020. Т. 93. № 5. С. 697-704.

3. Chu, S.; Zeng, X.; Lin, H.; Zhu, Y. High-performance catalytic wet oxidation of excess activated sludge derived from pharmaceutical wastewater treatment process over a CU/-AL2O3 catalyst. Water 2023, 15, 3494. https://doi.org/10.3390/w15193494.

4. Bhuiya MMK, Rasul MG, Khan MMK, Ashwath N, Azad AK (2015) Prospects of 2nd generation biodiesel as a sustainable fuel–part: 1 selection of feedstocks, oil extraction techniques and conversion technologies. Renew Sustain Energy Rev 55:1109–1128. https://doi.org/10.1016/j.rser.2015.04.163

5. Jain S, Sharma M (2010) Stability of biodiesel and its blends: a review. Renew Sustain Energy Rev 14:667–678. https://doi.org/10.1016/j.rser.2009.10.011

6. Bhaduri S, Doble M (2000) Homogeneous catalysis: mechanisms and industrial applications. Wiley, New York

УДК 692.415 ГРНТИ 67.15.51

ФУНКЦИОНАЛЬНЫЕ НАПОЛНИТЕЛИ И МОДИФИКАТОРЫ В РЕЦЕПТУРАХ ПОЛИМЕРНЫХ МЕМБРАН НА ОСНОВЕ ПВХ

Е.Ю. Храпова*, Г.И. Мельник**

**Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, hrapovakeit2000@gmail.com*

***Рязанский институт (филиал) Московского политехнического университета, Российская Федерация, Рязань, galame@yandex.ru*

Аннотация. В настоящей работе представлен комплексный анализ роли функциональных наполнителей и модификаторов в составе поливинилхлоридных (ПВХ) мембран. Рассмотрена классификация наполнителей по химическому составу и морфологии, их влияние на реологические, механические и барьерные свойства композиций. Особое внимание уделено структурным аспектам формирования наполненных систем, включая роль надмолекулярной организации ПВХ и термодинамику межфазных взаимодействий. Проведен сравнительный анализ модификаторов ударопрочности различных классов, выявлены закономерности их совместного действия с наполнителями. На основе обобщения экспериментальных данных сформулированы практические рекомендации по оптимизации рецептур ПВХ-мембран с заданным комплексом эксплуатационных свойств.

Ключевые слова: поливинилхлорид, ПВХ-мембраны, минеральные наполнители, модификаторы ударопрочности, надмолекулярная структура, межфазная граница, барьерные свойства.

FILLERS AND MODIFIERS IN PVC MEMBRANE FORMULATIONS

E. Yu. Khrapova*, G. I. Melnik**

**Ryazan State Radiotechnical University named after V.F. Utkin, Russian Federation, Ryazan, hrapovakeit2000@gmail.com*

***Ryazan Institute (branch) of Moscow Polytechnic University, Russian Federation, Ryazan, galame@yandex.ru*

The summary. This paper presents a comprehensive analysis of the role of functional fillers and modifiers in polyvinyl chloride (PVC) membranes. The classification of fillers by chemical composition and morphology, their influence on the rheological, mechanical and barrier properties of composites are considered. Special attention is paid to the structural aspects of the formation of filled systems, including the role of the supramolecular organization of PVC and the thermodynamics of interfacial interactions. A comparative analysis of impact modifiers of various classes is carried out, and the patterns of their combined action with fillers are revealed. Based on the gener-

alization of experimental data, practical recommendations for optimizing PVC membrane formulations with a given set of performance properties are formulated.
Keywords: polyvinyl chloride, PVC membranes, mineral fillers, impact modifiers, supramolecular structure, interface, barrier properties.

Поливинилхлорид является одним из важнейших полимеров в производстве водонепроницаемых мембран благодаря своим свойствам, химической стойкости и способности существенно изменять свои свойства [1]. Данный полимер допускает введение большого количества разнообразных добавок, что позволяет осознано регулировать характеристики полученного материала.

В многокомпонентных композициях ПВХ наполнители и модификаторы используются не только в качестве загустителей. Они образуют сложную гетерофазную структуру, где характер распределения частиц и их взаимодействие с полимерной матрицей определяют весь спектр физических свойств мембраны [2]. Понимание структурных закономерностей формирования наполненных систем особенно важен, поскольку именно структура материала на глубоком уровне определяет его внешние характеристики.

Структурные закономерности формирования наполненных композиции ПВХ

Особенности наполнения поливинилхлорида во многом определяется особенностями его надмолекулярной структуры. Промышленные полимеры, полученные суспензионным методом, представляют собой сложные иерархические структуры. Как показано в работах В.А. Каргина и его школы [3], основные частицы (сферы) размером около одного микрона, образующиеся на первых стадиях полимеризации, в дальнейшем сцепляются в более крупные зерна. Наиболее важным фактором является частичная защита структуры этой сферы в процессе переработки через расплав [4].

При вальцевании или экструзии при температурах 150–180°С происходит разрушение крупных спаек, однако зерна размером около микрона большей части сохраняются. Межзерновая область, обладающая пониженной плотностью, становится зоной большей размещения частиц вводимых наполнителей. Это явление можно назвать «межструктурным наполнением» [5], имеет важное значение: наполнитель распределяется не беспорядочно, а вынужденно располагается в межглобулярных областях, образуя специфическую пространственную структуру [2].

Вид этой структуры зависит от количества и размера молекул наполнителя. При малых содержаниях (до 3–5% объемных) частицы располагаются уединено. По достижении высокой концентрации(около 5–10% объемных) образуется непрерывная сетчатая структура, что ведёт к изменению многих свойств композиции [4].

Важным фактором является термодинамика межфазных взаимодействий. Поверхность наполнителя фиксирует прилегающие слои полимера, уменьшая подвижность макромолекул. Толщина этих пограничных слоев может достигать десятков нанометров, и при высоких степенях наполнения большая часть полимера переходит в связанное состояние [2]. Наряду с изменениями энтропии в процессе трансформации этих систем важную роль играет энергетический эффект за счет перестройки межступенчатых связей.

Классификация и функциональные особенности наполнителей

Анализ литературных данных [1, 2, 4] позволяет выделить несколько основных групп наполнителей, применяемых в производстве ПВХ-мембран.

Карбонатные наполнители. Карбонат кальция в форме тонкодисперсного мела остается наиболее распространенным наполнителем [1]. Частицы мела имеют изометричную форму и относительно невысокую удельную поверхность. Введение мела повышает жесткость и модуль упругости, снижает усадку при формовании. Однако при концентрациях,

превышающих 30–40 массовых частей на 100 частей ПВХ, наблюдается существенное снижение относительного удлинения при разрыве и ударной вязкости, что связано с отсутствием прочной адгезионной связи с матрицей [4]. Принципиально иная картина наблюдается при использовании наноразмерных карбонатов кальция. Частицы размером 50–100 нм способны проникать в межглобулярные области и выступать в роли «микроармирующих» элементов. При оптимальных концентрациях (3–7% объемных) такие наполнители могут повышать ударную вязкость за счет активации механизмов рассеяния энергии при развитии трещин [6].

Силикатные наполнители. Каолин и тальк относятся к слоистым силикатам и характеризуются пластинчатой формой частиц [1]. Пластинки, ориентируясь в процессе переработки преимущественно параллельно поверхности изделия, создают эффективный барьер для диффузии газов и паров. Коэффициент проницаемости таких композиций может снижаться в несколько раз даже при умеренных степенях наполнения [2]. Пластинчатые наполнители в большей степени повышают жесткость и термостойкость, но также в большей степени склонны снижать эластичность, что требует совместного применения с ударными модификаторами.

Высокодисперсный диоксид кремния. Особое место занимает пирогенный диоксид кремния (аэросил) с удельной поверхностью до 300–400 м²/г [4]. Даже небольшие добавки аэросила (1–3%) способны существенно изменять реологическое поведение пластизолей и расплавов. В области малых концентраций (до 3–4%) наблюдается аномальное снижение вязкости расплава, объясняемое «расклинивающим» действием частиц, проникающих в межглобулярные области. При дальнейшем увеличении содержания наполнителя, по мере формирования непрерывной сетки частиц, вязкость резко возрастает [4].

Поверхностная модификация наполнителей

Эффективность наполнения в значительной степени определяется характером взаимодействия на границе раздела фаз. Минеральные наполнители имеют гидрофильную поверхность с высокой поверхностной энергией, тогда как ПВХ является относительно гидрофобным полимером [2]. Это приводит к плохому смачиванию, агрегации частиц и слабой адгезионной связи.

Наиболее распространенным методом модификации является обработка стеаратами металлов, которые создают на поверхности карбонатов гидрофобный монослой [1]. Частицы с такой обработкой легче диспергируются, снижают вязкость расплава и позволяют достигать более высоких степеней наполнения без катастрофической потери механических свойств. Для наполнителей с развитой поверхностью (диоксид кремния, каолин) эффективна обработка органофункциональными силанами, обеспечивающая образование прочной связи между наполнителем и полимером [2].

Модификаторы ударопрочности

Для мембран, эксплуатирующихся при динамических нагрузках и пониженных температурах, критическое значение приобретает ударная вязкость. Немодифицированный ПВХ склонен к хрупкому разрушению, что неприемлемо для ответственных применений [1].

Механизм действия ударных модификаторов основан на формировании дисперсной эластомерной фазы. Частицы модификатора размером 0,1–1 мкм распределяются преимущественно в межглобулярных областях. При ударном воздействии вокруг них развиваются множественные микротрещины, поглощающие энергию удара и предотвращающие развитие магистральной трещины [4].

Наиболее распространенным типом является хлорированный полиэтилен (ХПЭ). Оптимальное содержание хлора (36–42%) обеспечивает хорошую совместимость с ПВХ при

сохранении эластичных свойств [1]. ХПЭ эффективно повышает ударную вязкость, однако снижает прозрачность и может ухудшать термостабильность.

Для прозрачных и атмосферостойких изделий предпочтительны акриловые модификаторы (МБС, МАС). Отсутствие ненасыщенных связей в их структуре обеспечивает высокую стойкость к фотоокислению, что критично для наружных мембран [1]. Акриловые модификаторы сохраняют прозрачность и в меньшей степени снижают модуль упругости.

В пластифицированных композициях для достижения высокой морозостойкости применяют нитрильные каучуки. Их высокая полярность обеспечивает хорошую совместимость с ПВХ, а эластичность сохраняется до температур –40°С и ниже [4].

Закономерности совместного действия наполнителей и модификаторов

В реальных рецептурах наполнители и модификаторы используются совместно, и характер их взаимодействия не всегда аддитивен. При совместном введении мела и ударного модификатора наблюдается типичная картина: модификатор в значительной степени компенсирует охрупчивающее действие наполнителя [1].

При сочетании пластинчатых наполнителей с эластомерными модификаторами ориентированные пластинки каолина или талька создают барьер для распространения трещин, тогда как эластомерные частицы обеспечивают диссипацию энергии [2]. В области огнезащитных композиций проявляется синергизм гидроксидов металлов и фосфорсодержащих соединений, позволяющий снизить их общую концентрацию при сохранении требуемого уровня огнестойкости [1]. Сводная таблица по влиянию на свойста представлена в таблице 1.

Таблица 1. Характер влияния компонентов на ключевые свойства ПВХ-мембран

Компонент / Свойство	Мел (карбонат кальция)	Каолин / Тальк (пластинчатые)	Аэросил (высокодисперсный)	ХПЭ (ударный модификатор)
Жесткость / Модуль упругости	Повышает	Значительно повышает	Повышает (при образовании сетки)	Снижает
Эластичность / Удлинение	Снижает (при высоких дозах)	Может снижать	Снижает	Слабо влияет или компенсирует
Ударная вязкость	Снижает (кроме нано-мела)	Требует добавок	Сложное влияние	Значительно повышает
Барьерные свойства	Не влияет	Значительно улучшает	Не влияет	Не влияет
Технологичность	Улучшается при модификации	Удовлетворительная	Регулирует вязкость расплава	Может ухудшать переработку

Практические рекомендации по разработке рецептур

Обобщение рассмотренных закономерностей позволяет сформулировать ряд рекомендаций. Для гидроизоляционных мембран общего назначения оптимальным представляется использование мела с поверхностной обработкой стеаратами в концентрации 20–40 массовых частей в сочетании с 5–8 частями ХПЭ [1].

Для мембран с повышенными требованиями к атмосферостойкости предпочтителен переход на акриловые модификаторы в сочетании с каолином и диоксидом титана [2]. При

разработке композиций для низкотемпературного применения необходимо использование нитрильных каучуков и пластификаторов с ограниченной совместимостью, обеспечивающих сохранение эластичности при отрицательных температурах [4].

Для огнезащитных мембран наиболее перспективно использование комбинаций гидроксида алюминия или магния с фосфорсодержащими синергистами при тщательной оптимизации рецептуры для минимизации ухудшения эластичности [1].

Создание современных ПВХ-мембран с заданным комплексом свойств требует понимания сложных взаимосвязей между составом, структурами и свойствами многокомпонентных систем. Ключевыми факторами являются сохранение надмолекулярной структуры полимера при переработке, формирование пространственной структуры фазы наполнителя и характер межфазных взаимодействий. Оптимизация рецептур представляет собой многопараметрическую задачу, успешное решение которой возможно лишь на основе системного подхода, учитывающего всю совокупность структурных и термодинамических факторов.

Библиографический список

1. Пахомов, Поливинилхлоридные композиции: учеб. пособие /С.И. Пахомов, И.П.Трифонова, В.А. Бурмистров; Иван. гос. хим.-технол. ун-т, - Иваново, 2010. – 104 с.

2. Ксантос, М. под ред. Функциональные наполнители для пластмасс / М.П. Ксантос, перевод с английского под ред. В.Н. Кулезнева. – Санкт-Петербург : Научные основы и технологии, 2010. – 462 с.

3. Милевски, Д.В. Наполнители для полимерных композиционных материалов : Справ. пособие / [Дж. Милевски, Г. Кац, Т.Х. Ферригно и др.]; Под ред. Г.С. Каца, Д.В. Милевски Перевод с англ. С.В. Бухарова и др. Под ред. П.Г. Бабаевского. - М. : Химия, 1981. - 736 с.

4. Гузеев, В.В. Структура и свойства наполненного ПВХ / В.В. Гузеев. – Санкт-Петербург : Научные основы и технологии, 2012. – 284 с.

5. Соломко В.П. Межструктурное наполнение полимеров // Механика полимеров. – 1976. – № 1. – С. 162-164.

6. Саммерс, Дж. ПВХ (Поливинилхлорид): получение, добавки и наполнители, сополимеры, свойства, переработка / Дж. Саммерс, Ч. Уилки, Ч. Даниэлс ; под ред. Г. Е. Заикова. – Санкт-Петербург : Профессия, 2007. – С. 270–313.

УДК 004.94; ГРНТИ 28.17.33

СИНТЕЗ СХЕМЫ РАЗДЕЛЕНИЯ СМЕСИ ПЕНТАН - ГЕКСАН - ГЕПТАН

Г.А. Шашкина, Н.Ю. Кулавина, В.В. Медведева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Россия, Рязань, xt-kontakt@mail.ru

Аннотация. При решении задач анализа и синтеза химико-технологических процессов (ХТП) возникают различные трудности, связанные с необходимость учета взаимодействий на молекулярном уровне, различных фазовых состояний, сочетанием различных физико-химических процессов. Для моделирования ХТП используют пакеты моделирующих программ. Они объединяют базы данных химических компонентов и расширенные методы расчёта термодинамических свойств. Программа COCO (CAPE OPEN to CAPE OPEN) - бесплатная среда моделирования химико-технологических процессов (стационарный режим). В данной работе рассматривается синтез схемы разделения смеси пентан – гексан – гептан, состоящей из двух ректификационных колонн в модуле ChemSep пакета моделирования химико-технологических процессов COCO.

Ключевые слова. синтез, оптимизация, ХТС, уравнение состояния Пенга - Робинсона, COCO (CAPE OPEN to CAPE OPEN), эвристическое правило разделения углеводородных смесей.

SYNTHESIS OF A PENTANE-HEXANE-HEPTANE SEPARATION SCHEME

G.A. Shashkina, N.Yu. Kulavina, V.V. Medvedeva
Ryazan State Radiotechnical University named after V.F. Utkin,
Russia, Ryazan, xt-kontakt@mail.ru

Annotation. When solving problems of analysis and synthesis of chemical and technological processes (CTP), various difficulties arise due to the need to take into account interactions at the molecular level, different phase states, and the combination of various physical and chemical processes. To model CTP, modeling software packages are used. These packages combine databases of chemical components and advanced methods for calculating thermodynamic properties. COCO (CAPE OPEN to CAPE OPEN) is a free software environment for modeling chemical and technological processes (stationary mode). This paper discusses the synthesis of a separation scheme for a pentane-hexane-heptane mixture consisting of two rectification columns in the ChemSep module of the COCO chemical process modeling package.
Keywords. Synthesis, optimization, CTS, Peng-Robinson equation of state, COCO (CAPE OPEN to CAPE OPEN), heuristic rule for the separation of hydrocarbon mixtures.

Задачи, которые возникают при использовании, реконструкции или проектировании химико-технологических систем, требуют научно-обоснованного подхода к их выполнению. Анализ позволяет разбить практически любую сложную проблему на более простые, синтез - объединить новые решения по каждому элементу в единое целое, оптимизация – выбрать лучший вариант для каждой конкретной задаче.

Сложность анализа и синтеза схем процессов химической технологии объясняется присутствием смесей веществ с разным строением молекул, находящихся одновременно в различных фазах в составе потоков, сложной сетью взаимосвязей аппаратов, сочетанием различных физико-химических процессов: кинетических, термодинамических, диффузионных, гидродинамических. Процессы переменны во времени и пространстве, часто протекают при высоких или низких давлениях и температурах. Все эти факторы значительно затрудняют моделирование и предсказание поведения химико-технологической системы (ХТС).

Средства автоматизации расчетов процессов химической технологии по данным причинам немногочисленны, дорогие и сложные в изучении.

Исключение составляет программа COCO (CAPE OPEN to CAPE OPEN) – бесплатная среда моделирования химико-технологических процессов (стационарный режим), разрабатываемая главным образом компанией AmsterCHEM [1]. Программа создана по стандарту CAPE OPEN (Computer-Aided Process Engineering). Это открытый, унифицированный международный стандарт, обеспечивающий взаимодействие программных компонентов для моделирования химико-технологических процессов (процессных симуляторов).

Синтезу схемы ХТС предшествует анализ начальных условий, состава аппаратных средств, режимов их работы, требований к параметрам выходных продуктов. Синтез заключается в выборе химического способа производства целевых продуктов, разработке технологической топологии системы аппаратов и соединяющих их технологических потоков, определение конструкционных и технологических параметров каждого элемента, обеспечивающих функционирование системы при оптимальной величине коэффициента эффективности и оптимальных показателях свойств технологической системы [2].

Дальнейший анализ и оптимизация полученной схемы позволяет получить модель процесса, приближенного к реальному по определяющим показателям. Такая модель может использоваться для исследований и оптимизации реального химико-технологического процесса [3].

Синтезируется схема процесса разделения смеси пентан, гексан, гептан при атмосферном давлении на продукты (пентан и гептан) чистотой не менее 99 %.

В таблице 1 приведен начальный компонентный состав разделяемой смеси в мольных долях. Для разделения углеводородных смесей на чистые компоненты определяются температуры кипения компонентов.

Таблица 1. Состав смеси

Вещество	Формула	Температура кипения °С	Состав, мольные доли
н-Пентан	C_5H_{12}	36,1	0,5
н-Гексан	C_6H_{14}	68,7	0,2
н-Гептан	C_7H_{16}	98,4	0,3

Для разделения выбирается ректификация. В составе смеси три компонента, поэтому для получения каждого из них в чистом виде необходимо использовать две модели колонных аппаратов с двумя выходами – дистиллятом и кубовым остатком. В один выход первой колонны может выделяться один компонент в чистом виде, во второй – смесь двух других. Кубовой продукт первой колонны подается на вход второй колонны для дальнейшего разделения смеси двух оставшихся компонентов. Исходя из этого для проведения процесса разделения необходимы две модели простых ректификационных колонн или одна модель ректификационной колонны с тремя выходами. В данной работе рассматривается более простой вариант модели разделения из двух ректификационных колонн.

Первый шаг синтеза любой схемы в программе COCO – выбор компонентов исходной продуктовой смеси из встроенной базы (модуля ChemSep) и термодинамической модели (уравнения состояния), которая будет использоваться для расчетов.

Компонентный состав смеси для синтезируемой схемы размещается в окне конфигурации системы, как показано на рисунке 1.

Selected components for simulation:

Identifier	L#	Tnb (K)	File	Loc.	CAS
N-pentane	7	309.220	c:\program file	115	109-66-0
N-hexane	11	341.880	c:\program file	135	110-54-3
N-heptane	17	371.570	c:\program file	147	142-82-5

Рис. 1. Набор компонентов, задействованных в синтезируемой схеме

Для заданного состава смеси наиболее подходит уравнение состояния Пенга-Робинсона (PR EOS). Это кубическая термодинамическая модель, связывающая давление, объем и температуру (*p, V, T*) реальных газов и жидкостей.

Модель использует критические температуру и давление, ацентрический фактор для расчетов. Эффективно применяется для расчета фазовых переходов, плотности жидкостей и составов фаз в смесях для точного описания углеводородных систем, критических свойств и фазовых равновесий (пар-жидкость).

Задается термодинамическая модель Пенга – Робинсона вместе с составом компонентов в окне параметров конфигурации схемы всего процесса, в разделе термодинамические свойства (Property/ Thermodynamics) (рис. 2).

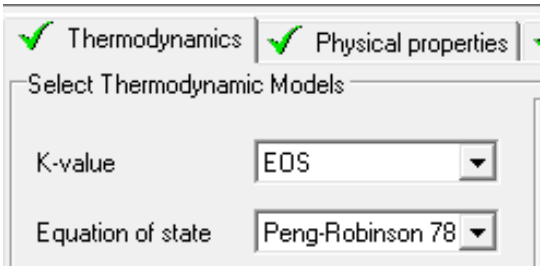


Рис. 2. Заданная термодинамическая модель Пенга – Робинсона

Для синтеза схемы процессов разделения используются эвристическое правило разделения углеводородных смесей на чистые компоненты: выделяется первым преобладающий компонент, предпочтительно эквимолярное разделение (50:50), продукты с повышенными требованиями к их чистоте следует выделять сначала как дистиллят.

Предполагается непосредственное разделение с выделением в дистиллят пентана в первой колонне в соотношении пар-жидкость 50:50 и последующим разделением остаточной смеси кубового продукта, который направляется в качестве питания на вторую колонну.

При разделении кубового продукта должно быть получено не менее 99% гексана в дистилляте второй колонны.

Для входного потока задаются давление 1 атм, мольные доли компонентов, расход 1 моль/с. Температура рассчитывается программой для 0,5 долей пара и жидкого продукта, в разделе Phase fraction. Получено значение 61,3209 ^{o}C (рис. 3).

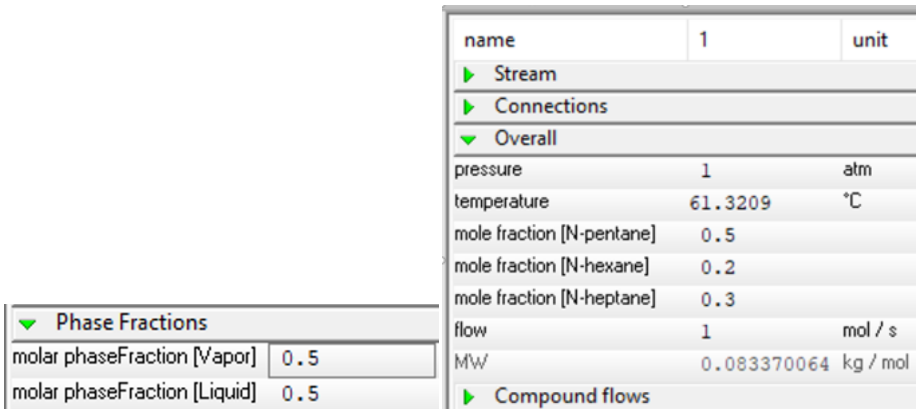
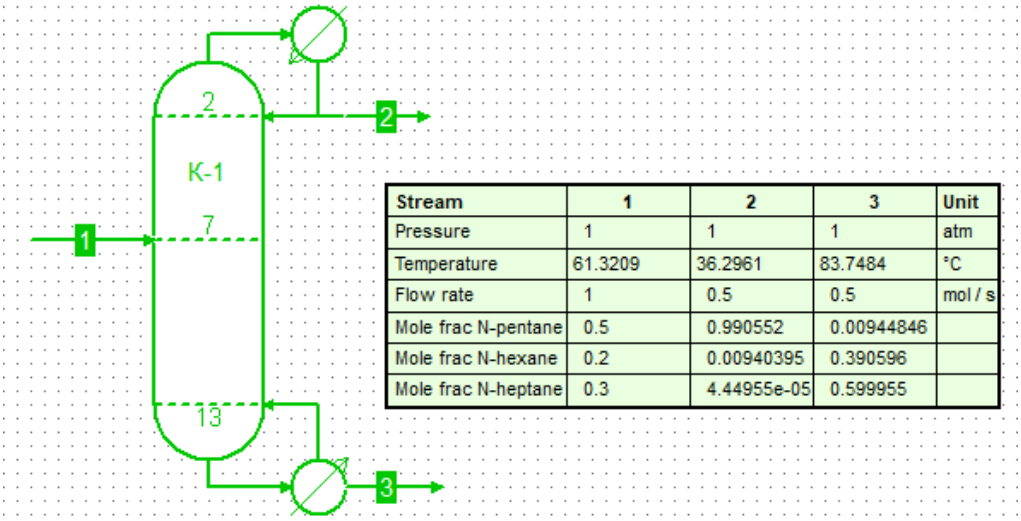


Рис. 3. Заданные и рассчитанные программой параметры

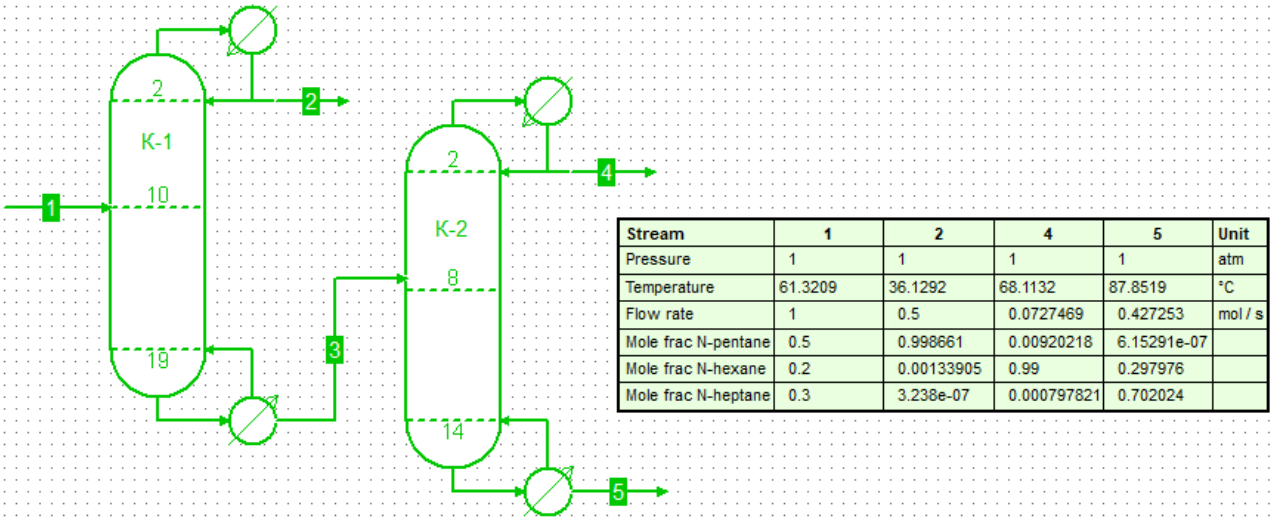
В таблице выходных параметров колонны (рис. 4) можно видеть, что в дистиллят выделилось 99 % пентана (2 поток).



Stream	1	2	3	Unit
Pressure	1	1	1	atm
Temperature	61.3209	36.2961	83.7484	°C
Flow rate	1	0.5	0.5	mol / s
Mole frac N-pentane	0.5	0.990552	0.00944846	
Mole frac N-hexane	0.2	0.00940395	0.390596	
Mole frac N-heptane	0.3	4.44955e-05	0.599955	

Рис. 4. Рассчитанные программой значение дистиллята

Результат второй колонны (рис. 5) – в дистилляте 99% гексана (4 поток), в кубовый остаток выделилось 70,2% гептана (5 поток).



Stream	1	2	4	5	Unit
Pressure	1	1	1	1	atm
Temperature	61.3209	36.1292	68.1132	87.8519	°C
Flow rate	1	0.5	0.0727469	0.427253	mol / s
Mole frac N-pentane	0.5	0.998661	0.00920218	6.15291e-07	
Mole frac N-hexane	0.2	0.00133905	0.99	0.297976	
Mole frac N-heptane	0.3	3.238e-07	0.000797821	0.702024	

Рис. 5. Рассчитанные программой значение кубового остатка

Синтез схемы завершен, полученные результаты соответствуют предполагаемым.

Для оптимизации схемы процесса разделения можно использовать встроенный модуль анализа зависимостей выходных параметров схемы от значения входных параметров, например, определить зависимости составов дистиллята и кубового остатка по каждой из колонн (или для всей схемы) от температуры.

Синтез схем ХТС в программах компьютерного моделирования химико-технологических процессов дает широкие возможности для их дальнейшей оптимизации. Актуальность оптимизации ХТП связана с необходимостью создавать высокоэффективные химические производства и учитывать неопределённость в исходной информации при проектировании ХТС поскольку существуют параметры, значение которых точно неизвестны, известны только диапазоны их изменения.

Библиографический список

1. Сайт программы COCO (CAPE-OPEN to CAPE-OPEN) https://www.cocosimulator.org/.
2. Лабораторный практикум по моделированию и оптимизации химико-технологических процессов и систем с помощью программного продукта ASPEN PLUS: Учебное пособие / Холоднов В.А., Викторов В.К., Ананченко И.В., Чепикова В.Н.; СПбГТИ, - СПб., - 2000 – 41с.
3. Шимова, Ю. С. Моделирование химико-технологических процессов : учебное пособие / Ю. С. Шимова, Н. Ю. Демиденко, Е. В. Лис. – Красноярск : Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, 2021. – 94 с. – ISBN 978-5-86433-860-5. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/116642.html.

УДК 66.067.8

ИССЛЕДОВАНИЕ ХИМИЧЕСКОГО СОСТАВА ДРЕНАЖНОЙ ВОДЫ ИЗ СЕПАРАТОРОВ БЕНЗИНА УСТАНОВОК АТ

М.В. Лызлова*, А.А. Шанин*, Э.В. Куценко*, М.С. Гоголицына*, А.В. Киселёв*, Г.И. Мельник**

**Рязанский государственный радиотехнический университет им. В.Ф. Уткина, Российская Федерация, Рязань, mvlsid@rambler.ru*

***Рязанский институт (филиал) Московского политехнического университета, Российская Федерация, Рязань, galame@yandex.ru*

Аннотация. В работе представлены результаты экспериментального исследования химического состава дренажной воды из сепараторов бензина Е-1 и Е-2 установки АТ. Целью работы являлся анализ содержания ионов железа (Fe^{3+}), хлоридов (Cl^-), сульфидов (S^{2-}) и показателя pH, которые определяют коррозионную активность среды. Исследования проводились с применением фотометрических и титриметрических методов. Выполнено сравнение данных за 2017 и 2026 годы, выявившее превышение нормативных значений по содержанию хлоридов и железа в дренажной воде сепаратора Е-2, что свидетельствует о коррозии оборудования или нарушении технологического режима. В качестве способа оптимизации предложено использование поточного анализатора для непрерывного контроля качества воды.

Ключевые слова: дренажная вода, содержание железа, содержание серы, содержание хлора, pH воды.

INVESTIGATION OF CHEMICAL OF DRAINAGE WATER FROM GASOLINE SEPARATION OF ATMOSPHERIC DISITILLATION UNITS

M.V. Lyzlova*, A.A. Shanin*, E.V. Kutsenko*, M.S. Gogolitsyna*, A.V. Kiselyov*, G.I. Melnik**

**Ryazan State Radiotechnical University named after V.F. Utkin, Russian Federation, Ryazan, mvlsid@rambler.ru*

***Ryazan Institute (branch) of Moscow Polytechnic University, Russian Federation, Ryazan, galame@yandex.ru*

The summary. This paper presents the results of an experimental study of the chemical composition of drainage water from the E-1 and E-2 gasoline separators of the AT unit. The aim of the study was to analyze the content of iron ions (Fe^{3+}), chlorides (Cl^-), sulfides (S^{2-}), and pH, which determine the corrosivity of the medium. The studies were conducted using photometric and titrimetric methods. A comparison of data for 2017 and 2026 revealed that chloride and iron content in the drainage water from the E-2 separator exceeded regulatory limits, indicating equipment corrosion or a process violation. The use of an in-line analyzer for continuous water quality monitoring is proposed as an optimization method.

Keywords: drainage water, iron content, sulfur content, chlorine content, water pH.

Дренажная вода представляет собой многокомпонентную смесь, образующуюся в результате конденсации острого водяного пара и выделения эмульсионной воды из нефтяного сырья в процессе атмосферно-вакуумной перегонки. Вода содержит примеси сульфидов, хлоридов, катионов железа.

Сильным коррозионным агентом является HCl, который образуется в результате гидролиза хлоридов магния и кальция при температурах от 120 до 350 ^{0}C, а также при термическом разложении хлорорганических соединений нефти, происходящем наиболее интенсивно в интервале от 250 до 380 ^{0}C. На коррозию влияет изменение концентрации хлорид- и сульфат- ионов. Если значения концентрации хлорид-ионов находятся в диапазоне 100-1000 мг/дм^3, электропроводность раствора увеличивается и, следовательно, протекает электрохимическая реакция, что свидетельствует о разрушении железа. Низкая же концентрация в пределах 10 мг/ дм^3 из- за малого содержания хлоридов не оказывает сильного влияния на коррозию, особенно в присутствии ингибиторов [1, 2].

Основной источник ионов железа в дренажных водах – это коррозия технологического оборудования (трубопроводов, емкостей). Агрессивная среда, содержащая хлориды, суль-

фаты и растворенные газы (CO_2, H_2S), приводит к переходу металлического железа (Fe^0) в растворимые формы Fe^{2+}/Fe^{3+}.

При отсутствии или малом содержании в нефти хлористых солей интенсивность коррозии снижается, т.к. защитная пленка из сульфида железа частично предохраняет металл от дальнейшей коррозии. Хлорид-ион, обладая малым радиусом и высокой проникающей способностью, адсорбируется на поверхности, внедряется в решетку и это приводит к локальному растворению защитной пленки и образованию точечных поражений.

В местах нарушения пленки обнажается чистое железо. Происходит анодная реакция:

$$Fe^0 \rightarrow Fe^{2+} + 2e^-.$$

Далее $FeCl_2$ взаимодействует с HCl с образованием $FeCl_3$, который диссоциирует на ионы железа и хлора.

Сероводород в сырой нефти в сочетании с хлористым водородом вызывает наиболее сильную коррозию оборудования, трубопроводов, механизмов [3]. Хлористое железо переходит в водный раствор, а выделяющийся сероводород вновь реагирует с железом:

$$Fe + H_2S = FeS + H_2 \qquad FeS + HCl = FeCl_2 + H_2S$$

Таким образом, при совместном присутствии в нефти хлоридов металлов и сероводорода во влажной среде происходит взаимно инициируемая цепная реакция.

Один из способов борьбы с коррозией – применение нейтрализаторов и ингибиторов.

Нейтрализатор (Геркулес 54505 марки А) способствует разрушению активных сернистых соединений. Он представляет собой концентрированный раствор аминов в ароматическом растворителе и предназначен для контроля pH в верхних потоках колонн и конденсационных системах установок первичной переработки нефти на нефтеперерабатывающих предприятиях. Нейтрализатор обладает высокой нейтрализующей способностью, что позволяет устойчиво удерживать уровень pH дренажной воды в узких пределах 5,5 - 6,5. Продукты нейтрализации не образуют отложений на поверхности металла. Дозировки реагента могут колебаться в пределах от 3 г/тонну до 20 г/тонну на нефтеперерабатывающих предприятиях. Подачу нейтрализатора рекомендуется осуществлять с помощью дозировочного насоса. Нейтрализатор в виде раствора через распределительно-дозировочное устройство подается в середину потока паров бензина в первую линию (по ходу паров в шлеме К-2) шлемовой трубы колонны К-2 и направляется навстречу потока паров.

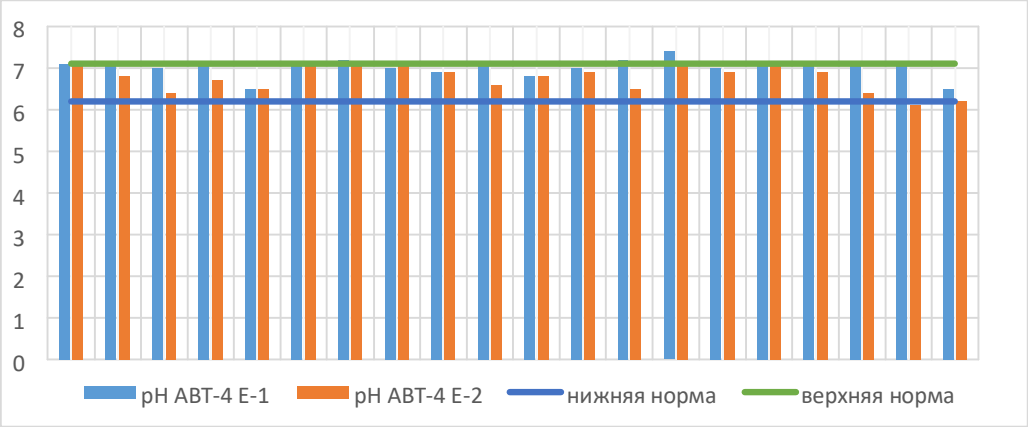
Ингибитор коррозии (Геркулес 30617 марки А) создает тонкую защитную пленку на внутренних поверхностях оборудования и препятствуют коррозионному разрушению металла. Он представляет собой специально подобранную комбинацию производных имидазолина в ароматическом растворителе. Ингибитор создает на поверхности металла защитную пленку за счет физической и химической адсорбции, и тем самым предохраняет металл от воздействия коррозионно- агрессивных компонентов технологических сред. Дозировки реагента могут колебаться в пределах от 3 г/тонна до 20 г/тонна на нефтеперерабатывающих предприятиях, и от 10 г/тонна до 200 г/тонна на нефте- и газовых промыслах. Ингибитор в виде раствора в бензине через распределительно-дозировочное устройство подается в середину потока паров бензина во вторую линию (по ходу паров в шлеме К-2) шлемовой трубы колонны К-2 и направляется навстречу потока паров.

Целью настоящей работы является изучение химического состава дренажной воды из сепараторов бензина Е-1 и Е-2 установки АВТ. Известно, что основная задача любого технологического процесса – это обеспечение качества получаемых продуктов при заданных параметрах, а также обеспечение устойчивой и безаварийной работы оборудования установки. Для этого чётко прописываются контролируемые параметры процесса. Одним из таких является аналитический контроль дренажных стоков [4, 5].

Поэтому для проведения исследования были выбраны следующие нормируемые в воде показатели: pH, Fe^{3+}, Cl^{-}, S^{2-}. Анализ химического состава дренажной воды проводился в зимний период работы установки АВТ-4: активность ионов водорода, pH и измерение концентрации растворенного железа определялись один раз в сутки, содержание сульфидной серы, мг/дм^3 1 раз в неделю, измерение концентрации хлорид-ионов 2 раза в месяц.

Измерение pH проводили с помощью pH-метра (5,5÷6,8). Измерение концентрации растворенного железа в дренажных водах технологических процессов фотометрическим методом (мг/дм^3, не более 1). Данный метод исследования включает следующие операции: минерализацию измеренного объема пробы (устранение мешающих влияний, к которым относятся разложение органических соединений, растворенного сероводорода, труднорастворимых комплексов железа путем выпаривания пробы со смесью соляной и азотной кислоты), связывание ионов железа в виде комплекса с сульфациловой кислотой, измерение оптической плотности окрашенного в желтый цвет раствора и вычисление результата измерений по градуировочной характеристике. Сущность метода определения сульфидной серы заключается в поглощении сероводорода водным раствором гидроксида натрия с последующим потенциометрическим титрованием образующегося сульфида щелочного металла азотнокислым аммиакатом серебра. Титрование проводится с помощью автоматического титратора. Определение сульфидной серы (мг/дм^3) не нормируется, но определение обязательно. Измерение концентрации хлорид-ионов (мг/дм^3, не более 25) определяют методом титрования предварительно отфильтрованной и подвергшейся кипячению пробы в присутствии перекиси водорода и гидроксида натрия. Титруют раствором азотнокислой ртути в присутствии смешанного индикатора (0,05 г дифенилкарбазона и 0,05 бромфенолового синего в 70 см^3 96%-ного этилового спирта).

Результаты измерений химического состава дренажной воды за определенный период 2017 и 2026 года представлены на рисунках 1-4.



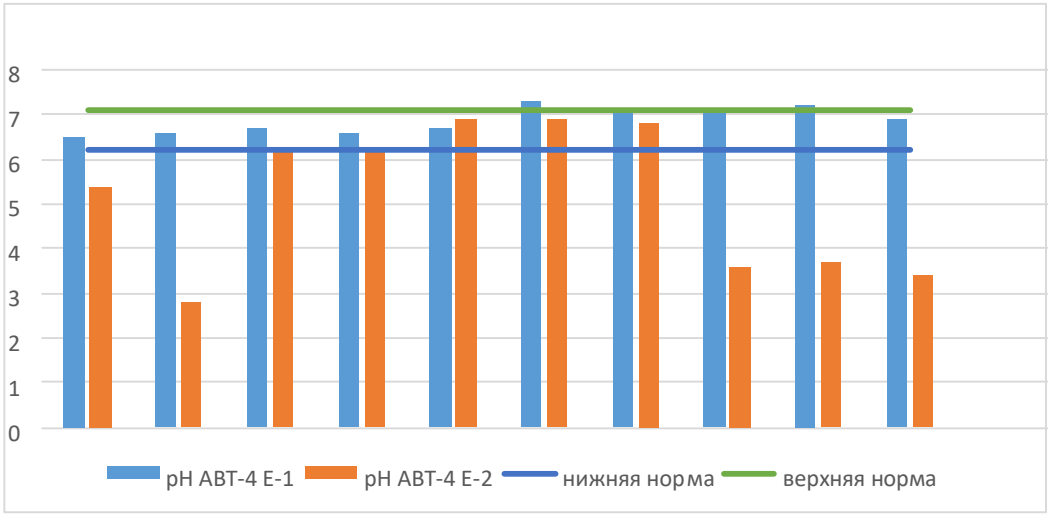
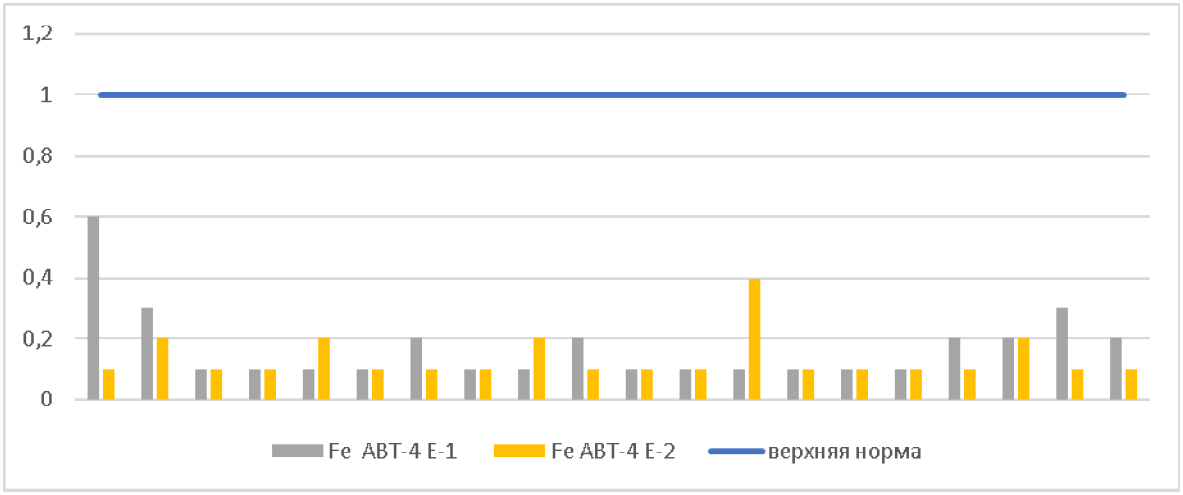


Рис. 1. Результаты измерений pH дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 и 2026 год
Нижняя норма pH- 6,2, верхняя норма pH -7,1



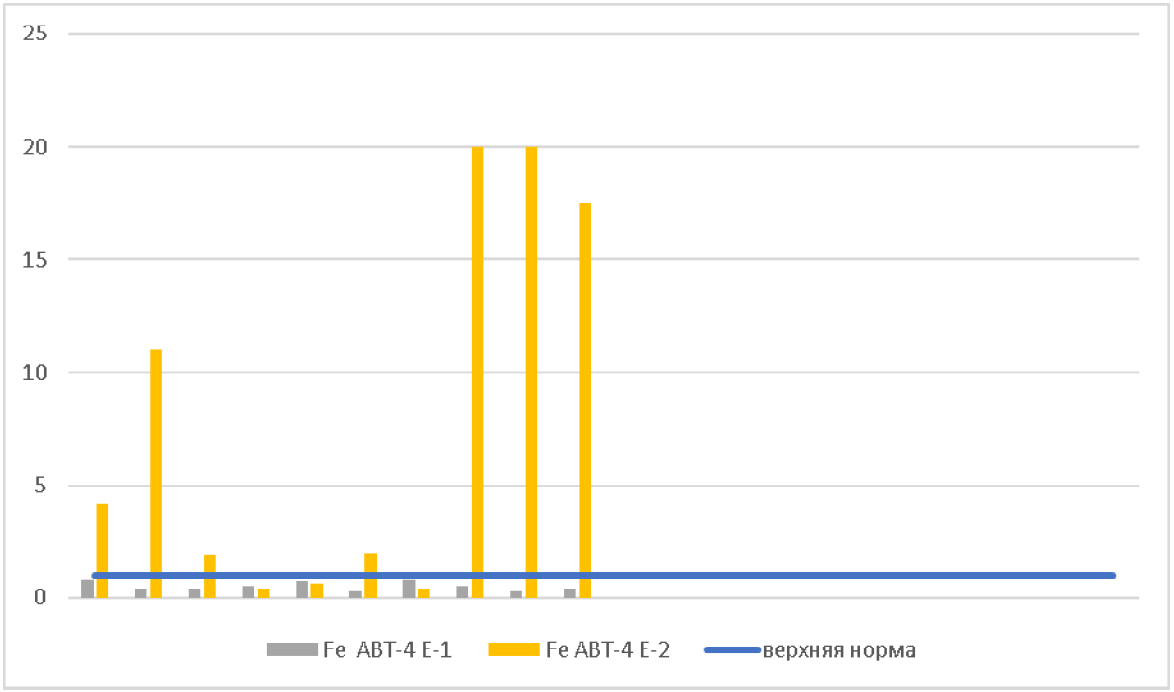
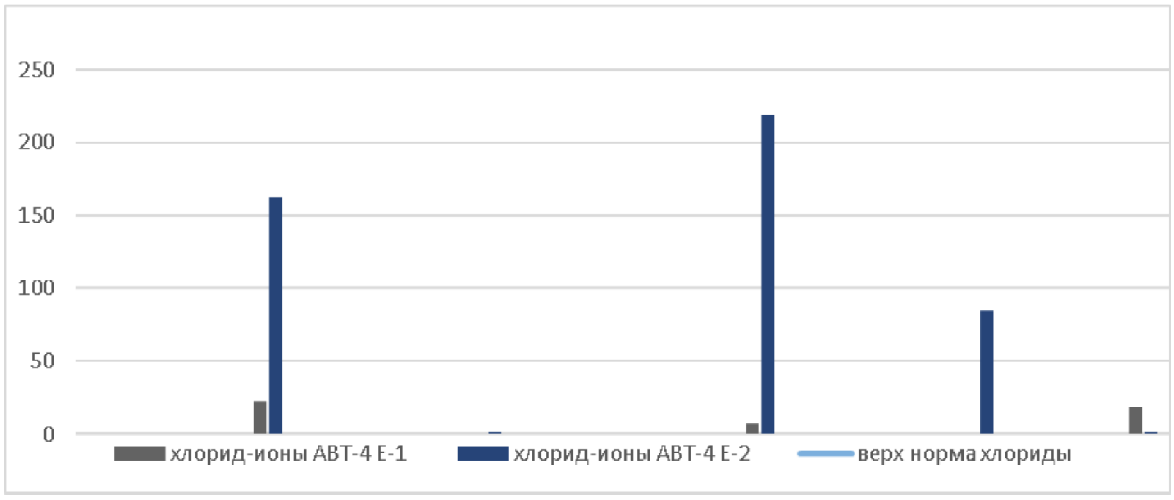


Рис. 2. Результаты измерений Fe^{3+} дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 и 2026 год



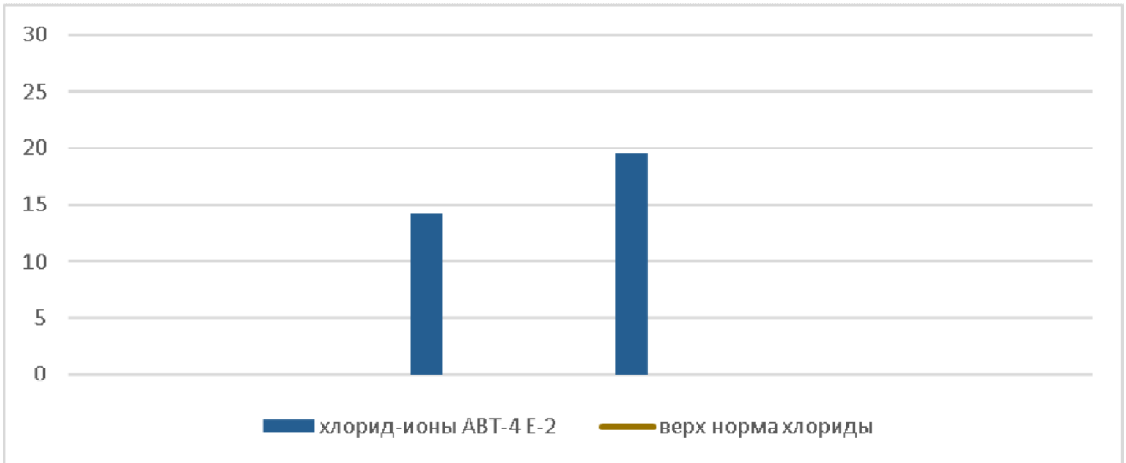
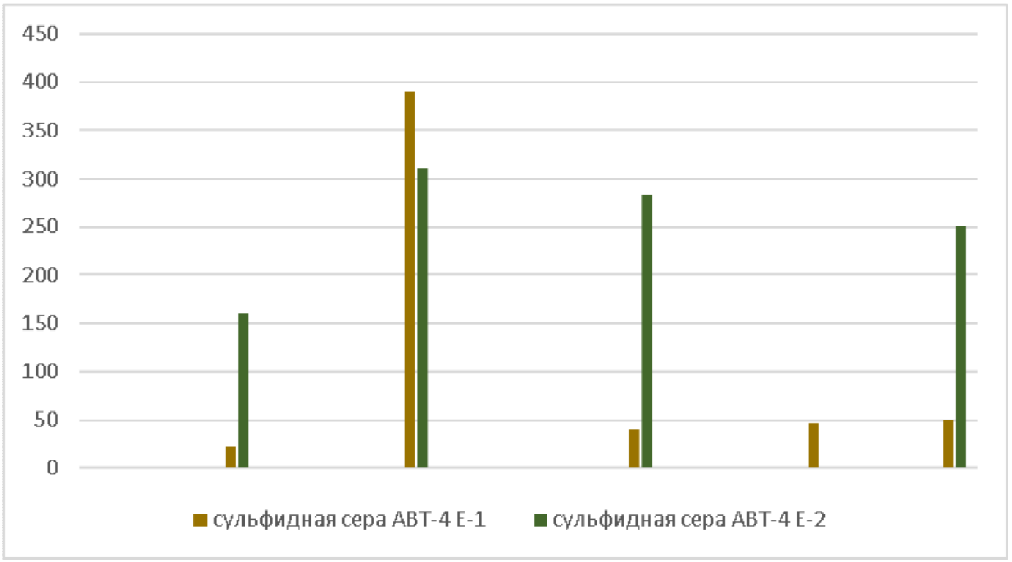


Рис. 3. Результаты измерений Cl^- дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 и 2026 год
верхняя норма Cl^- - не более 25 мг/дм^3



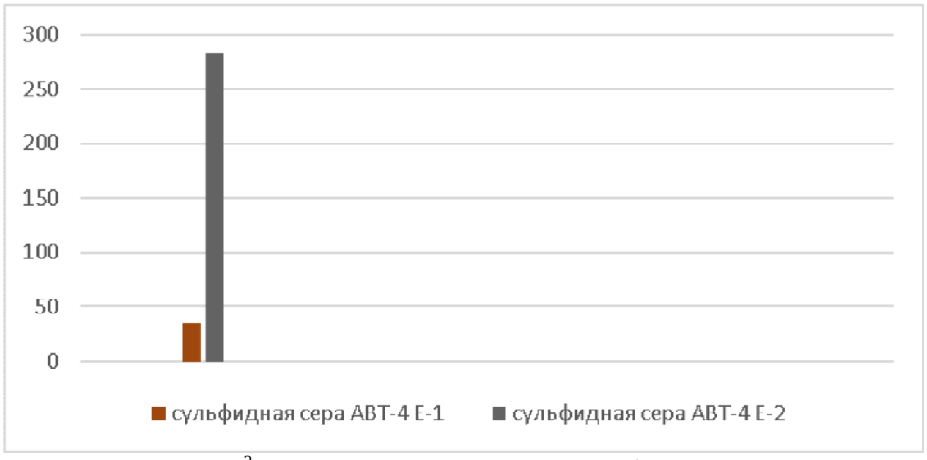


Рис. 4. Результаты измерений S^{2-} дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 и 2026 год

Анализ результатов исследования химического состава дренажной воды из сепараторов бензина Е-1 и Е-2 позволяет сделать следующие выводы.

1. Результаты измерений pH дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 находятся в пределах нормируемых показателей 6,2-7.6 для емкости Е-1 и 6,2 -7,1 для емкости Е-2. Это говорит о защитных функциях нейтрализатора и ингибитора коррозии, подаваемых в шлемовый трубопровод колонн К-1 и К-2, обеспечивающих защиту блока атмосферной перегонки нефти. Снижение показателя pH (2,8; 3,4; 3,6) за 2026 год в емкости Е-2 показывает на возможную аварийную ситуацию в блоке.

2. Результаты измерений Fe^{3+} дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 находятся в пределах нормы. Резкое увеличение содержания ионов железа (11, 17,5, более 20 мг/дм^3) при норме не более 1 мг/дм^3 в дренажной воде сепаратора Е-2 говорит либо о коррозии оборудования, либо связан с аварийным пуском и остановкой блока в 2026 году, либо с длительной эксплуатацией определенных узлов установки.

3. Результаты измерений Cl^- дренажной воды за 2017 из сепаратора бензина Е-1 находятся в норме - не более 25 мг/дм^3, в то время как результаты измерения хлоридов в емкости Е-2 за 2017 значительно превышают норму (163, 219 мг/дм^3). Это может быть связано с повышенным содержание хлорорганических соединений в нефти, которые не удалились на блоке ЭЛОУ, а в основной фракционирующей колонне К-2 произошло их разложение с образованием ионов хлора. При этом коррозии металла не наблюдается, либо она очень низ-

кая, так как содержание железа в дренажной воде Е-2 в норме. В 2026 году анализ хлоридов проводился только для емкости Е-2, показатели не превышают норму, что может быть связано с ужесточением требований к сырью по содержанию хлорорганики.

4. Результаты измерений S^{2-} дренажной воды из сепаратора бензина Е-1 и Е-2 за 2017 и 2026 год показывают, что в емкости Е-2 сульфидов в 5-8 раз больше, чем в емкости Е-1. Данные значения характеризуют хорошую работу нейтрализатора коррозии, поглощающего активные сернистые соединения, которые на фоне нормальной pH дренажной воды увеличивают содержание сульфидов в воде.

5. В качестве способа оптимизации проведения анализа можно предложить наряду с сокращением периодичности проведения анализов (2 раза в месяц определение концентрации хлорид-ионов, анализ сульфид-ионов только в емкости Е-2), использование поточного анализатора для определения pH и ионов железа. Примером такого прибора может быть поточный анализатор АкваТОС-К, предназначенный для колориметрического анализа качества воды (жесткость воды, содержание в воде железа, алюминия, никеля, хлора, аммиака нитритов, фосфатов, сульфидов и других веществ) [6]. Метод исследования: дифференциальная фотометрическая абсорбция. Это метод количественного анализа, основанный на измерении изменения оптической плотности раствора при взаимодействии аналитического вещества с реагентом или при изменении условий среды.

Библиографический список

1. Каландаров, Н. О. Защита от коррозии оборудования первичной подготовки нефти / Н. О. Каландаров. – Текст : непосредственный // Молодой ученый. – 2016. – № 9 (113). – С. 173-175. – URL: https://moluch.ru/archive/113/28513.

2. Кац, Н.Г. Химическое сопротивление материалов и защита оборудования нефтегазопереработки от коррозии: учебное пособие / Н.Г. Кац, В.П. Стариков, С.Н. Парфенов – Москва, Машиностроение, 2011г. – 436с.

3. Бауэр, А.А. Надежность трубопроводов, транспортирующих сероводородсодержащие среды: монография / А.А. Бауэр, В.М. Кушнаренко, А.Е. Пятаев, Ю.А. Чирков, Д.Н. Щепинов.– Оренбург: ОГУ, 2015г. – 592с.

4. Гоев, М.М, Модернизация технологии и оборудования процесса защелачивания обессоленной нефти, автореферат диссертации на соискание ученой степени кандидата технических наук, Москва-Кириши, 2012 г, – 27с.

5. Очистка пластовых вод [Электронный ресурс] - URL: https://ahmadullins.com/libraryw/plastovye-vody/ochistka-plastovyx-vod/?active_way=3#ways.

6. Поточный анализатор АкваТОС-К [Электронный ресурс] - URL: https://www.tocteh.ru/produkciya/analizatory-akvatos/potochnyj-analizator-akvatos-k/?ysclid=mm2fsud3tn598592027.

УДК 543.51; ГРНТИ 31.19.15

МОДЕЛИРОВАНИЕ ФРАГМЕНТАЦИИ ИОНОВ В ТАНДЕМНОМ КВАДРУПОЛЬНОМ МАСС-СПЕКТРОМЕТРЕ ПРИ РАБОТЕ ВО ВТОРОЙ ЗОНЕ ДИАГРАММЫ СТАБИЛЬНОСТИ

А.Д. Ветшева, М.В. Дубков

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, adr1999@list.ru

Аннотация. Проведено математическое моделирование процессов фрагментации ионов в тандемном квадрупольном масс-спектрометре при работе в области верхней вершины второй зоны диаграммы стабильности. Определены оптимальные значения углового коэффициента, при которых достигаются наилучшие аналитические характеристики. Исследовано влияние параметров работы фрагментационной ячейки на интенсивность сигнала, разрешение и добротность.

Ключевые слова: тандемная масс-спектрометрия, квадрупольный масс-анализатор, диаграмма стабильности, фрагментация ионов.

SIMULATION OF ION FRAGMENTATION IN A TANDEM QUADRUPOLE MASS SPECTROMETER OPERATING IN THE SECOND STABILITY REGION

A.D. Vetsheva, M.V. Dubkov
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, adr1999@list.ru

The summary. Mathematical modeling of ion fragmentation processes in a tandem quadrupole mass spectrometer operating in the region of the upper tip of the second stability region has been performed. Optimal values of the scan line parameter (angular coefficient) providing the best analytical characteristics have been determined. The influence of the fragmentation cell operating parameters on signal intensity, resolution, and figure of merit has been investigated.
Keywords: tandem mass spectrometry, quadrupole mass analyzer, stability diagram, ion fragmentation.

Тандемная масс-спектрометрия занимает ключевое место в современном химическом анализе. Она позволяет более точно и эффективно идентифицировать сложные структуры. Метод включает в себя три основные стадии:

- выделение ионов-предшественников;
- их последующая фрагментация;
- масс-анализ образовавшихся продуктов.

В настоящее время существует множество различных конфигураций тандемных масс-спектрометров. Широкое распространение благодаря своей надежности, компактности и универсальности получили квадрупольные анализаторы.

Работа квадрупольного масс-анализатора определяется условиями устойчивости колебаний ионов в высокочастотном электрическом поле. Математически движение ионов в идеальном квадрупольном поле описывается уравнением Матье, решения которого разделяются на области устойчивых и неустойчивых траекторий [1]. Диаграмма стабильности в координатах безразмерных параметров a и q графически отображает условия, при которых ионы способны проходить через анализатор, не сталкиваясь с электродами. Традиционно в масс-спектрометрии используется первая зона стабильности, расположенная вблизи начала координат ($a \approx 0$, $q \approx 0{,}709$). Однако существуют и более высокие области стабильности. Особый исследовательский интерес представляет вторая зона, характеризующаяся специфическими параметрами ионных траекторий. При работе во второй зоне стабильности представляется возможным проводить анализ ионов с повышенными энергиями и достичь высокого разрешения масс-анализа.

Ранее были проведены исследования фрагментации ионов в области нижней вершины второй зоны диаграммы стабильности [2]. Целью настоящей работы является математическое моделирование процессов фрагментации ионов в тандемном квадрупольном масс-спектрометре при работе в области верхней вершины второй зоны диаграммы стабильности.

Установлено, что в рассматриваемой области в квадрупольном масс-фильтре уменьшение углового коэффициента приводит к увеличению интенсивности и уменьшению показателей разрешающей способности и добротности. Зависимости представлены на рисунках 1 и 2.

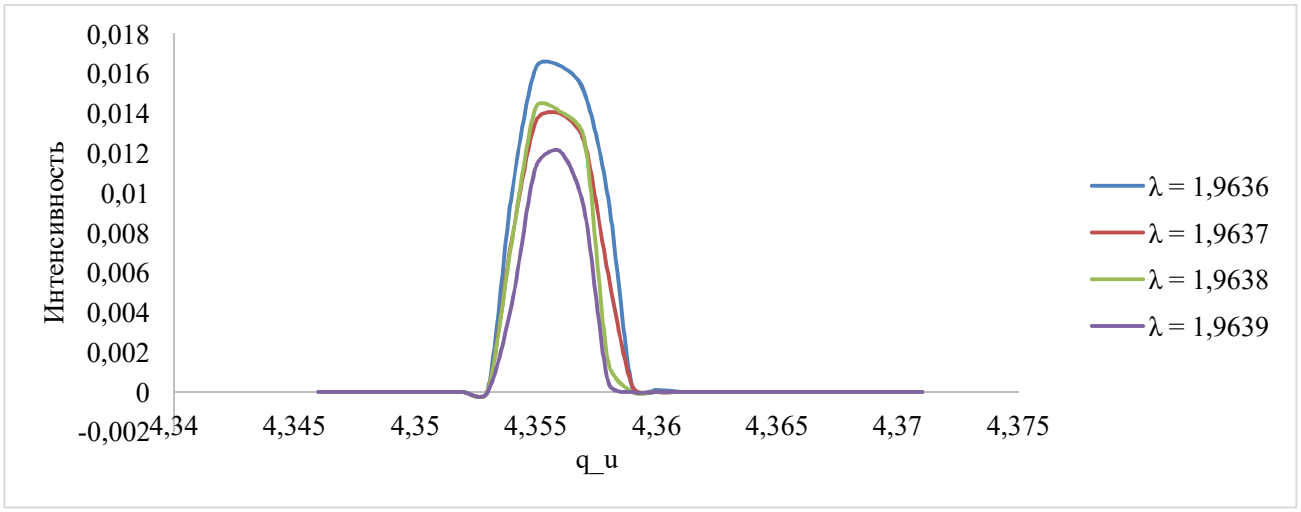


Рис. 1. Влияние углового коэффициента на форму и высоту массовых пиков при работе с одним квадрупольным масс-фильтром

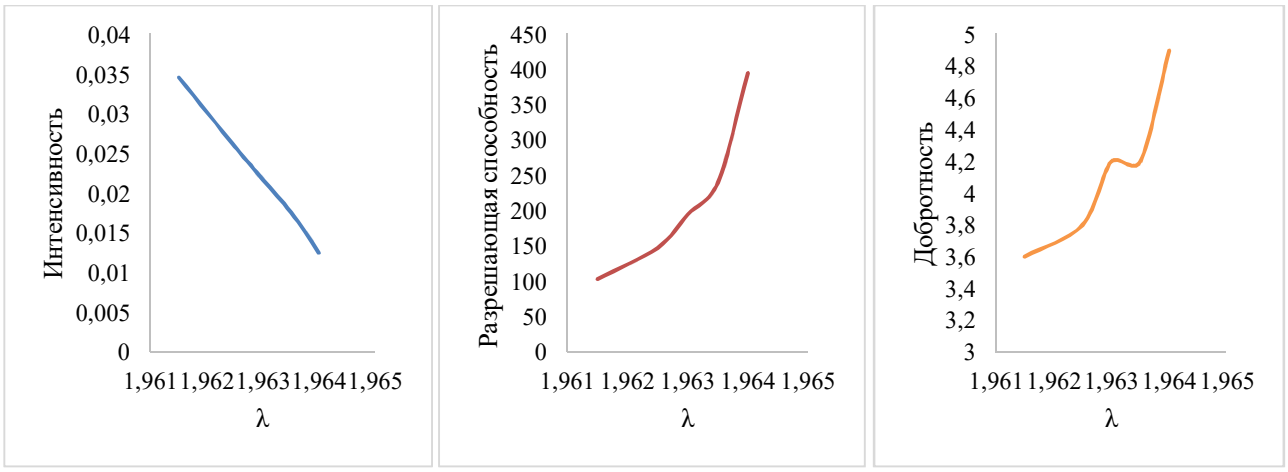


Рис. 2. Зависимости основных качественных характеристик от углового коэффициента при работе с одним квадрупольным масс-фильтром

Наиболее оптимальным значением углового коэффициента в данных условиях является λ = 1,9638. При таком параметре пролет ионов составляет порядка 1,43 %, разрешающая способность находится на уровне 300 единиц, добротность равна 4,4. Каскад из двух масс-фильтров позволяет повысить четкость получаемого массового пика и, как следствие, улучшает его основные качественные характеристики. В данном случае уменьшение углового коэффициента приводит к снижению разрешающей способности и добротности. Зависимости представлены на рисунках 3 и 4.

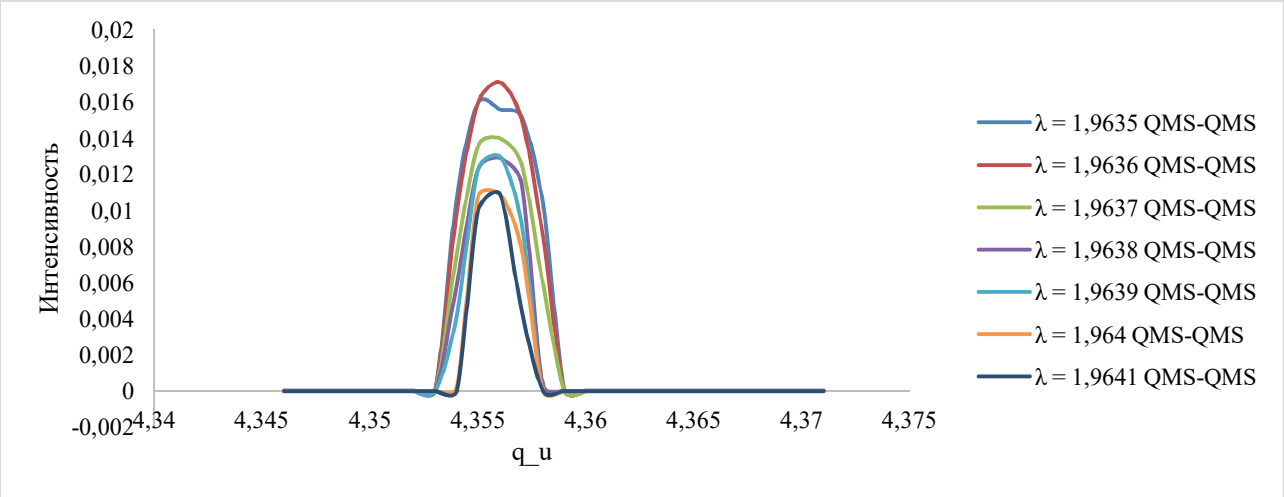


Рис. 3. Влияние углового коэффициента на форму и высоту массовых пиков при работе с тандемом из двух квадрупольных масс-фильтров

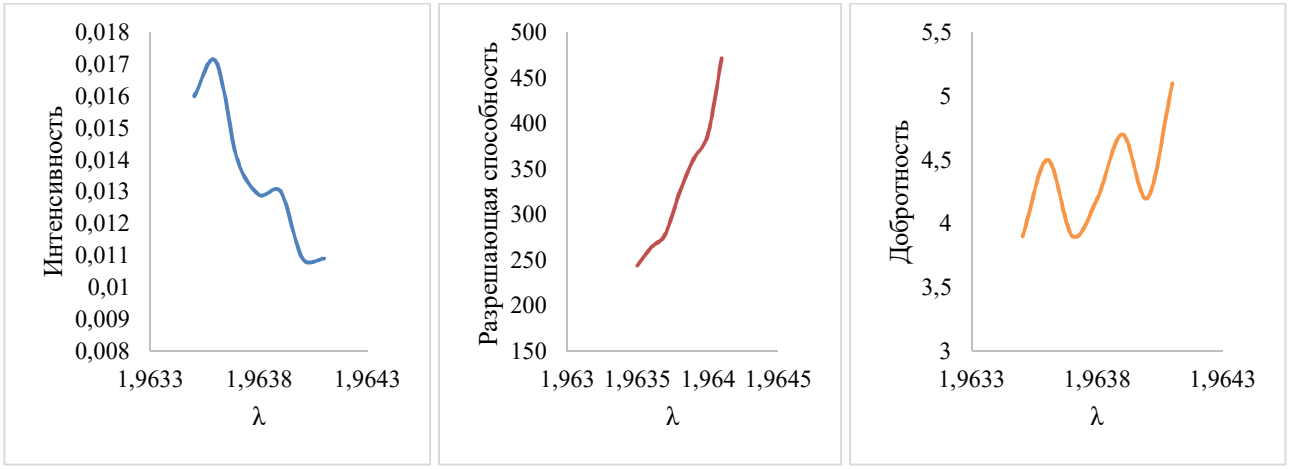


Рис. 4. Зависимости основных качественных характеристик от углового коэффициента при работе с тандемом из двух квадрупольных масс-фильтров

Наиболее оптимальным значением также является λ = 1,9638: пролет ионов составляет порядка 1,3 %, разрешающая способность находится на уровне 320 единиц, добротность равна 4,2. Таким образом, использование обсуждаемой конфигурации прибора с использованием двух последовательных масс-фильтров позволяет несколько увеличить разрешающую способность и чувствительность анализа при незначительных потерях интенсивности получаемых массовых пиков.

При внедрении в обсуждаемую конфигурацию ячейки фрагментации ионов, располагаемой посередине между первым и вторым квадрупольными масс-фильтрами, отмечается, что исходные зависимости сохраняются: уменьшение углового коэффициента приводит к снижению разрешающей способности и добротности. Оптимальным также принято прежнее значение λ = 1,9638. В работе моделируется фрагментация посредством электронного удара.

Можно отметить, что аналогично прошлым исследованиям, наилучшие аналитические показатели обеспечиваются при низком проценте фрагментации исходных молекул (порядка 5 %) и в условиях мягкой фрагментации (в диапазоне энергий 10-20 эВ). Однако жесткая фрагментация (в диапазоне энергий 30-50 эВ) в условиях низкой эффективности позволяет добиться более стабильных показателей. Таким образом, для практической работы в исследуемой области параметров целесообразно выбирать условия, обеспечивающие умеренную

фрагментацию, что позволяет сохранить баланс между чувствительностью и достоверностью идентификации соединений.

Для достижения оптимальных аналитических характеристик при работе в области верхней вершины второй зоны диаграммы стабильности целесообразно выбирать небольшую длину фрагментационной ячейки (до 30 мм) и использовать пониженное давление газа в ячейке соударений, что позволяет минимизировать неупорядоченное рассеяние ионов и сохранить достигнутые ранее показатели разрешающей способности (порядка 315 единиц) и добротности (порядка 5 единиц).

Установлено, что в качестве газа-бомбардировщика оптимально использовать аргон или гелий. Дальнейший выбор определяется приоритетом анализа: аргон обеспечивает более эффективную передачу энергии и, следовательно, большую глубину фрагментации, тогда как гелий предпочтителен в задачах, требующих максимального разрешения и минимального уширения пиков.

Таким образом, в результате моделирования определены рабочие параметры для тандемного квадрупольного масс-спектрометра при фрагментации ионов в области верхней вершины второй зоны диаграммы стабильности. Показано, что оптимальный угловой коэффициент составляет $\lambda = 1{,}9638$, а для сохранения разрешающей способности на уровне 300–320 единиц целесообразно использовать фрагментационную ячейку длиной до 30 мм с пониженным давлением газа-бомбардировщика. Полученные данные могут быть использованы при разработке режимов работы тандемных квадрупольных масс-спектрометров, эксплуатируемых во второй зоне диаграммы стабильности.

Библиографический список

1. Дубков М.В., Ветшев К.А., Рубцова А.Д. Расчет формы массового пика посредством метода Рунге-Кутты для решения задач аналитической химии // Современные технологии в науке и образовании – СТНО-2023 : сборник трудов VI Международного научно-технического форума : в 10 т. / под общ. ред. О.В. Миловзорова. – Рязань : Рязан. гос. радиотехн. ун-т, 2023. – Т. 3. – С. 28–31.

2. Ветшева А.Д., Ветшев К.А., Дубков М.В. Моделирование работы фрагментационной ячейки в тройном квадрупольном тандемном масс-спектрометре в нижней точке диаграммы стабильности // Двенадцатый съезд ВМСО. XI Всероссийская конференция с международным участием «Масс-спектрометрия и ее прикладные проблемы» : сборник тезисов, 13–17 октября 2025 г., г. Москва. – Москва, 2025. – С. 145.

УДК 620.193; ГРНТИ 81.33

ИССЛЕДОВАНИЕ КОРРОЗИОННОЙ СТОЙКОСТИ ЦИНКОВЫХ ПОКРЫТИЙ

О.А. Родионова, А.Д. Ветшева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, olyaradio05@mail.ru

Аннотация. В работе рассмотрены режимы гальванического цинкования и их влияние на коррозионную стойкость защитных покрытий. Приведены особенности электроосаждения цинка в сернокислом электролите. Рассмотрены различные режимы нанесения покрытия. Проведены коррозионные испытания в 5%-ном растворе хлорида натрия с оценкой изменения массы. Установлена зависимость коррозионной стойкости покрытий от режима цинкования.

Ключевые слова: цинкование, цинковые покрытия, электроосаждение, коррозионная стойкость, режимы цинкования.

INVESTIGATION OF CORROSION RESISTANCE OF ZINC COATINGS

O.A. Rodionova, A.D. Vetsheva
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, olyaradio05@mail.ru

The summary. The paper discusses the modes of galvanic zinc plating and their effect on the corrosion resistance of protective coatings. It presents the features of zinc electrodeposition in a sulfuric acid electrolyte. Various coating modes are considered. Corrosion tests were conducted in a 5% sodium chloride solution to assess the change in mass. The dependence of the corrosion resistance of coatings on the zinc plating mode was established.
Keywords: galvanization, zinc coatings, electrodeposition, corrosion resistance, galvanization modes.

Цинк является химически активным металлом, способным образовывать устойчивые соединения с кислородом. Благодаря этому свойству его часто используют в гальванике в качестве коррозионностойкого защитного покрытия. Основной недостаток цинкования заключается в высокой пористости образующегося осадка. Кроме того, длительное воздействие повышенной влажности и хлорид-ионов ведет к утрате защитных свойств и появлению продуктов коррозии самого цинка.

Технологии нанесения цинка на металлические поверхности различаются по способу обработки и итоговым характеристикам изделия. Наиболее распространенные методы представлены ниже.

Метод горячего цинкования предполагает погружение детали в расплавленный цинк. Такая технология позволяет добиться покрытия, обладающего высокой стойкостью к коррозии. Однако излишнее тепловое воздействие может вызвать деформацию обрабатываемого элемента [1].

В основе метода холодной оцинковки лежит нанесение специального состава, на 92–96% состоящего из цинкового порошка. Данный процесс похож на обычную покраску: состав наносится кистью, валиком или распылителем на предварительно загрунтованную поверхность [2]. Таким образом, основным достоинством метода является его простота, однако срок службы защитного покрытия, нанесенного обсуждаемым способом, значительно уступает другим видам цинкования.

При термодиффузионном цинковании деталь нагревается в герметичной емкости вместе с цинкосодержащей порошковой смесью. В результате высокотемпературного воздействия происходит диффузия цинка в материал покрываемой детали, в результате чего формируется прочное и однородное покрытие, характеризующееся высокой степенью адгезией [1]. К недостаткам технологии можно отнести ее высокую себестоимость и невозможность обработки крупногабаритных конструкций.

Газотермическое напыление заключается в подаче расплавленных частиц цинка на обрабатываемую поверхность с помощью высокотемпературной газовой или плазменной струи [2]. Эта технология обеспечивает равномерность слоя, но связана с перерасходом материала из-за его распыления и потерь в процессе нанесения.

Одним из самых распространённых видов цинкования является гальваническое. Используется электролитический раствор, который заливается в гальваническую ванну. Данный метод предполагает использование электродной пары – катода и анода. В качестве катода выступает деталь, подлежащая защите, в качестве анода – цинковая пластина. При пропускании электрического тока через электролитическую систему цинк растворяется в электролите, а его ионы равномерно оседают на поверхности детали [3]. Достоинствами данного метода являются высокая производительность, эстетичный внешний вид самого покрытия, сравнительная простота технологии. Недостатки – вредное воздействие на окружающую среду, склеивание деталей, метод не подходит для крупногабаритных изделий.

В данной работе для исследования коррозионной стойкости цинкового покрытия в рамках лабораторного исследования был выбран гальванический способ цинкования.

Покрытие наносилось на три стальные пластины, которые предварительно были подвергнуты механической зачистке, обезжириванию и травлению. Обезжиривание проводилось по 3 минуты в щелочном растворе при использовании в качестве анода стального стрежня. Сила тока составила 0,5 А. Далее проводилось химическое травление с использованием раствора серной кислоты в течение 10 минут.

Экспериментальная установка состояла из источника питания, химического стакана объёмом 250 мл, пары электродов – стального анода и стальной пластины в качестве катода. В работе был использован стандартный электролит, содержащий цинк сернокислый с концентрацией 250 г/л и алюминий сернокислый с концентрацией 30 г/л [3].

Схематическое изображение установки представлено на рисунке 1.

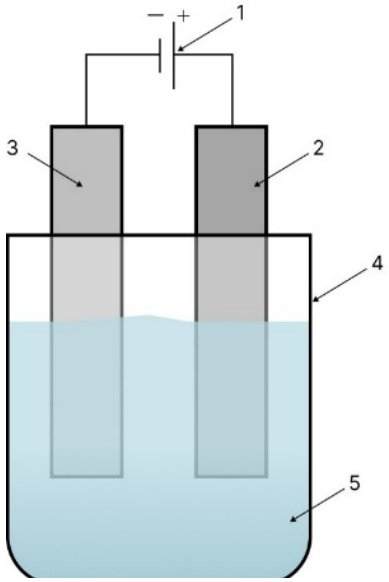


Рис. 1. Схема установки для нанесения цинкового покрытия (1 – источник питания, 2 – стальной анод, 3 – стальной катод, 4 – электролизёр, 5 – электролит)

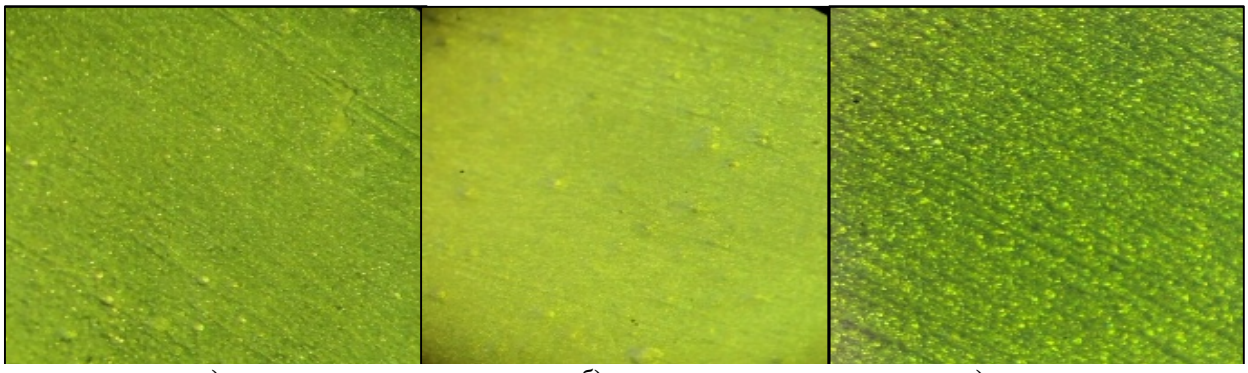
Для образцов были выбраны разные режимы цинкования. Первая пластина покрывалась на протяжении 10 минут при малой, относительно стандартного значения, величине силы тока (0,5 А), 5 минут при стандартной величине силы тока (2,5 А). Электроосаждение второй пластины проводилось в стандартом режиме 15 минут. Электроосаждение третей пластины проводилось в режиме скачка тока: при повышенном значении силы тока (3 А) на протяжении 30 секунд, 15 минут при стандартной величине силы тока.

Первоначальная визуальная оценка показала, что покрытие первой пластины неплотное, при цинковании второй пластины образовалось большое количество дендритов. Покрытие третей пластины равномерное, с меньшим количеством дендритов (по сравнению со вторым образцом).

Далее представлены изображения пластин, полученные с помощью микроскопа, на рисунке 2.

При рассмотрении данных изображений покрытий видно, что покрытие третьей пластины получилось более равномерное, плотное, без непрокрытых участков. Его структура свидетельствует о наличии большего количества кристаллизационных центров, что объясняется выбором нестационарного режима проведения электроосаждения. Первое и второе покрытия выглядят менее плотными. На них также можно заметить участки «пузырения». Это,

вероятно, связано с более интенсивным выделением водорода на катоде в конкуренции с осаждением цинка, что характерно для данных режимов.



а) б) в)

Рис. 2. Цинковые покрытия первой (а), второй (б) и третьей (в) пластины

Далее были проведены испытания полученных цинковых покрытий на коррозионную стойкость. Для исследования использовался раствор хлорида натрия с массовой концентрацией 5 %, в который погружались испытуемые пластины. Ежедневно в течение трех суток проводился анализ потери массы. Внешний вид пластин по прошествии указанного времени представлен на рисунке 3.

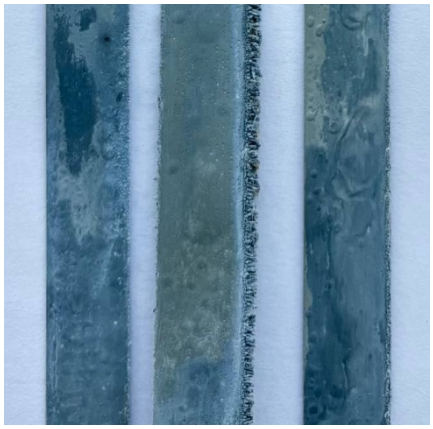


Рис. 3. Изменённые под воздействием раствора хлорида натрия цинковые покрытия первой, второй и третьей пластины соответственно

На рисунке видно, что непокрытые части платин почернели, появился белый налёт. На покрытиях появились пятна, в некоторых местах покрытие вздулось.

Результаты испытаний на коррозионную стойкость представлены в таблице 1.

Таблица 1 – Результаты испытания на коррозионную стойкость

№ пластины	Масса пластины до испытания, г	Масса пластины после испытания, г	Изменение массы, г	Характер коррозии
1	2,7582	2,7473	0,0109	Преимущественно равномерная, с локальными поверхностными очагами
2	3,8937	3,8821	0,0116	Локализованная (очаговая), с признаками более интенсивного разрушения покрытия
3	2,9255	2,9182	0,0073	Преимущественно поверхностная, местами неравномерная, без ярко выраженных глубоких очагов разрушения.

Исходя из полученных результатов, можно сделать следующие выводы:

1. Наименьшая потеря массы зафиксирована для пластины №3, покрытие которого было получено в нестационарном режиме. Это свидетельствует о более высокой коррозионной стойкости данного покрытия по сравнению с другими пластинами.

2. Пластина №2, осажденная в стандартном гальваностатическом режиме в течение 15 минут, показала наибольшую потерю массы и локализованный характер коррозии с признаками интенсивного разрушения. Вероятно, это связано с формированием менее плотной и более дефектной (дендритной) структуры покрытия.

3. Пластина №1, несмотря на минимальное время осаждения и низкую плотность тока, продемонстрировала промежуточный результат по потере массы. Характер коррозии преимущественно равномерный, что может указывать на меньшую толщину покрытия, но относительно равномерное растворение поверхности.

В ходе выполнения работы было исследовано влияние различных режимов гальванического цинкования на коррозионную стойкость формируемых покрытий. Экспериментально установлено, что режим электроосаждения оказывает существенное влияние на структуру и защитные свойства цинковых покрытий. Наилучшие результаты по комплексу характеристик (равномерность покрытия, минимальные коррозионные повреждения и наименьшая потеря массы в ходе испытаний) показала пластина, оцинкованная в нестационарном режиме скачка тока. Формирование более плотной мелкокристаллической структуры в данном режиме обеспечивает эффективное торможение коррозионных процессов в 5%-ном растворе хлорида натрия.

Таким образом, применение нестационарных режимов электролиза является перспективным направлением повышения эксплуатационных свойств гальванических цинковых покрытий. Для получения более достоверных данных о долговечности покрытий целесообразно проведение дальнейших исследований с увеличением продолжительности коррозионных испытаний и применением электронно-микроскопического анализа структуры осадков.

Библиографический список

1. Полькин И. В Цинк для защиты от коррозии // Строительные технологии и материалы. - 2019. - С. 86-89.

2. Асталюхина А.С., Пикалов Е.С. Характеристика современных методов нанесения защитных цинковых покрытий // Успехи современного естествознания. - 2015. - №11. - С. 11-14.

3. Ямпольский А.М., Ильин В.А. Краткий справочник гальванотехника. - 1962. - 244 с.

УДК 543.51; ГРНТИ 31.19

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПАРАМЕТРОВ ВХОДНОЙ АПЕРТУРЫ НА АНАЛИТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ТРИПОЛЬНОГО МАСС-АНАЛИЗАТОРА

М.В. Дубков, К.А. Ветшев

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, dubkov.m.v@rsreu.ru, vetshev.k.a@rsreu.ru

Аннотация. В исследовании рассматривается, как смещение всей электродной системы, включая уголковый электрод, влияет на эффективность прохождения ионов в трипольном масс-анализаторе при импульсном питании. Эксперимент был проведен в четыре этапа с разными уровнями смещения: 0, 3, 6 и 12 единиц. Результаты показывают, что даже небольшие отклонения - более 3 единиц - могут заметно снизить пропускную способность ионов. А при смещении более 6 единиц эффективность прохождения ионов резко падает.

Это лишний раз подчеркивает важность точного контроля над геометрией системы в современных трипольных масс-анализаторах.

Ключевые слова: трипольный масс-анализатор, входная апертура, массовый пик, разрешающая способность, интенсивность массового пика.

STUDY OF THE INFLUENCE OF ENTRANCE APERTURE PARAMETERS ON THE ANALYTICAL CHARACTERISTICS OF A THREE-POLE MASS ANALYZER

M.V. Dubkov, K.A. Vetshev

Ryazan State Radio Engineering University named after V.F. Utkin,
Russian Federation, Ryazan, dubkov.m.v@rsreu.ru, vetshev.k.a@rsreu.ru

Abstract. This study examines how the offset of the entire electrode system, including the corner electrode, affects the ion transmission efficiency of a tripole mass analyzer under pulsed power supply. The experiment was conducted in four stages with different offset levels: 0, 3, 6, and 12 units. The results show that even small offsets—more than 3 units—can significantly reduce ion transmission. And with an offset greater than 6 units, ion transmission efficiency drops sharply.This further emphasizes the importance of precise control over the system geometry in modern tripole mass analyzers.

Keywords: tripole mass analyzer, input aperture, mass peak, resolving power, mass peak intensity.

Масс-спектрометрический анализ остаётся одним из самых универсальных и мощных инструментов для детального изучения химического состава веществ. Его широкое применение охватывает химические, биохимические, медицинские и другие области исследований, где важны точность и чувствительность измерений. Метод основан на принципе измерения отношения массы к заряду (m/z) ионов, образовавшихся в результате ионизации молекул. Полученные ионы направляются в аналитор, где их разделяют по m/z с помощью различных приборов, таких как квадрупольные, ионные ловушки, ионные линзы и матричные аналоги. На выходе анализатора ионы фиксируются детекторами, которые преобразуют их в электрический сигнал. Этот сигнал позволяет построить спектр. Анализируя полученный спектр, можно с высокой точностью определить химический состав образца. Масс-спектроскопия обеспечивает высокую чувствительность, хорошую воспроизводимость результатов и возможность идентификации даже низкоконцентрированных компонентов в сложных смесях [1].

В последние годы наблюдается значительный рост возможностей масс-спектрометрии благодаря новым методам ионизации, таким как матрично-активная лазерная десорбция/ионизация (MALDI) и электроспрей-ионзация (ESI). Эти технологии позволяют анализировать более крупные биомолекулы, включая белки, нуклеиновые кислоты и сложные липиды. Современные приборы обладают высокой разрешающей способностью. Например, использование высокоразрешающих квадрупольных или ионных ловушек повысило точность и чувствительность измерений.

Интеграция масс-спектрометрии с хроматографическими методами, такими как жидкостная хроматография (HPLC) и газовая хроматография (GC), стала стандартом для анализа сложных смесей. Это привело к более эффективному разделению компонентов перед их ионизацией. Новейшие автоматизированные системы ускоряют процесс анализа, уменьшают влияние человека и повышают воспроизводимость результатов.

Несмотря на эти достижения, остаётся множество неизученных параметров, влияющих на эффективность и точность измерений. Одним из перспективных направлений является развитие трипольных анализаторов. Благодаря своей уникальной конструкции они демонстрируют хорошую разрешающую способность и чувствительность. Однако, их изучение остаётся менее полным по сравнению с квадрупольными системами. На рисунке 1 показана электродная конфигурация исследуемого масс-анализатора [2].

Таким образом, дальнейшее исследование и оптимизация параметров масс-спектрометрических систем, включая трипольные анализаторы, являются ключевыми для расширения их применения и повышения эффективности в различных областях науки и техники [3].

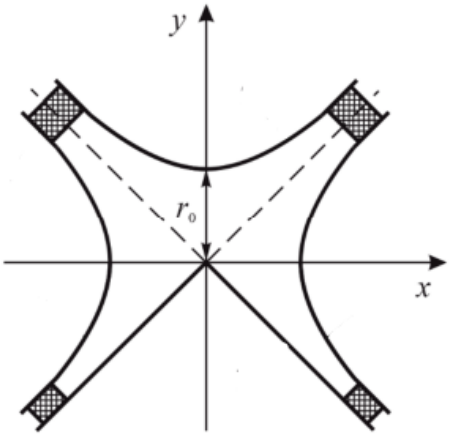


Рис. 1. Конфигурация электродов трипольного анализатора масс с уголковым электродом

Для моделирования системы, применяемой в данном исследовании, задаются исходные значения, представлены в таблице 1. Питание системы – импульсное. Начальные фазы и координаты ионов задаются случайным образом[4].

Таблица 1. Начальные условия системы

Параметр	Значение
Напряжение U_1	60,75 В
Напряжение U_2	39,25 В
Частота f	0,5626 МГц
Радиус отверстия ввода ионов r_0	0,1
Количество вводимых ионов	20000
Форма отверстия ввода ионов	Овальная вытянутая по оси OX

Изначально входная диафрагма располагалась вплотную к электродной системе. В данном исследовании было изучено влияние сдвига всей электродной системы, включая уголковый электрод, от диафрагмы.

Изначально для сдвига была выбрана велична в 3 ед. При такой конфигурации процент пролетевших ионов получился 21,6%, что достаточно близко к значению системы при исходной конфигурации (22,7%).

Далее величну сдвига увеличили до 6 ед, что привело к снижению колчества пролетевших ионов до значения 11,7%. В таком случае наблюдается примерно двухкратное ухудшение анализируемых характеристик системы, что уже является критичным.

Для финальной проверки был выбран отступ в 12 ед, при этом было получено знаечние процента пролетевших ионов равное 2,3%. Подобное изменение системы приводит к снижению пролета ионов более чем в 10 раз, что категорически неприемлимо.

На рисунке 2 показаны результаты исследования представленные в виде графика зависимости процента пролетевших ионов от величины сдвига электродной системы.

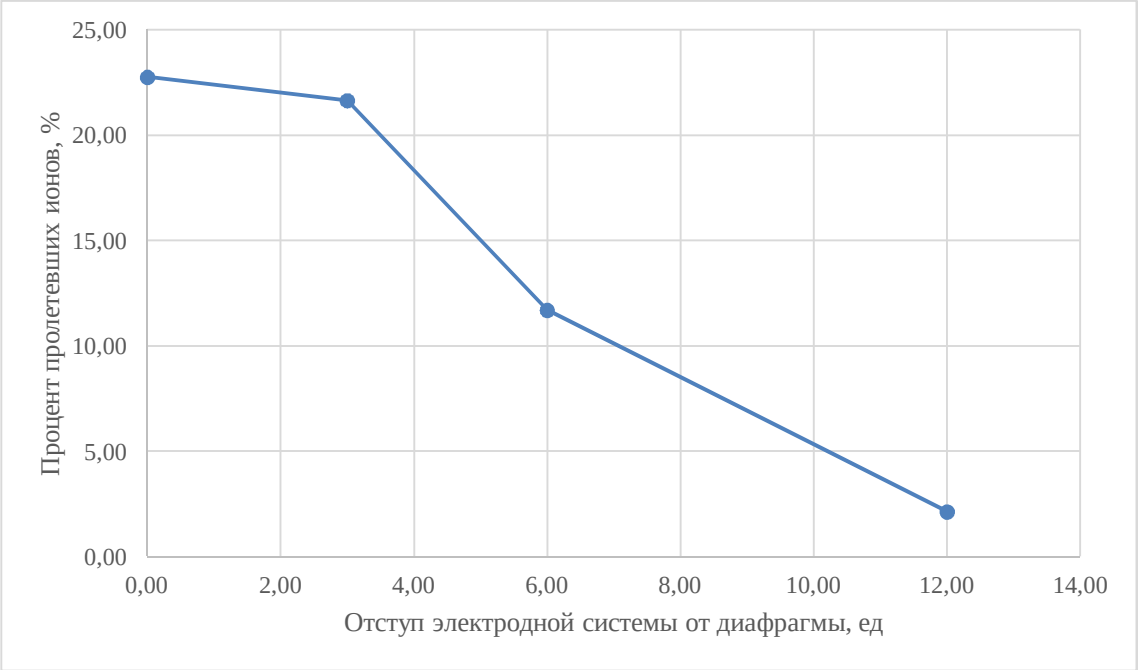


Рис. 2. График зависимости процента пролетевших ионов от величины сдвига электродной системы от входной апертуры

В исследовании было показано, что при импульсном питании и исходных условиях системы процент пролетевших ионов в базовой конфигурации составляет 22,7 %. Если набор электродов сдвинуть на три единицы, процент пролетевших ионов, снижается до 21,6 %. Это изменение не очень заметно по сравнению с исходным значением. Однако когда электроды сдвигаются на шесть единиц, процент пролетевших ионов, падает до 11,7%. Это означает, что система работает почти вдвое хуже, и это уже критично. Если электроды сдвинуть на 12 единиц, процент ионов, которые пролетают, опускается до 2,3%. Это более чем в десять раз хуже исходного значения, и система становится непригодной для использования.

Таким образом, сдвиги в расположении электродов на более чем три единицы, могут привести к значительному снижению эффективности системы. В реальных системах часто невозможно расположить электроды идеально без каких-либо отступов. Это исследование показывает, что если сдвиги небольшие, эффективность системы должна остаться примерно на том же уровне или снизиться лишь немного.

Библиографический список

1. Слободенюк Г. И. Квадрупольные масс-спектрометры. М.: Атомиздат, 1974. 272 с

2. Шеретов Э. П., Дубков М. В., Карнав Т. Б., Иванов В. В. и др. Триполь (фильтр масс с уголковым электродом) // Тезисы II съезда ВМСО «Масс-спектрометрия и ее прикладные проблемы». Москва. 2005. С. 189.

3. Дубков М.В., Буробин М.А., Иванов В.В., Ветшев К.А., Рубцова А.Д. Влияние условий ввода заряженных частиц на аналитические характеристики трипольного масс-анализатора // Вестник Рязанского государственного радиотехнического университета. 2024. № 90. С. 144-152.

4. Дубков М.В., Буробин М.А., Иванов В.В., Ветшев К.А., Ветшева А.Д. Влияние формы входной апертуры на аналитические характеристики трипольного масс-анализатора //Вестник Рязанского государственного радиотехнического университета. 2025. №94. С. 158-165.

УДК 543.062; ГРНТИ 31.19.15

ДОСТУПНАЯ СПЕКТРОСКОПИЯ: АНАЛИЗ СОВРЕМЕННЫХ КОНСТРУКТОРСКИХ РЕШЕНИЙ ДЛЯ СОЗДАНИЯ МАЛОБЮДЖЕТНЫХ ПОРТАТИВНЫХ СПЕКТРОМЕТРОВ

К.А. Ветшев, В.В. Максимов, Г.Д. Онофраш

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, vetshev.k.a@rsreu.ru

Аннотация. Эта статья посвящена анализу современных конструкторских решений для недорогих портативных спектрометров, которые предназначены для использования вне лабораторий. В статье рассматриваются три основных типа спектрометров: щелевые, безщелевые и смартфон интегрированные системы. Оцениваются компромиссы между стоимостью, размерами и точностью этих устройств, включая разрешение, точность калибровки, динамический диапазон и уровень шума. Массовое производство оптических и электронных компонентов, таких как камеры смартфонов, позволяет снизить стоимость спектрометров. Однако это требует более сложной программной обработки и точной калибровки для обеспечения точных результатов. Исследование подтверждает, что доступная спектроскопия имеет большую перспективу, но для повышения точности без увеличения затрат необходимо провести дальнейшую оптимизацию оптических схем и алгоритмов калибровки.

Ключевые слова: спектроскопия, конструкционные решения, портативный

AFFORDABLE SPECTROMETRY: ANALYSIS OF MODERN DESIGN SOLUTIONS FOR CREATING LOW-COST, PORTABLE SPECTROMETERS

K.A. Vetshev, V.V. Maksimov, G.D. Onofrash

Ryazan State Radio Engineering University named after V.F. Utkin, Russian Federation, Ryazan, vetshev.k.a@rsreu.ru

Abstract. This article analyzes current design solutions for low-cost portable spectrometers intended for use outside the laboratory. Three main types of spectrometers are considered: slit, slitless, and smartphone-integrated systems. The tradeoffs between cost, size, and accuracy of these devices are assessed, including resolution, calibration accuracy, dynamic range, and noise level. Mass production of optical and electronic components, such as smartphone cameras, allows for a reduction in the cost of spectrometers. However, this requires more complex software processing and precise calibration to ensure accurate results. The study confirms that accessible spectroscopy holds great promise, but further optimization of optical circuits and calibration algorithms is necessary to improve accuracy without increasing costs.

Keywords: spectrometry, design solutions, portable.

Спектроскопия уже несколько десятилетий является одним из основных методов исследования веществ в физике, химии, медицине, экологии и материаловедении. Обычные спектрометрические системы, используемые в лабораториях, дают очень точные результаты, но они дорогие, большие и потребляют много энергии, что ограничивает их использование вне специализированных исследовательских центров. Сейчас есть большая потребность в быстрой диагностике, мониторинге окружающей среды, образовательных технологиях и мобильных аналитических платформах, поэтому разработка доступных и портативных спектрометров очень важна.

За последние годы развитие микроэлектроники, оптоэлектронных компонентов и 3D-печати привело к созданию компактных спектрометрических решений. Эти решения используют миниатюрные дифракционные решётки, светодиодные источники света и могут работать с мобильными устройствами. Использование смартфонов как детекторов и вычислительных модулей привело к появлению нового направления – доступной спектроскопии. Эти системы используются не только в образовательных проектах, но и в задачах контроля качества продукции, агрохимического анализа и быстрой оценки состояния окружающей среды.

Несмотря на большой интерес к этой теме, вопросы оптимизации конструктивных решений доступных спектрометров еще недостаточно изучены. Необходим комплексный анализ того, как тип оптической схемы, характеристики детектора, качество калибровки и

алгоритмы обработки сигнала влияют на метрологические параметры прибора, такие как спектральное разрешение, точность определения длины волны, динамический диапазон и уровень шума.

Цель этой работы – проанализировать современные конструктивные решения, используемые при создании доступных и портативных спектрометров, и выявить компромиссы между стоимостью, размерами и функциональными характеристиками устройств. В рамках исследования рассматриваются различные подходы и компоненты, используемые для сборки портативных спектрометров при минимизации затрат. Результаты этого исследования могут быть использованы при разработке доступных спектрометрических систем для образовательных и прикладных задач.

Современные исследования в области спектроскопии показывают, что есть большой интерес к созданию недорогих и портативных решений. Обычно спектрометры – это большие приборы с точной оптикой и дорогими компонентами, что ограничивает их использование вне лабораторий. Однако в последние десятилетия учёные активно работают над миниатюризацией оптики и цифровых компонентов, чтобы создать дешёвые и компактные спектрометры, которые можно использовать в полевых условиях и в образовательных целях.

Многие исследователи подчёркивают, что доступность спектрометрии - это не только снижение стоимости, но и сохранение метрологических характеристик, которые необходимы для практических задач анализа. Существуют обзоры, которые сравнивают различные применения таких приборов – от мониторинга сельского хозяйства до диагностики материалов.

В области доступной спектроскопии выделяются три основных направления:

1. Щелевые спектрометры на базе дифракционных решёток – это классическая схема, которая использует дешёвые решётки и узкие щели для формирования спектра. Такие конструкции имеют лучшую спектральную разрешающую способность по сравнению с безщелевыми решениями, но требуют более точной механической настройки.

2. Безщелевые спектрометры, такие как те, которые основаны на тангенциальных решётках или оптических фильтрах, упрощают оптическую часть и сокращают стоимость производства, но имеют ограниченное разрешение и кросстоки между каналами.

3. Смартфон-спектрометры и интеграция с портативными вычислительными модулями используют камеру смартфона или CMOS/CCD-матрицы дешёвых модулей для регистрации спектра. Существуют многочисленные DIY-проекты и лабораторные реализации, ориентированные на образовательные цели и полевые измерения.

Некоторые исследования подчёркивают важность выбора компонентов.

1. Дифракционная решётка влияет на спектральное разрешение и однородность распределения длин волн. Решётки с большим числом линий на мм обеспечивают более высокое разрешение, но требуют более точного позиционирования.

2. Детекторы, такие как CMOS/CCD-матрицы, определяют чувствительность прибора, а также его динамический диапазон и уровень шума. В недорогих решениях часто используются массовые камеры от смартфонов или микроконтроллерные модули, что приводит к компромиссу между стоимостью и точностью.

3. Оптические узлы и механические стабилизаторы существенно влияют на аберрации и дрейф измерений.

Одной из ключевых проблем при создании недорогих спектрометров является выбор оптической схемы. В недорогих устройствах часто используется классическая схема Вина, адаптированная под компактные модули: коллиматор, дифракционная решётка, спектральный анализатор и детектор. В щелевых схемах для увеличения спектрального разрешения используется узкая щель, однако точная механическая регулировка удорожает сборку. В альтернативных безщелевых схемах применяются оптические фильтры, сочетающие простоту конструкции с приемлемым диапазоном спектрального разрешения. На рисунке 1 представлен портативный дифракционный спектрометр.

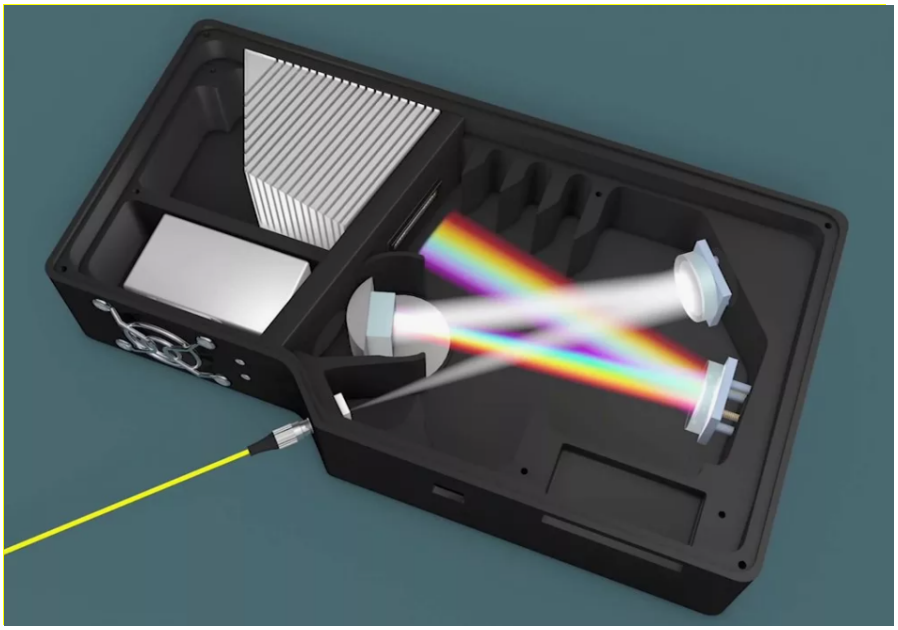


Рис. 1. Портативный дифракционный спектрометр

Многие современные спектрометры используют оптические компоненты, которые производятся массово и стоят дешево. К ним относятся дифракционные решётки, пластиковые линзы и коллиматоры, а также линейные матрицы из обычных камер. Это делает их более доступными, но ограничивает точность измерений в ультрафиолетовом диапазоне.

Одной из основных проблем при использовании дешёвых детекторов является обработка спектральных данных. В научных статьях предлагаются различные алгоритмы для коррекции шума, компенсации изменений освещённости и температурного дрейфа. Очень важно калибровать приборы по известным эталонным линиям, например, ртутной лампы или эталонного источника. Это позволяет повысить точность определения длин волн. Было показано, что программные методы могут существенно компенсировать физические ограничения прибора, особенно в портативных устройствах.

Результаты анализа литературы показывают, что снижение стоимости достигается в основном за счёт упрощения оптической схемы и использования массовых компонентов. Однако это не должно происходить за счёт утери метрологической достоверности. Компромисс между ценой и точностью остаётся ключевым фактором при выборе архитектуры прибора.

Проведённый анализ современных конструкторских решений для малобюджетных портативных спектрометров показал, что доступная спектроскопия является перспективным направлением, способным расширить сферу применения спектрометрических методов за пределы лабораторий. Значительный прогресс связан с развитием микроэлектроники, цифровой обработки сигналов и массовых оптических компонентов. Тем не менее, возникает потребность в дальнейшем совершенствовании методов калибровки и оптимизации оптических схем для повышения точности измерений без значительного увеличения стоимости.

Библиографический список

1. Smith, et al. Portable low-cost open-source wireless spectrophotometer for fast and reliable measurements // HardwareX 2020, 7, e00108.

2. Даниловских М. Г., Винник Л. И., Стрещук В. А. Мини-спектрометр для смартфона // МНИЖ. 2018. №10-1 (76).

3. Yetisen, Ali K., et al. A smartphone algorithm with inter-phone repeatability for the analysis of colorimetric tests //B. Chemical, Volume 196, pp. 156-160.

УДК 628.33; ГРНТИ 70.25.17

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ОЧИСТКИ МОДЕЛЕЙ СТОЧНЫХ ВОД НЕФТЕПЕРЕРАБАТЫВАЮЩИХ ПРЕДПРИЯТИЙ МЕТОДОМ ПНЕВМАТИЧЕСКОЙ СЕПАРАЦИИ

Е.В. Воробьева, В.В. Медведева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, vorobeva-70@bk.ru, valegjua@yandex.ru

Аннотация. В статье рассматривается способ очистки моделей сточных вод, содержащих нефтепродукты, пневмосепарацией в условиях активного гидродинамического режима. Данный метод предусматривает разрушение коллоидной структуры, может использоваться после механической очистки стоков нефтеперерабатывающих предприятий. В данных условиях разрушается гидратная оболочка мицеллярных структур, что позволяет каплям нефтепродуктов коалесцироваться. Образующиеся в виде пены крупные агрегаты удаляются с поверхности воды скребковым механизмом. Метод необходимо проводить при pH стоков от 8,0 до 8,3, что позволяет очистить стоки от нефтепродуктов до ПДК.

Ключевые слова: сточные воды, эмульсия нефтепродуктов в воде, пневмосепарация, коалесценция, гидродинамический режим, методы очистки.

RESEARCH OF THE POSSIBILITY OF PURIFYING WASTEWATER MODELS OF OIL-PROCESSING ENTERPRISES BY PNEUMATIC SEPARATION

E.V. Vorobyeva, V.V. Medvedeva

Abstract. The article discusses a method for cleaning wastewater models containing petroleum products using pneumatic separation under active hydrodynamic conditions. This method involves the destruction of the colloidal structure and can be used after mechanical treatment of wastewater from oil refineries. Under these conditions, the hydrate shell of the micellar structures is destroyed, allowing the petroleum product droplets to coalesce. The resulting large foam aggregates are removed from the water surface using a scraping mechanism. The method should be carried out at a pH of 8.0 to 8.3, which allows for the removal of petroleum products to the permissible limit.

Keywords: wastewater, petroleum product emulsion in water, pneumatic separation, coalescence, hydrodynamic regime, and purification methods.

Предприятия нефтеперерабатывающей отрасли являются крупнейшими потребителями воды. Первоначально ее берут из природных источников. Значительная часть этой воды используется для важных технологических процессов – для охлаждения, удаления солей, промывки и приготовления необходимых растворов. В результате работы цикла производства образуется всегда большое количество сильно загрязненных сточных вод, качество которых определяет вид сырья, технологии переработки и характеристики выпускаемой продукции. В составе отработочных сточных вод есть минеральнеые соли, создающие практически невозможность осуществления замкнутого цикла водооборота. Из-за этого на предприятиях используют две системы канализации: одна обеспечивает частичный повторный водооборот, вторая – отводит стоки на очистные сооружения. После таких процессов, как очистка и подготовка, часть воды возвращается всегда в дальнейший производственный процесс, а другая – поступает в природные водоемы в соответствии с экологическими нормами.

У сточных вод предприятий нефтеперерабатывающего типа достаточно сложный состав: они представляют из себя коллоидные многокомпонентные системы с взвешенными частицами, нефтепродуктами, неорганическими веществами, поверхностно-активными веществами и электролитами. В таблице 1 представлен усредненный состав производственных сточных вод предприятия нефтепереработки исследуемого региона.

Таблица 1. Примерный состав сточных вод НПП

Компоненты	**Содержание в стоках**
Нефтепродукты, мг/л	2500 – 4500
ПАВ, мг/л	50 – 120
Механические взвеси, мг/л	650–850
Фенолы, мг/л	2 – 5
Сульфаты (расчет на SO_4^{2-}), мг/л	140 – 300
Аммонийный азот (расчет на N), мг/л	13 – 25
Хлориды (расчет на $C1^-$), мг/л	3100 –6000
(БПК5), мг/л	400 –600
pH	7.5 – 8.0

Все входящие в состав компоненты из приведенной ранее таблицы повышают стабильность дисперсных систем, а это, в свою очередь, значительно усложняет и замедляет процесс очистки сточных вод. Ключевое условие эффективного решения этой проблемы – разрушение коллоидной структуры с последующим разделение фаз в сточных водах. На сегодняшний день существует множество методов очистки стоков предприятий этого типа, однако по-прежнему важным и востребованным направлением является поиск наиболее экологически безопасных и эффективных.

В ходе наших исследований [1], направленных на изучение способов разрушения коллоидных систем, моделирующих нефтеперерабатывающие сточные воды, разработана технология очистки с использованием пневмосепарации для удаления нефтепродуктов из сточных вод.

Для проведения экспериментов применялась лабораторная установка, имитирующая аэротенк, а также специальные эмульсии нефтепродукт–вода, подготовленные в лабораторных условиях [2]. Диспергированием нефтепродуктов в воде с добавлением компонентов, характерных для сточных вод, создавались модельные эмульсии. После этого смесь тщательно перемешивалась и доводилась до pH 8,0–8,3, соответствующего реальному уровню сточных вод. Температурный режим варьировался в диапазоне +16÷18°C для зимних моделей и +20÷23°C для летних, что отражало сезонные условия. Скорость движения воды контролировалась с помощью задвижек, а время задержки в модели аэротенка составляло 1–1,5 часа.

В ходе эксперимента проводили анализ содержания таких загрязнителей, как нефтепродукты, хлориды, сульфаты, аммиачный азот, сульфиды и фенол. Пробы брались через каждые 3 часа как на входе, так и на выходе установки.

Исследования выполнялись в двух режимах – статическом и динамическом. В статическом режиме аэротенк заполнялся жидкостью, после чего подача воды прекращалась, и происходил процесс барботажа воздуха через неподвижную воду. В динамическом режиме барботаж осуществляли в потоке воды, непрерывно проходящем через аэротенк. Результаты эксперимента представлены в таблицах 2 и 3.

Таблица 2. Очищение промышленных стоков в ламинарном состоянии

Опыт, №	Интервал времени отбора проб для анализов, ч	Компонент и его содержание, мг/л				pH
		нефтепродукт	Хлориды	Сульфаты	Аммиачный азот	
1	0	20,0	37,5	110,0	14,7	7,8
	3	10,0	37,0	105,0	12,3	8,4
	6	6,0	34,5	100,5	10,5	8,4
	9	5,2	40.9	103,5	13,0	8,2
	24	0	60,0	105,0	14,0	8,0
2	0	25,0	23,5	100,5	12,5	8.1
	3	12,3	23,0	90,5	13,0	7,6
	6	8,0	31,5	100,0	14,0	8,0
	9	6,0	36,5	100,5	14,5	8,2
	24	0	35,0	104,5	13,5	7,5
3	0	25,0	23,5	100,5	12,5	8.1
	3	12,3	23,0	90,5	13,0	7,6
	6	8,0	31,5	100,0	14,0	8,0
	9	6,0	36,5	100,5	14,5	8,2
	24	0	35,0	104,5	13,5	7,5
4	0	20,0	10,0	110,0	14,7	7,8
	3	10,0	37,0	105,0	12,3	8,4
	6	6,0	105,0	100,5	10,5	8,4
	9	5,2	12,3	103,5	13,0	8,2
	24	0	8,4	105,0	14,0	8,0

Анализ полученных данных позволяет сделать вывод: уровень сульфатов практически не изменяется, при этом примеси нефтепродуктов полностью устраняются. Наблюдается повышение концентрации хлоридов и аммиачного азота, что связано именно с разрывом связей между этими веществами и поверхностью нефтепродуктов, а также с испарением некоторых компонентов в газовую фазу.

Таблица 3. Очищение промышленных стоков в активном гидродинамическом режиме

Опыт, №	Интервал времени отбора проб для анализов, ч	Компонент и его содержание, мг/л				pH
		нефтепродукт	Хлориды	Сульфаты	Аммиачный азот	
1	0	20,0	37,0	118,0	15,0	7,8
	3	6,9	35,4	115,0	14,5	7,6
	6	4,5	30,0	108,5	14,3	7,6
	9	4,0	40,0	110,5	14,1	7,9
	24	0	55,0	120,0	15,0	8,1
2	0	35,2	38,0	106,0	17,0	8,0
	3	9,6	37,0	100,5	15,5	7,4
	6	5,3	40,0	102,5	14,5	7,8
	9	4,8	58,0	104,0	15,0	7,4
	24	0	60,0	107,0	16,0	8,3

Продолжение таблицы 3

3	0	38,2	32,0	106,0	14,2	7,5
	3	8,3	36,5	96,5	12,3	7,6
	6	5,5	43,0	99,0	10,5	7,8
	9	6,0	50,0	100,0	9,5	8,0
	24	0	62,0	105,0	9,0	8,0
4	0	33,0	37.0	145,0	18,0	8,5
	3	10,0	35.0	147,0	0	8.1
	6	9,0	36,0	148.0	0	8.2
	9	5,5	48,0	155,0	0	8,3
	24	0	52,0	160,0	0	8,3

Во всех сериях экспериментов отмечается уменьшение концентрации нефтепродуктов уже через 2–4 часа пневмосепарации, с полной их ликвидацией спустя 24 часа. В условиях динамического режима частицы движутся упорядоченно и с одинаковой скоростью, снижающей вероятность столкновений микрокапель эмульсии, необходимой для коалесценции. При этом как в статическом, так и в динамическом режимах наблюдается рост концентрации хлоридов, что, по предположению, связано с разрушением мицеллярной структуры и освобождением хло-рид-ионов. Практически отсутствует участие сульфат-ионов в формировании мицелл, вследствие чего их уровень после барботажа остается неизменным.

Из анализа полученных данных можно заключить, что пневмосепарация моделей сточных вод эффективно удаляет нефтепродуктовые загрязнения за 2–4 часа либо снижает их концентрацию до ПДК (<0,05 мг/л), независимо от наличия минеральных солей. При этом нефтяная пена собирается на поверхности, что обеспечивает удобство ее удаления с помощью скребкового механизма.

Библиографический список

1. Кувшинников И.М., Черепанова Е.В., Воробьева Е.В., Яковлев А.И., Пермяков Д.Г. Опытно-промышленные исследования очистки сточных вод методом пневмосепарации // Химическая промышленность. 2002. № 7. С. 42.

2. Гальченко С.В., Воробьева Е.В., Чердакова А.С., Посевина Ю.М. Экологические аспекты очистки сточных вод от нефтепродуктов методом пневмосепарации при внесении гумата калия // Экология и промышленность России. 2018. Т. 22. № 1. С. 38-43.

3. Минлигулова, Г. А. Исследование очистки сточных вод, содержащих ионы тяжелых металлов, стоками нефтехимических производств / Г. А. Минлигулова, И. Г. Шайхиев //Вестник Казанского технологического университета. – 2011. – № 6. – С. 166–171.

4. О состоянии и об охране окружающей среды Российской Федерации в 2020 году. Государственный доклад. – Москва : Минприроды России ; МГУ имени М. В. Ломоносова, 2021. – 864 с.

5. Долина, Л. Ф. Современная техника и технологии для очистки сточных вод от солей тяжелых металлов : монография // Л. Ф. Долина. – Днепропетровск : Континент, 2008. – 254 с.

УДК 665.738 ГРНТИ 61.51.01

ПРОИЗВОДСТВО ДОПОЛНИТЕЛЬНОГО ВЫСОКООКТАНОВОГО КОМПОНЕНТА АВТОМОБИИЛЬНОГО БЕНЗИНА В ПЕРИОД ДЕФИЦИТА ТОЛУОЛА

Е.В. Воробьева, Ю.С. Агаршева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, vorobeva-70@bk.ru, agarsheva.yuliya@yandex.ru

Аннотация. В работе предлагается поделить катализат с топливного риформинга ЛГ-35-8/300Б на легкую и высокооктановую тяжелую части, с последующим использованием тяжелой, как компонента АИ-100-К5 в периоды дефицита толуола. В ходе работы был рассмотрен период простоя установки Л-35-6/300 и применена схема с делением катализата с установки ЛГ-35-8/300Б в колонне К-4 установки АТ-6. Легкую часть фракции направляли в линию лекого бензина каталитического крекинга, а тяжелую часть фракции – на смешение АИ-100-К5 в ТСЦ. На инженерной модели установки 35-8/300Б была разработана схема деления катализата в колонне К-4 АТ-6 и рассчитаны технологический режим, качество продуктов деления. На модели PIMS был рассчитан экономический эффект от внедрения предложеной схемы и расчитаны материальные затраты.

Ключевые слова: катализат, бензины, моделирование, октан, схема, АО «РНПК».

PRODUCTION OF AN ADDITIONAL HIGH-OCTANE COMPONENT OF AUTOMOBILE GASOLINE DURING THE TOLUENE SHORTAGE PERIOD

E.V. Vorobyeva, Yu.S. Agarsheva

Ryazan State Radio Engineering University named after V.F. Utkin, Russian Federation, Ryazan, vorobeva-70@bk.ru, agarsheva.yuliya@yandex.ru

Annotation. In this paper, it is proposed to separate the catalyzate from the fuel reforming of LH-35-8/ 300B for light and high-octane heavy parts, followed by the use of heavy as a component of AI-100-K5 during periods of toluene deficiency. During the work, the downtime of the L-35-6/300 unit was reviewed and a scheme with fission of the catalysate from the LG unit was applied.-35-8/ 300B in column K-4 of the AT-6 installation. The light part of the fraction was sent to the catalytic cracking gasoline gas line, and the heavy part of the fraction was mixed with100-K5 in the shopping mall. Based on the engineering model of the 35-8/300B installation, a scheme for the separation of catalyzate in the K-4 AT-6 column was developed and the technological regime and the quality of the fission products were calculated. Using the PIMS model, the economic effect of implementing the proposed scheme was calculated and the material costs were calculated.

Keywords: catalyzate, gasoline, modeling, octane, scheme, RNPC JSC.

Процесс риформинга является одним из ключевых этапов в нефтепереработке, направленным на повышение октанового числа бензиновых фракций и получение ароматических углеводородов. Катализат риформинга, представляющий собой сложную смесь углеводородов, обладает высоким потенциалом для дальнейшего разделения и использования в производстве высококачественных топлив. В условиях растущих требований к экологичности и энергоэффективности топлив, а также увеличения спроса на высокооктановые бензины, актуальным становится вопрос рационального использования всех компонентов катализата.

Особый интерес представляет технология разделения катализата риформинга на легкую и тяжелую фракции. Легкая фракция традиционно используется для получения бензинов с улучшенными характеристиками, тяжелая фракция, насыщенная ароматическими углеводородами, обладает значительным потенциалом в приготовлении высокооктановых автобензинов. Ее применение в качестве добавки при производстве бензина класса АИ-100 позволяет не только повысить октановое число конечного продукта, но и оптимизировать использование ресурсов, снижая зависимость от дорогостоящих компонентов, например толуола[1].

Использование тяжелой фракции катализата риформинга при производстве бензина класса АИ-100 открывает новые возможности для повышения конкурентоспособности про-

дукции нефтеперерабатывающих предприятий. Это направление соответствует современным тенденциям в области создания высококачественных топлив, отвечающих как эксплутационным, так и экологическим требованиям.

В работе поднимается вопрос об ограниченном объеме резервуаров для хранения толуола без возможности производства нового объема в период простоя 35/6, что представляет собой фактор, влияющий на объем производства высокооктанового бензина в период высокого спроса на него, возможность максимально накопленого объема в резервуарах Е-26, 27, 28 по БП на 2025-2029 года – составляет 900 т. При таком объеме накапливаемого толуола эффективность производства АИ-100 близка к нулю.

Однако, если рассматривать рецептуру производства АИ-100-К5, то в нем только лишь два компонента имеют ОЧИ выше 100 – это эфиры (в случае нашего завода это МТАЭ и МТБЭ с октанами 105 или 115) и толуол (ИОЧ 110), который производит установка 35/6. Остальные компоненты состава имеют октановое число ниже 100, туда входят катализат с риформингов с октановым число от 94 до 96, алкилат (ИОЧ 95-96), изогексан – ИОЧ 89 и нормальный бутан с октановым числом 94 [2]. Тогда была выдвинута мысль, что с целью повышения производства достаточного объема АИ-100, в условиях дефицита толуола можно разделить катализат с установки риформинга ЛГ-35/8-300Б в К-4 установки АТ-6 на легкую и тяжелую высокооктановые части и использовать последнюю в качестве аналога толуола.

В нынешних условиях работы завода АО «РНПК» на установке АТ-6 на блоке вторичной переработки существует комплекс оборудования, не использующийся по прямому назначению. В данном проекте предлагается использовать этот ресурс и завести в К-4 АТ-6 стабильный катализат с установки топливного риформинга ЛГ-35-8/300 для его последующего деления. Минимальная загрузка К-4 АТ-6 – 22 т/ч, что сопоставимо с загрузкой данного риформинга.

Используя метод моделирования, было выявлено, что оптимальная пропорция деления это 80% легкого катализата с ОЧИ 92, который мы можем направить в линию ЛБКК, и 20% тяжелого катализата с ОЧИ 110, который мы будем использовать по аналогии с толуолом для производства высокооктанового бензина АИ-100. Благодаря делению на данные фракции можно добиться выхода высокооктановой части без содержания в ней бензола, что положительно скажется на общей смеси в будущем[3]. Так как экологические стандарты постоянно ужесточаются, то инновационные решения должны помогать в соблюдении норм по качеству топлива – поиск таких решений становится все более актуальной задачей.

Для технической реализации новой технологической схемы, необходимо проложить линию трубопровода от колонны К-4 установки ЛГ-35-8/300 до К-4 установки АТ-6. При этом существующего оборудования на блоке вторичной перегонки установки АТ-6 достаточно для технической реализации работы колонны в режиме деления катализата.

Для вывода тяжелой фракции с установки потребуется проложить трубопровод от установки АТ-6 до товарно-сырьевого цеха, а для потока легкой части необходима прокладка трубопровода с осуществлением врезки в линию легкого бензина каталитического крекинга.

Ниже приведен рисунок с предлагаемой схемой технической реализации (рисунок 1), а также таблицы с качеством новых потоков (таблица 1) и технологическим режимом деления колонны К-4 установки АТ-6 (таблица 2).

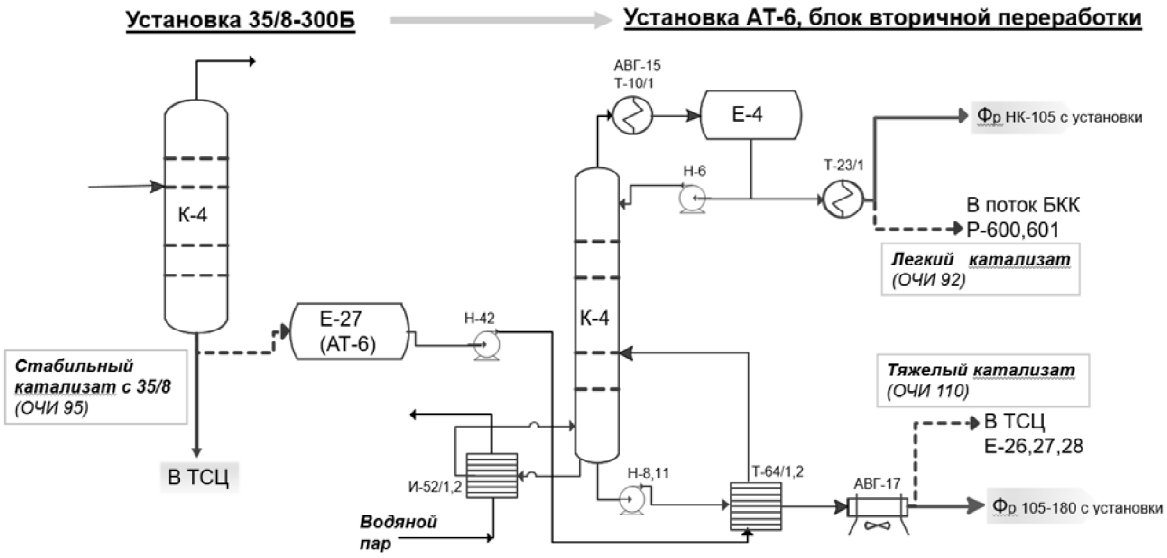


Рис. 1. Схема технологической реализации

Таблица 1. Качество катализата при стандартной работе 35/8-300Б и в режиме деления катализата в К-4 установки АТ-6

Параметры	Ед. изм.	Стандартный режим Вывод катализата 35/8-300Б	Режим деления потока с 35/8-300Б	
			Лёгкий катализат	Тяжелый катализат
Расход потока	т/ч	26,02	21,05	4,97
ОЧИ	-	95,1	92,0	110,5
ДНП	кПа	69,2	80,9	1,4
Бензол	%об.	0,70	0,89	0,00
Ароматика	%об.	53,49	45,36	93,77
Начало кипения	°С	36,0	29,68	147,5
Конец кипения	°С	190,5	142,4	200,8

Таблица 2. Технологический режим колонны К-4 установки АТ-6

Показатель	Ед. изм.	Смоделированный режим
ПРОФИЛЬ ДАВЛЕНИЯ		
Вверху колонны	кг/см^2	0,967
Внизу колонны		1,437
В рефлюксной емкости		0,667
ТЕМПЕРАТУРНЫЙ РЕЖИМ		
Вверху колонны	°С	136,8
Внизу колонны		192,2
В рефлюксной емкости		62,5
РАСХОДЫ		
Легкого катализата с верха колонны	т/ч	21,1
Тяжелого катализата с низу колонны		4,9
Острого орошения	м^3/ч	10,0
ТЕПЛОВЫЕ НАГРУЗКИ		
Нагрузка на конденсатор	Гкал/ч	3,26
Нагрузка на ребойлер		1,98

Экономическая эффективность данного проекта, представленого в работе, рассчитана на модели бизнес плана на Май 2025 г. Внедрение предложенной технологической схемы деления катализата позволит увеличить объемы производства высокооктанового товарного бензина в период простоя Л-35-6/300 примерно в 5 раз, при равном количестве накопленного толуола (таблица 3).

При расчете экономического эффекта от реализации данной схемы, наблюдается увеличение дорогостоящего бензина АИ-100, что в результате дало суммарную маржу по модели +71 млн рублей. При этом суммарный баланс бензинов не изменяется, а весь экономический эффект достигается за счет увеличения объема производства высокооктанового автобензина в период дефицита высокооктанового компонента (таблица 4).

Таблица 3. Сравнение смешений PIMS

ДО ДЕЛЕНИЯ		
Компонент смешения	**БП Май 2025**	
	тн/период	**%**
МТАЭ марки В - с ННК	277	15,07
Компонент толуола	489	26,61
Алкилат	477	25,95
Ст.катализат 11/600	416	22,63
Буллиты ТСЦ (ГФУ)	151	8,22
Изогексан/Ст.изомер	28	1,52
Сумма:	**1838**	**100,00**
ПОСЛЕ ДЕЛЕНИЯ		
Компонент смешения	**БП Май 2025**	
	тн/период	**%**
МТАЭ марки В - с ННК	1347	14,97
Компонент толуола	489	5,43
Алкилат	2259	25,10
Ст.катализат 11/600	2313	25,70
Тяжелый катализат	**1739**	**19,32**
Буллиты ТСЦ (ГФУ)	765	8,50
Изогексан/Ст.изомер	88	0,98
Сумма:	**9000**	**100,00**

Таблица 4. Экономический эффект от реализации БП

Варианты планов производства	**Цены**	**БП Май 2025**		**План на Май с учетом деления катализата**		**Разница**
Наименование	**руб/тонна**	**тонн/мес.**	**%**	**тонн/мес.**	**%**	**Δ**
Бензин АИ-100-К5	70 299,80	1 838	0,16	9 000	0,81	+7 162
Бензин АИ-95-К5 "Евро 6"	58 709,40	131 825	11,83	121 871	10,94	-9 954
Бензин Регуляр-92 (АИ-92-К5)	53 277,50	104 698	9,39	107 606	9,66	+2 908
Пересчет в цены						
Маржа по модели, тыс. руб.		**7 472 616**		**7 544 035**		**+71 419**

В таблице 5 представлены затраты на реализацию схемы деления катализата. Суммарная стоимость проекта состовляет 41 млн. руб., она включает в себя все необходимые затраты на разработку, внедрение и запуск схемы в работу.

Таблица 5. Стоимость работ по реализации проекта

Вид работы	Стоимость, млн. руб.
Проектно-изыскательные работы	5,5
Строительно-монтажные работы	12,8
Материально-техническое обеспечение	15,7
Прочие	7,2
ИТОГО:	**41,2**

Работы по возведению проекта начинаются с осени 2025 года, тогда схема войдет в эксплуатацию и начнет работать уже при следующем ремонте установки Л-35-6/300 в апреле 2027 года. В таблице 6 отражены реальные сроки окупаемости данного проекта с учетом дисконтирования и затрат на монтаж схемы.

Таблица 6. Стоимость работ по реализации проекта

Ставка дисконтирования	20%	в год
Расчетный период, лет	10	
Показатели эк. эффективности предложения на полн./остат. стоимость		
Чистый дисконтир. доход **(NPV)**	**82,4 / 82,4**	млн руб.
Индекс прибыльности **(PI)**	**4 / 4**	ед.
Срок окупаемости дисконтированный **(DPP)**	**2,6 / 2,6**	лет
Внутр.норма доходности **(IRR)**	**>100% / >100%**	% год.

Итог от внедрения предложенной технологической схемы с делением катализата позволит увеличить прибыль примерно на 10 млн.руб с каждой 1000 т произведенного АИ-100 в период дефицита толуола. Схема быстро окупаема и имеет высокую эффектиность от производства дополнительного высокооктанового компонента.

Данный проект позволит не только повысить объем производства конечного продукта и снизить зависимость от выработки толуола, но и оптимизировать использование ресурсов нефтеперерабатывающих предприятий. Таким образом, данный вариант применим не только к производственной цепочке АО «РНПК», а также его реализация возможна на других предприятиях Общества.

Библиографический список

1. Петров А. А., Сидорова, Е. В. (2016). Смешение товарной продукции: принципы и технологии. Нефтегазовая индустрия, 72(4), 44-48.

2. Гуреев А. А. Производство высокооктановых бензинов / А. А. Гуреев − М.: Химия, 1981 с. 256–264

3. Васильев А. А., Романов И. И. (2019). Особенности процессов смешения нефтепродуктов. Реферат СЗТУ, 52(2), 78-84.

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ. ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ»

СЕКЦИЯ «МОДЕЛИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В САПР»

УДК 004.42; ГРНТИ 28.23

РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ КАЧЕСТВА НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ РАСПОЗНАВАНИЯ ДЕФЕКТОВ

М.А. Бакулева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, m.a.bakuleva@yandex.ru

Аннотация. В работе рассматриваются основные проблемы распознавания дефектов при сдаче объектов строительства. Основным таким дефектом являются сколы или трещины на поверхности оштукатуренных стен. Поскольку современные объекты строительства носят масштабный характер и дома сдаются с большим количеством квартир, и каждую квартиру необходимо осмотреть и сформировать заключение в краткие сроки, задача автоматизации процесса идентификации дефектов является актуальной.

Ключевые слова: дефектоскопия, распознавание образов, сверточные нейронные сети, экспертная система, контроль качества.

DEVELOPMENT OF AUTOMATED QUALITY ASSESSMENT SOFTWARE MODULE BASED ON INTELLIGENT DEFECT RECOGNITION SYSTEM

M.A. Bakuleva

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, horek.colupaeva@yndex.ru m.a.bakuleva@yandex.ru

The summary. The paper discusses the main problems of defect recognition during the commissioning of construction projects. The main defect is chipping or cracking on the surface of plastered walls. Since modern construction projects are large-scale and involve multiple apartments, it is necessary to inspect and evaluate each apartment in a timely manner. Therefore, automating the process of defect identification is crucial.

Keywords: flaw detection, pattern recognition, convolutional neural networks (CNN), expert system, and quality control.

Интеллектуальная система распознавания дефектов (система дефектоскопии на базе искусственного интеллекта, ИИ) – это система, которая автоматизирует процесс выявления дефектов, анализирует не только явные дефекты, но и скрытые параметры – микроструктуру поверхности, плотность распределения, локальные изменения цвета и текстуры.

При выборе интеллектуальной системы распознавания строительных дефектов учитываются следующие факторы:

1. *Характер доступных данных*. Данные, получаемые с видеокамеры (инженера или квадрокоптера) отличаются большим объёмом, непрерывностью поступления и высокой размерностью, поэтому очевидна целесообразность применения методов машинного обучения, способных обучаться на накопленных примерах и строить собственные модели зависимостей;

2. *Требования к результату*. Разрабатываемая система должна иметь возможность в режиме реального времени распознавать дефекты;

4. *Интеграция с информационными системами предприятия*. Позволяет фиксировать дефекты, для повышения эффективности контроля качества устранения недостатков.

В данной работе рассматривается актуальная прикладная задача распознавания дефектов поверхности оштукатуренных и покрашенных стен (рисунок 1). Решение данной задачи основывается на применении искусственных нейронных сетей, распознавания изображений и специализированных экспертных систем. Для решения задачи распознавание дефектов применяется сверточная нейронная сеть, позволяющая идентифицировать дефект оштукатуренных поверхности. Разработанный программный модуль производит классификацию по следующим параметрам дефекта:

-характер повреждения (скол, трещина, необработанный участок)

-размер повреждения;

- глубина повреждения.

Далее применяется экспертная система для оценки объема работ по устранению выявленных недостатков и количеству необходимого материала для проведения работ. Также предусмотрен программный модуль, позволяющий прогнозировать сроки проведения повторного анализа поверхности.

Все работы по устранению дефектов (заказ-наряды) вносятся в соответствующую базу данных для дальнейшего проведения анализа по эффективности работы строительных бригад и расчёта ущерба от выполнения работ ненадлежащего качества.



Рис. 1. Пример исходных данных (снимка квадрокоптера) для анализа дефектов поверхности

Следует отметить, что задача распознавания дефектов поверхностей успешно решается с помощью аппарата сверточных нейронных сетей (**CNN**). Данная задача распознавания трещин (размеры и локализация) является стандартной и может быть эффективно решена средствами Python (рисунок 2.)

```
model = tf.keras.Sequential([
    tf.keras.layers.Conv2D(32, (3, 3), activation='relu', input_shape=(224, 224, 3)),
    tf.keras.layers.MaxPooling2D((2, 2)),
    tf.keras.layers.Conv2D(64, (3, 3), activation='relu'),
    tf.keras.layers.MaxPooling2D((2, 2)),
    tf.keras.layers.Conv2D(128, (3, 3), activation='relu'),
    tf.keras.layers.MaxPooling2D((2, 2)),
    tf.keras.layers.Flatten(),
    tf.keras.layers.Dense(512, activation='relu'),
```

```
    tf.keras.layers.Dropout(0.5),
    tf.keras.layers.Dense(1, activation='sigmoid')
train_generator = datagen.flow_from_directory(
    'dataset/train',
    target_size=(224, 224),
    batch_size=32,
    class_mode='binary'
)
validation_generator = datagen.flow_from_directory(
    'dataset/validation',
    target_size=(224, 224),
    batch_size=32,
    class_mode='binary'
)
```

Рис. 2. Пример фрагмента кода для создания модели CNN

При условии, что модель будет предварительно обучена на цифровых изображениях дефектных участков стен и на тех поверхностях, которые приняты к эксплуатации. Заметим, что для обучения сети достаточно иметь базу данных изображений, собранных на одном объекте строительства (20 этажный дом по 8 квартир на этаже). Фрагмент кода, реализующий обучение сети представлен на рисунке 3.

```
history = model.fit(
    train_bd_im,
    epochs=20,
    validation_data=validation_image
)
```

Рис. 3. Пример фрагмента кода обучения CNN

После того, как свёрточная нейронная сеть распознала класс дефекта на стене, происходит определение координат размеров трещины. Полученные результаты сохраняются в базе данных и передаются специалисту; далее происходит дополнительное исследование поверхности для того, чтобы оценить масштаб работы и сроки устранения выявленных дефектов. Соответствующие показатели также вводятся в базу данных, и затем происходит формирование заказ-наряда.

Далее планируется разработка и внедрение системы нечеткого вывода «если, то» на основе нечёткой логики, которая позволит формализовать зависимость параметров дефектов поверхности (выходные данные сверточной нейронной сети и алгоритма интерпретации результатов классификации) и соответствующие выходные данные (требуемое количество материала для устранения дефектов и сроки выполнения работ), что позволит исключить дополнительный осмотр специалистом на этапе промежуточной (внутренней) сдачи- приемки. Очевидно, что для оценки эффективности и качества выполнения работ необходимо разработать алгоритмы аналитической обработки данных (регрессия и ассоциативный анализ), которые сохранятся в базе данных после идентификации дефектов поверхностей.

Библиографический список

1. Корячко В.П., Бакулев А.В., Бакулева М.А. АЛГОРИТМ ИДЕНТИФИКАЦИИ ТРАНСПОРТНЫХ СРЕДСТВ В УСЛОВИЯХ НЕПОЛНЫХ ДАННЫХ. В сборнике: BIG DATA и анализ высокого уровня. сборник научных статей X Международной научно-практической конференции. Минск, 2024. С. 170-174.

2. Бакулева М.А., Костин В.Ю., Грушкин С.Г., Юрасов В.А ПРОГРАММА РАСПОЗНАВАНИЯ ИЗОБРАЖЕНИЯ ЗАДАННОГО КЛАССА ПО АНАЛИЗУ МОБИЛЬНОГО ФОТО.Свидетельство о регистрации программы для ЭВМ RU 2023667712, 17.08.2023. Заявка № 2023666534 от 04.08.2023.

3. Бакулева М.А., Бакулев А.В АНАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ДЛЯ ОЦЕНКИ ДИНАМИКИ ОБЛАСТИ ДЕСТРУКЦИИ.В книге: Новые информационные технологии в научных исследованиях НИТ-2021. материалы XXVI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов. Рязань, 2021. С. 281-282.

4. Бакулев А.В., Бакулева М.А., Лукьянова В.М. ИСПОЛЬЗОВАНИЕ APACHE SPARK В ПРИЛОЖЕНИЯХ ПОТОКОВОЙ ОБРАБОТКИ ДАННЫХВ сборнике: Новые информационные технологии в научных исследованиях. Материалы XXIII Всероссийской научно-технической конференции студентов, молодых ученых и специалистов: в 2 томах. 2018. С. 205-206.

5. Бакулев А.В., Бакулева М.А. РАЗРАБОТКА АЛГОРИТМА ПОИСКА АССОЦИАТИВНЫХ ПРАВИЛ СЛАБОСТРУКТУРИРОВАННЫХ ДАННЫХВ сборнике: Современные технологии в науке и образовании - СТНО-2018. Сборник трудов международного научно-технического форума: в 11 томах. Под общ. ред. О.В. Миловзорова. 2018. С. 215-218.

УДК 681.5; ГРНТИ 28.23

ПРОБЛЕМА ДЕГРАДАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ ЦИФРОВЫХ ДВОЙНИКОВ И ПУТИ ЕЕ РЕШЕНИЯ

М.С. Кошелева, В.И. Орешков

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань

Аннотация. В работе рассматривается проблема деградации интеллектуальных цифровых двойников (ИЦД). Приводится классификация ее видов и основные причины появления. Анализируются возможные пути решения данной проблемы за счет своевременного выявления и всестороннего мониторинга работы ИЦД.

Ключевые слова: интеллектуальные цифровые двойники, модели машинного обучения (ML-модели), деградация моделей, дрейф данных.

THE PROBLEM OF DEGRADATION OF INTELLECTUAL DIGITAL TWINS AND WAYS TO SOLVE IT

M.S. Kosheleva, V.I. Oreshkov

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan

The summary. This paper examines the problem of intelligent digital twin (IDT) degradation. It classifies its types and provides the main causes. Possible solutions through timely detection and comprehensive monitoring of IDT performance are analyzed.

Keywords: intelligent digital twins, machine learning models (ML), model degradation, data drift.

Цифровые двойники в настоящее время становятся все более привычным элементом современного бизнес-ландшафта [2]. При этом наблюдается интенсивная интеллектуализация цифровых двойников, что позволяет им решать более сложные задачи, становиться более автономными и адаптивными к изменениям во внешнем окружении [1].

В основе построения интеллектуальных цифровых двойников (ИЦД) лежит использование в них моделей машинного обучения (ML-моделей), обучаемых на данных, которые описывают предметную область, в которой они должны функционировать. ИЦД имеют следующие преимущества перед обычными:

– высокая скорость разработки и развертывания в производственной среде за счет применения самообучающихся алгоритмов;

– адаптивность к изменениям во внешнем окружении – достаточно добавить в структуру ИЦД новые модели или переобучить существующие.

Вместе с тем, использование в ИЦД ML приводит к такому негативному явлению, как деградация цифровых двойников, известному также, как старение ИИ. Оно выражается в том, что ИЦД, развертываемые в производственных средах, часто оказываются подвержены постепенному снижению точности, что приводит к ухудшению качества их работы. Хотя ML-модели в ЦД изначально обучаются на исторических данных, реальные условия их эксплуатации обычно вносят изменения, которые со временем негативно влияют на точность их предсказаний.

Исследования показали, что 91% моделей машинного обучения со временем деградируют, 75% компаний наблюдали снижение их производительности, а более половины сообщили о значительных финансовых потерях из-за падения точности. Когда в моделях, оставленных без внимания в течение шести месяцев или дольше, частота ошибок для новых данных увеличивается на 35%, влияние их деградации на бизнес становится невозможно игнорировать [5].

Одной из основных причин деградации моделей и ИЦД, построенных на их основе, является дрейф данных, который имеет три составляющих [3].

1. Изменения в распределении входных данных в условиях эксплуатации ИЦД относительно данных, использовавшихся при его обучении (собственно дрейф данных). Например, при обучении доля клиентов в возрасте 30 – 40 лет составляла 60%, а спустя некоторое время снизилась до 40% из-за изменения демографической ситуации. Обнаружить и обработать дрейф данных относительно легко.

2. Изменение характера взаимосвязи между входными и выходными переменными моделей, что приводит к смещению их предсказаний (дрейф концепции). Базовая концепция, которой обучился ИЦД, перестает быть актуальной. Обнаружить дрейф концепции сложнее, поскольку распределение входных данных может выглядеть неизменным. Простые отклонения в данных часто можно устранить путем периодического повторного обучения, в то время как дрейф концепции может потребовать перепроектирования ML-модели, изменений в разработке или даже фундаментального переосмысления проблемы.

3. Изменения значимости признаков (дрейф признаков), когда признаки, сильно влияющие на изменчивость выходных переменных на этапе обучения модели, в процессе ее промышленной эксплуатации утрачивают свою значимость, а другие, ранее менее значимые, увеличивают ее.

4. Дрейф репрезентативности, который возникает из-за того, что обучающая выборка, использовавшаяся для построения модели в ИЦД, не учитывала всех особенностей проблемной области, проявляющихся в эксплуатационной среде, на которые модель не может адекватно реагировать.

Независимо от причин деградации, если ее своевременно не обнаружить и не контролировать, её появления приводят к ухудшению работы ИЦД. Выявление причин деградации является сложной задачей. Во многих случаях трудно определить, вызвана ли она смещением данных, изменениями в эксплуатационной среде или просчетами в процессе обучения. Поэтому без эффективных механизмов анализа первопричин, обнаружение и устранение последствий деградации оказывается весьма затратным процессом, часто требующим трудоемкого ручного вмешательства.

Для предотвращения деградации ИЦД необходимы непрерывный мониторинг качества работы, его повторное обучение на новых актуальных данных, соответствующих текущему состоянию эксплуатационной среды. Однако стратегия повторного обучения должна быть тщательно проработана для достижения баланса между адаптивностью и устойчивостью. Слишком частое повторное обучение может привести к перекосу ML-моделей в сторону последних тенденций и закономерностей эксплуатационной среды, а слишком редкое приводит к риску длительных периодов плохой работы.

Ситуация усугубляется еще и тем, что разные ML-модели деградируют с совершенно разной скоростью на одних и тех же данных. Одни – постепенно и предсказуемо, другие же испытывают «взрывную деградацию» – хорошо работают в течение длительного периода, а затем внезапно рушатся. Без надлежащего мониторинга невозможно узнать, какой именно паттерн поведения демонстрирует конкретная модель, пока не станет слишком поздно

Различают два типа деградации ЦД (рисунок 1):

– взрывной, когда ИЦД длительное время работает хорошо, но в какой-то момент его точность резко падает. Эта точка как правило трудно предсказуема и может не зависеть от

конкретных изменений в данных. Мониторинг не обеспечивает эффективного контроля и позволяет только констатировать, что уже все плохо;

– плавный, когда имеет место постепенное повышение вариативности ошибок. В среднем ИЦД продолжает работать хорошо и количество допускаемых им ошибок остается на одном уровне, но их величина постепенно возрастает. Хорошо отслеживается мониторингом.

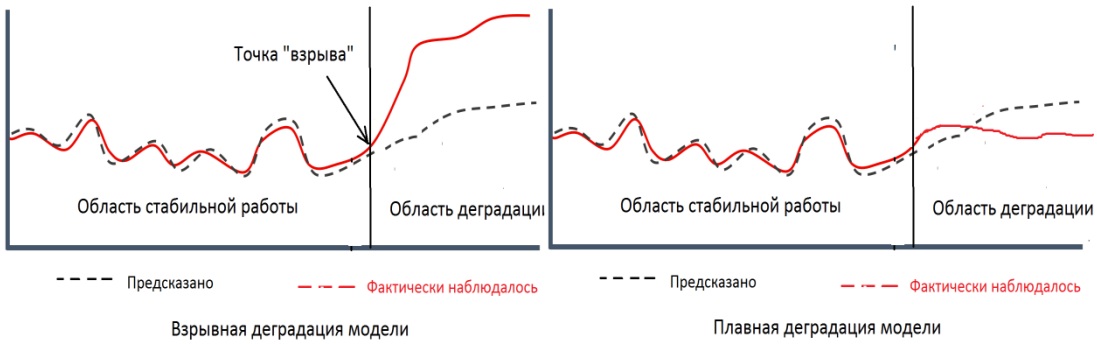


Рис. 1. Типы деградации ЦД

Интеграция процедур раннего обнаружения деградационных явлений, выявление их причин и повторного обучения в единый автоматизированный рабочий процесс управления жизненным циклом ИЦД позволит обеспечить его устойчивое и надежное функционирование в течение длительных периодов после развертывания в эксплуатационной среде. При этом важно обеспечить:

– непрерывный мониторинг – отслеживание показателей эффективности ИЦД (точность, отклонение) в режиме реального времени;

– повторное обучение (retraining) его моделей – регулярное обновление на основе актуальных данных;

– использование в ИЦД адаптивных моделей, способных к динамическому обучению и адаптации.

Основой эффективного обнаружения деградации в ИЦД является всесторонний мониторинг его производительности без которого невозможно обнаружить деградационные явления, разработать и реализовать комплекс мер для их преодоления, а также оценить их результативность. Система мониторинга состояния ИЦД должна отслеживать показатели по четырём типам.

1. Прямые показатели эффективности – метрики, которые напрямую показывают, решает ли ML-модель поставленную задачу. Для моделей классификации это может быть F1-мера, точность, полнота, AUC-ROC и т.д. Для регрессии удобно использовать RMSE, MAE, R-квадрат или MAPE [4];

2. Косвенные показатели эффективности. Прямые показатели эффективности позволяют увидеть, насколько де-факто уже ухудшилась работа системы. В то же время косвенные метрики, отражающие изменения в распределении входных данных, позволяют предупредить о вероятном снижении производительности ИЦД еще до того, как его можно будет непосредственно измерить. К таким косвенным метрикам относятся:

– индекс стабильности популяции (PSI), который показывает, насколько изменилось распределение признака по сравнению с обучающей выборкой. Рассчитывается для каждого значимого признака. Значения PSI выше 0.25 требуют изучения, а выше 0.1 требуют внимания.

– критерий Колмогорова-Смирнова позволяет сравнить наблюдаемые распределения данных с теми, на которых производилось обучение;

3. Мониторинг по отдельным параметрам распределения. Отслеживание среднего значения или стандартного отклонения, минимума, максимума и квартилей распределения для каждого числового признака.

4. Мониторинг характера ошибок. Анализ причин ошибок позволяет получить важную информацию об изменениях в работе ИЦД. Поэтому следует:

– отслеживать не только частоту ошибок, но и их типы. Различные типы ошибок указывают на разные первопричины;

– временные закономерности ошибок: увеличиваются ли ошибки равномерно разнонаправлено в определенных временных интервалах? Неравномерность вариативности ошибки может указывать на изменения во внешней среде (появление новых конкурентов, сезонные сдвиги и т.д.);

– специфические для каждого признака закономерности ошибок: какие признаки участвуют в предсказаниях, где модель дает сбой? Специфические для каждого признака ошибки указывают на то, что именно в них произошло смещение распределений.

Еще одной проблемой, связанной с деградацией ИЦД и необходимостью их корректировки для восстановления производительности, является вынужденная приостановка поддержки ИЦД соответствующего бизнес-процесса [5]. Это может привести к его частичной или полной остановке на время «ремонта» и потери прибыли, либо к переходу управления бизнес-процессом в ручной режим, что увеличивает риск ошибочных решений, приводящих к убыткам. Чтобы решить проблему «простоя» ИЦД, возможно использование ансамбля моделей, обученных на разных подмножествах данных, предсказания которых агрегируются с целью повышения точности. Подход позволяет постепенно отказываться от устаревших, деградировавших моделей в ИЦД и плавно «накатывать» новые, актуальные модели, на останавливая ход бизнес-процесса. Метод реализуется следующим образом:

– построить и поддерживать ансамбль из 2-3 моделей разного «возраста», т.е. обученных на данных из разных временных интервалов;

– увеличить вес моделей, обученных на наиболее поздних данных;

– постепенно уменьшить вес «старых» моделей по мере снижения их производительности;

– заменить самую «старую» модель, когда наиболее «новая» продемонстрирует стабильно высокую производительность.

Способность ИЦД оставаться точными и генерирующими высокую бизнес-ценность на протяжении длительных периодов времени полностью зависит от систем их поддержки в производственной среде. Таким образом, решение проблемы деградации ИЦД является достаточно затратным и трудоемким, хотя и необходимым процессом. При этом его ручная реализация малоперспективна, поскольку оказывается слишком сложной и длительной, а кроме того, связана с большими рисками и ошибками.

Поэтому единственно правильным подходом является комплексная автоматизация всего процесса мониторинга производительности ИЦД с целью обнаружения деградации и борьбы с ней. Для этого необходимо создавать автоматизированные конвейеры, которые включают процедуры проверки и подготовки данных, выполнения ретрейнинга или иных видов коррекции моделей, их всестороннее оценивание и непрерывное разворачивание в производственной среде.

Библиографический список

1. Кошелев А.Д., Кошелева М.С., Орешков В.И. Эволюция концепции цифровых двойников/ Кошелев А.Д., Кошелева М.С., Орешков В.И. // Информационные технологии в прикладных исследованиях: межвузовский сборник научных трудов. – Рязань: ИП Коняхин А.В. (Book Jet), 2024. – 336 с.

2. Кошелева М.С., Орешков В.И. Обобщенный подход к проектированию цифровых двойников/ Кошелева М.С., Орешков В.И. // Новые информационные технологии в научных исследованиях: материалы XXIX Все-

российской научно-технической конференции студентов, молодых ученых и специалистов. – Рязань: РГРТУ, 2024. – 260 с.

3. Ферлитш, Э. Шаблоны и практика глубокого обучения / Э. Ферлитш; перевод с английского А. В. Логунова. – Москва: ДМК Пресс, 2022. – 538 с.

4. Мэрфи, К.П. Вероятностное машинное обучение. Дополнительные темы: предсказание, порождение, обнаружение, действие: руководство / К. П. Мэрфи; перевод с английского А. А. Слинкина. – Москва: ДМК Пресс, 2024. – 766 с.

5. Vela, D., Sharp, A., Zhang, R. et al. Temporal quality degradation in AI models. Sci Rep 12, 11654 (2022).

УДК 004.032.26; ГРНТИ 28.23.37

ПРИМЕНЕНИЕ НЕЙРОСЕТЕВЫХ ИНСТРУМЕНТОВ В РАДИОЛОКАЦИИ

Т.Р. Боцман, А.В. Бакулев

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, botsman.tatjana@yndex.ru

Аннотация. В работе рассматриваются возможности интеграции глубокого обучения в тракты обработки радиолокационной информации. Особое внимание уделяется переходу от классических детерминированных алгоритмов к адаптивным нейросетевым моделям в задачах фильтрации помех, распознавания целей, когнитивного управления ресурсами радиолокационных систем (РЛС) и синтеза обучающих данных.

Ключевые слова: нейросетевые инструменты, радиолокационные системы (РЛС), типичные архитектуры, адаптивность.

APPLICATION OF NEURAL NETWORK TOOLS IN RADAR

Bakulev A.V., T.R. Boatman

V.F. Utkin Ryazan State Radio Engineering University, Russian Federation, Ryazan, botsman.tatjana@yndex.ru

Abstract. The paper discusses the possibilities of integrating deep learning into the processing of radar information. Special attention is paid to the transition from classical deterministic algorithms to adaptive neural network models in the tasks of interference filtering, target recognition, cognitive management of resources of radar systems (radar), and synthesis of training data.

Keywords: neural network tools, radar systems (radar), typical architectures, adaptability.

До появления нейронных сетей в радиолокации наиболее эффективными считались некоторое количество ключевых методов обработки сигналов, которые и сейчас решают задачи обнаружения, фильтрации и отслеживания целей. Эти методы заложили основу для развития современных систем.

Традиционные методы обработки сигналов в радиолокации

Фильтр Калмана – это рекурсивный алгоритм, который оценивает вектор состояния динамической системы на основе неполных и зашумлённых измерений. Он оптимален по критерию минимума среднеквадратической ошибки и широко применялся в системах траекторного сопровождения воздушных объектов. Модификации фильтра (например, с разными коэффициентами для описания прямолинейного, плавного или сложного манёвренного движения) позволяли адаптировать его к различным условиям.

Согласованная фильтрация основана на использовании фильтра, оптимизированного под конкретный тип сигнала и позволяет максимизировать отношение сигнал/шум на выходе.

Алгоритмы CFAR (Constant False Alarm Rate – постоянная вероятность ложных тревог) адаптируют порог обнаружения к уровню помех, поддерживая заданный уровень ложных тревог.

Методы вторичной обработки включают алгоритмы формирования траекторий, которые объединяют отметки от разных обзоров в единые траектории целей. Традиционные алгоритмы основываются на предположении о прямолинейном равномерном движении целей и их достаточной удалённости друг от друга. Используются стробы (области вокруг предполагаемого положения цели), и отметки, попавшие в строб, которые связываются с соответствующей траекторией.

Методы на основе байесовского подхода и линейного комбинирования признаков применяются для распознавания целей. Байесовский подход позволяет оптимизировать решающие правила, минимизируя ошибки. Линейное комбинирование признаков используется для классификации объектов, хотя такие методы не всегда обеспечивают оптимальную эффективность из-за ограничений линейной модели.

В настоящее время традиционные алгоритмы цифровой обработки сигналов (ЦОС) сталкиваются с рядом ограничений, в результате чего возникает необходимость перехода от жестких математических моделей к адаптивным нейросетевым архитектурам.

Основные принципы работы нейронных сетей

Нейронная сеть – это математическая модель, состоящая из взаимосвязанных нейронов, которые обрабатывают информацию. Нейроны объединены в слои: входной, скрытые и выходной. Данные поступают на входной слой, проходят через скрытые слои, где происходит их обработка, и выходят через выходной слой в виде результата.

Обучение нейронной сети происходит на основе набора данных (обучающей выборки), где для каждого входного сигнала известен желаемый выходной результат («учитель»). В процессе обучения сеть корректирует веса связей между нейронами, чтобы минимизировать разницу между фактическим и желаемым выходом. Один из распространённых методов обучения – обратное распространение ошибки [3].

Ключевые свойства нейронных сетей

- **Нелинейность.** Способность моделировать нелинейные зависимости, что важно для радиолокации, где физические процессы часто нелинейны.
- **Адаптивность**. Возможность адаптироваться к изменениям внешней среды и обобщать знания на новые данные.
- **Способность к распознаванию образов**. Нейронные сети эффективно выявляют паттерны и признаки в данных, что используется для классификации объектов и фильтрации шума.

За счет этих свойств НС способны решить следующие проблемы классических алгаритмов ЦОС.

- Нелинейность систем и сигналов.
- Работа с негауссовскими шумами и сложными помехами.
- Обработка больших объёмов данных и высокая размерность
- Адаптация к изменяющимся внешним условиям.
- Распознавание образов и классификация целей.
- Решение задач, не формализуемых классическими методами.
- Траекторное сопровождение и сглаживание отметок.
- Повышение разрешающей способности.

Внедрение нейросетевых инструментов в рамках САПР позволяет существенно повысить эффективность, гибкость и адаптивность РЛС [6].

Типичные архитектуры в радиолокации

Свёрточные сети (CNN). Основной элемент – операция свёртки: фильтр (ядро) «скользит» по входным данным, вычисляя скалярное произведение между своими весами (числовыми параметрами, определяющими силу связи между нейронами) и локальными участками данных. В результате формируются карты признаков – результат применения фильтра к входным данным, где каждый элемент показывает наличие определённого паттерна (края, текстуры, формы) в соответствующей области.

Ключевые компоненты:

- свёрточные слои – извлекают локальные признаки (линии, углы, текстуры);
- пулинговые слои (pooling) – уменьшают размерность карт признаков, повышая устойчивость к сдвигам (например, max pooling выбирает максимальное значение в окне);
- полносвязные слои – принимают обобщённые признаки для классификации или регрессии.

Применяются для классификации и сегментации радиолокационных изображений (РЛИ), выделения контуров целей на фоне помех [5, 3].

*Рекуррентные сети (RNN/LSTM***)** – обрабатывают последовательности данных (текст, временные ряды, аудио), сохраняя «память» о предыдущих элементах. На каждом шаге сеть получает новый элемент последовательности и обновляет внутреннее состояние, которое передаётся на следующий шаг.

Проблемы простых RNN – затухание/взрыв градиента (вектора, указывающего направление наискорейшего роста функции, противоположного направлению обучения) при обучении длинных последовательностей.

Модификации для решения проблем:

1. LSTM (Long Short Term Memory) – имеет три механизма контроля потока информации (вентиля):
   а. забывание,
   б. вход,
   в. выход, контролирующих поток информации. Позволяет запоминать долгосрочные зависимости.
2. GRU (Gated Recurrent Unit) – упрощённая версия LSTM с двумя вентилями (обновления и сброса). Быстрее обучается, но может уступать в точности на длинных последовательностях.

Применяются для анализа траекторий и временных рядов (сопровождение целей, прогнозирование движения) [4,3].

Автоэнкодеры –состоят из двух частей:

1. Энкодер – сжимает входные данные в компактное представление (латентное пространство, которое содержит ключевые признаки без избыточности);
2. Декодер – восстанавливает исходные данные из сжатого вектора.

Цель обучения – минимизировать разницу между входом и выходом.

Разновидности:

- денойзинг автоэнкодеры – обучаются восстанавливать чистые данные из зашумлённых;
- сжимающие автоэнкодеры (Sparse Autoencoders) – искусственно сужают латентное пространство, выделяя ключевые признаки;
- вариационные автоэнкодеры (VAE) – позволяет генерировать новые данные через выборку из латентного пространств, моделируя распределение латентных переменных.

Применяются для шумоподавления, сжатия данных, обнаружения аномалий (необычных траекторий, новых типов помех) [6].

Генеративно состязательные сети (GAN, Generative Adversarial Networks) – состоят из двух конкурирующих сетей:

1. Генератор — создаёт синтетические данные (изображения, сигналы), пытаясь имитировать реальные;
2. Дискриминатор — оценивает, насколько данные реалистичны (настоящие или сгенерированные).

Обучение происходит в режиме «соревнования»: генератор старается обмануть дискриминатор, а дискриминатор — отличить подделку.

Проблемы GAN:

- нестабильность обучения;
- модальный коллапс (генератор выдаёт однотипные образцы).

Применяются для синтеза обучающих данных (имитация РЛИ редких целей), восстановления повреждённых кадров [3].

Гибридные модели — комбинируют сильные стороны разных типов сетей для решения сложных задач, например: комбинация CNN+RNN для задач «изображение + траектория» [3].

Помимо типичных архитектур в радиолокации применяются продвинутые, специализированные решения для сложных распределённых задач – **мультиагентные ИИ сети (MAS).**

Мультиагентная система (Multi Agent System, MAS) – это вычислительная система, состоящая из нескольких автономных ИИ агентов, которые взаимодействуют друг с другом и с внешней средой для решения сложных задач. В отличие от единой нейросети, которая пытается справиться со всем самостоятельно, MAS распределяет работу между несколькими «специалистами». [6].

Ограничивающие факторы применения НС

Несмотря на высокую эффективность, существуют ключевые проблемы применения НС, которые сейчас пытаются решить.

- Дефицит и низкое качество данных — нехватка размеченных наборов, дисбаланс классов, зашумлённость сигналов, динамичность среды [3, 6].
- Вычислительные ограничения — высокие требования к ресурсам, задержки в обработке реального времени, энергопотребление в мобильных системах.
- Плохая обобщаемость и переобучение — модели хорошо работают в условиях обучения, но дают сбои при изменении среды, параметров РЛС или появлении новых типов помех [6].
- Сложность интерпретации решений ИИ — «чёрные ящики» не объясняют логику выводов, что критично для ответственных задач (например, ПВО) [6].
- Трудности сопровождения целей — перекрытие отметок при плотном построении, маневрирующие и малоразмерные цели, нестационарные помехи [3].
- Интеграция с существующими системами — несовместимость с legacy оборудованием, проблемы синхронизации в многопозиционных РЛС, уязвимости в распределённых сетях [6].
- Основные направления решений:
- Синтетические данные и симуляция — использование GAN и симуляторов для генерации размеченных РЛИ и сигналов (в т.ч. редких сценариев и стелс целей) [3].

- Edge AI и специализированные ускорители — внедрение FPGA, ASIC и оптимизированных нейросетевых процессоров для работы в реальном времени и с низким энергопотреблением [6].
- Трансферное обучение — дообучение предобученных моделей на малых специализированных наборах данных [6, 3].
- Интерпретируемый ИИ (Explainable AI, XAI) — внедрение механизмов объяснения решений (тепловые карты внимания, анализ признаков) для повышения доверия и соответствия нормативным требованиям [6].
- Гибридные подходы — комбинация ИИ и классических методов (например, CNN + фильтр Калмана) для повышения точности и надёжности [1,5,3].
- Стандартизация — разработка единых протоколов взаимодействия, форматов данных и метрик качества для ИИ в радиолокации [6].

Интеграция нейросетевых инструментов в радиолокацию — это не замена классической ЦОС, а создание гибридных систем. Использование нейросетей в рамках САПР открыло путь к созданию интеллектуальных радиолокационных комплексов нового поколения — более адаптивных, надёжных и эффективных в сравнении с традиционными системами.

Библиографический список

1. Бакулев, П. А. Радиолокационные системы: учебник для вузов / П. А. Бакулев. — Москва: Радиотехника, 2004. — 320 с. — ISBN 5 93108 125 6.

2. Нечаев, Ю. Б. Современные методы обработки радиолокационной информации / Ю. Б. Нечаев, В. И. Пшеницын. — Москва: Горячая линия — Телеком, 2016. — 244 с. — ISBN 978 5 9912 0567 3.

3. Goodfellow, I. Generative Adversarial Nets / I. Goodfellow, J. Pouget Abadie, M. Mirza [et al.] // Advances in Neural Information Processing Systems (NeurIPS). — 2014.

4. Hochreiter, S. Long Short Term Memory / S. Hochreiter, J. Schmidhuber // Neural Computation. — 1997. — Vol. 9, No. 8. — P. 1735–1780.

5. Krizhevsky, A. ImageNet Classification with Deep Convolutional Neural Networks / A. Krizhevsky, I. Sutskever, G. E. Hinton // Communications of the ACM. — 2017. — Vol. 60, No. 6. — P. 84–90.

6. McMullen, P. Deep Learning for Radar: A Review / P. McMullen [et al.] // IEEE Aerospace and Electronic Systems Magazine. — 2020. — Vol. 35, No. 7. — P. 4–15.

СЕКЦИЯ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КОНСТРУИРОВАНИИ ЭЛЕКТРОННЫХ СРЕДСТВ»

УДК 681.51; ГРНТИ 50.43.17

АНАЛИЗ ВЛИЯНИЯ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ НА УСТОЙЧИВОСТЬ СИСТЕМЫ С ПЕРЕМЕННОЙ СТРУКТУРОЙ

С.В. Скворцов, В.И. Хрюкин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, vi_x@mail.ru

Аннотация. Рассмотрена система управления, в которой реализовано цифровое управление с переменной структурой. Целью работы является анализ влияния способа формирования регулирующего воздействия на объект, а также дискретизации измеряемого сигнала по времени и квантования по уровню на устойчивость движения системы. Для системы с объектом управления, описываемым дифференциальным уравнением второго порядка, получены аналитические соотношения для определения параметров алгоритма управления микроконтроллера, при которых в системе реализуется с требуемой точностью движение в квазискользящем режиме.

Ключевые слова: система с переменной структурой, объект управления, переключение структуры, дискретизация сигнала, пространство состояния, фазовые координаты, скользящий режим, конечные разности, непрерывные разности.

ANALYSIS OF THE IMPACT OF DIGITAL SIGNAL PROCESSING ON THE STABILITY OF A VARIABLE STRUCTURE SYSTEM

S.V. Skvortsov, V.I. Khryukin

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, vi_x@mail.ru

Abstract. A control system in which digital control with a variable structure is implemented is considered. The purpose of the work is to analyze the effect of the method of forming a regulatory effect on an object, as well as sampling of the measured signal in time and quantization in level on the stability of the system movement. For a system with a control object described by a second-order differential equation, analytical relations have been obtained to determine the parameters of the microcontroller's control algorithm, in which motion in a quasi-sliding mode is realized with the required accuracy in the system.

Keywords: variable structure system, control object, switching the structure, signal discretization, state space, vector of phase coordinates, sliding mode, finite differences, continuous differences.

Введение

Повышение качества систем управления в условиях наличия непредсказуемых и неконтролируемых воздействий требует использования нелинейных законов управления, к числу которых относятся методы с разрывным управлением [1]. Применение такого управления, при котором осуществляется скользящий режим вдоль многообразия поверхностей переключения, позволяет при определенных условиях добиться инвариантности системы, как к внешним воздействиям и возмущениям, так и к изменению параметров объекта управления [2].

Задача синтеза в системах с разрывными воздействиями обычно сводится к выбору поверхностей в фазовом пространстве состояния, на которых функция переключения претерпевает разрывы. При выполнении определенных соотношений в таких системах с переменной структурой (СПС) может возникнуть специфический вид движений – так называемый скользящий режим. Причем, как показано в [2], если функция управления формируется из регулируемой величины и ее производных, то движение в скользящем режиме не зависит от параметров объекта управления и внешних воздействий и определяется только коэффициентами уравнений гиперплоскости переключения. Этот факт и используется при построении

систем, которые обеспечивают, начиная с некоторого момента времени, движение в скользящем режиме с желаемыми динамическими свойствами.

Практическая реализация СПС приводит к существенному усложнению законов управления и диктует необходимость использования для их реализации цифровых устройств управления (микроконтроллеров) [3, 4]. В связи с этим приходится учитывать влияние на динамику системы ряда особенностей, присущих программной реализации законов управления: амплитудного квантования сигналов и их дискретизации по времени, способов формирования приближенных значений производных и т.д. Нелинейный характер законов управления еще более усложняет анализ таких систем.

В работе исследуется влияние времени дискретизации и времени задержки измеряемого сигнала для формирования конечных разностей первого порядка на динамику системы, поскольку увеличение запаздывания приводит к потере качества переходного процесса (появление квазискользящего режима) и даже устойчивости СПС.

Теоретическая часть

Рассмотрим свободное движение СПС, описываемое уравнениями вида

$$\frac{dx_1}{dt} = x_2; \tag{1}$$

$$\frac{dx_2}{dt} = a_2 x_2 + a_1 x_1 + bu, \tag{2}$$

где $x_1 = x$ – измеряемый сигнал ошибки;

a_1, a_2, b – параметры объекта управления;

u – сигнал управления, который определяется как

$$u = \varphi x;$$

$$\varphi = \begin{cases} \alpha \text{ при } S[nT]x > 0; \\ \beta \text{ при } S[nT]x < 0; \end{cases}$$

$$S[nT] = \Delta x[nT] + cx[nT]; \tag{3}$$

$$x[nT] = x(nT) + \delta(t)x_0. \tag{4}$$

Здесь α и β - параметры регулятора;

$s[nT]$ – функция переключения;

$\Delta x[nT]$ – конечная разность первого порядка, формируемая через период $\tau = kT$ (k = 1, 2,…):

$$\Delta x[nT] = \frac{x[nT] - x[(n-k)T]}{kT};$$

c – коэффициент наклона линии переключения, выбираемый из требований обеспечения динамических свойств системы в скользящем режиме;

T – период дискретизации измеряемого сигнала по времени (n = 0, 1, 2, …);

x_0 – вес единицы младшего разряда;

$\delta(t)$ – ошибка квантования по уровню, удовлетворяющая условию $-0{,}5 \le \delta(t) \le 0{,}5$.

Предположим, что коэффициент c выбран таким образом [2], что в системе (1) осуществляется скользящий режим по линии

$$S' = x_2 + cx_1 = 0.$$

Реализация $S[nT]$ в виде (3) приводит к тому, что при определенном выборе значений τ, T и x_0 движение в системе будет проходить не в скользящем режиме по линии переключения S', а в некоторой ее окрестности. Эти отклонения обусловлены следующими причинами:

- заменой производной конечной разностью при формировании S;
- ошибкой в определении координаты из-за квантования по уровню.

В работе [5] рассмотрено влияние запаздывания τ при формировании функции переключения с помощью непрерывных разностей на качество скользящего режима. В частности, показано, что переключения в системе происходят не на линии

$$x_2 + cx_1 = 0,$$

а на прямых

$$x_2 + c^* x_1 = 0,$$

где

$$c^* = \frac{c + \frac{(a_1+\varphi)\tau}{2}\left\{1 + \frac{a_2\tau}{3} + \frac{[a_2^2 - (a_1+\varphi)]\tau^2}{12} + \ldots\right\}}{1 + \frac{\tau}{2}\left\{a_2 + \frac{a_2^2 - (a_1+\varphi)\tau}{3} + \frac{[a_2^3 - 2a_2(a_1+\varphi)\tau^2]}{12} + \ldots\right\}}.$$

Такой подход справедлив лишь для случая, когда $\tau >> T$ и квантованием по уровню можно пренебречь. Однако при соизмеримости значений τ и T необходимо учитывать тот факт, что измерения сигнала $x_1(t)$ происходят в дискретные моменты времени $t = nT$. Следовательно, и смена структуры в (1) будет осуществляться не в моменты, когда $S = 0$, а с некоторой задержкой. Очевидно, что эта задержка может меняться в пределах от 0 до T и наибольшее отклонение от линии $x_2 + c^* x_1 = 0$ будет происходить на линии

$$S(t - T) = 0,$$

где $S(t)$ определяется через непрерывные разности:

$$S(t) = \frac{x_1(t) - x_1(t-\tau)}{\tau} + cx_1(t) = x_2 + c^* x_1.$$

Используя методику, изложенную в работе [5], можно показать, что

$$S(t - T) = k_1 x_1(t) + k_2 x_2(t),$$

где k_1 и k_1 определяются через параметры системы и выражаются в виде рядов по степеням T и τ:

$$k_1 = \frac{\Delta_1}{\Delta}; \qquad k_1 = \frac{\Delta_1}{\Delta},$$

где

$$\Delta_1 = \begin{vmatrix} e^{-\lambda_1 T}(\lambda_1 + c^*) & \lambda_1 \\ e^{-\lambda_2 T}(\lambda_2 + c^*) & \lambda_2 \end{vmatrix}; \qquad \Delta_2 = \begin{vmatrix} 1 & e^{-\lambda_1 T}(\lambda_1 + c^*) \\ 1 & e^{-\lambda_2 T}(\lambda_2 + c^*) \end{vmatrix}; \qquad \Delta_2 = \begin{vmatrix} 1 & \lambda_1 \\ 1 & \lambda_2 \end{vmatrix}.$$

Представляя, как

$$e^{-\lambda_j T} = \sum_{n=1}^{\infty} (-1)^n \frac{T^n}{n!} \lambda_j^n; \quad j = 1, 2$$

и учитывая, что

$$\lambda_1 + \lambda_2 = -a_1; \quad \lambda_1 \lambda_2 = (a_1 + \varphi)$$

после исключения нулевых слагаемых получим:

$$c^{**} = \frac{c + (a_1 + \varphi)T\left\{1 + \frac{a_2 T}{2} + \frac{[a_2^2 - (a_1 + \varphi) - c^* a_2]T^2}{6} + \ldots\right\}}{1 + a_2 T + T^2 \frac{a_2^2 - (a_1 + \varphi)c^* a_2}{2} + T^3 \frac{a_2^3 - 2(a_1 + \varphi) + c^*[a_2^2 - (a_1 + \varphi)]}{6} + \ldots}.$$

Таким образом, дискретизация измеряемого сигнала по времени приводит к тому, что переключения в системе происходят на прямых $x_2 + c^{**}x_1 = 0$. Для того, чтобы изображающая точка не покинула область фазовой плоскости, ограниченную этими прямыми, т.е. в системе (1) существовал квазискользящий режим, достаточно выполнения условий:

$$\begin{cases} \alpha > \max\{-a_1 + c^{**}(\alpha)a_2 - [c^{**}(\alpha)]^2\}; \\ \beta < \min\{-a_1 + c^{**}(\beta)a_2 - [c^{**}(\beta)]^2\}. \end{cases}$$

Данные неравенства определяют ограничения на параметры системы, время запаздывания τ и период дискретизации T, при которых обеспечивается существование квазискользящего режима.

Выше отмечалось, что кроме уже рассмотренных неидеальностей, на динамику системы (1) при формировании функции переключения в виде (3), влияет также квантование по уровню. Оно приводит к появлению ошибки в пределах веса единицы младшего разряда. Подставив (4) в (3), получим:

$$S[nT] = \Delta x[nT] + cx[nT] + F(t)x_0,$$

где

$$F(t) = \frac{\delta(t) - \delta(t - T)}{T} + c\delta(t),$$

причем

$$\max F(t) = -\min F(t) = \frac{1}{T} + \frac{c}{2} = F_0.$$

Таким образом, границы области, в которой происходит смена структуры, определяется прямыми

$$x_2 + c^{**}(\alpha)x_1 + F(t)x_0 = 0;$$
$$x_2 + c^{**}(\beta)x_1 - F(t)x_0 = 0;$$

Это позволяет выбрать вес единицы младшего разряда x_0 так, чтобы движение происходило в квазискользящем режиме до значения регулируемой координаты меньше заданной ошибки.

Выводы

В работе показано, что в результате цифровой обработки информации микроконтроллером происходит изменение динамики СПС по сравнению с системами с полной информацией о фазовых координатах, что может привести к потере устойчивости движения в квазискользящем режиме. При этом основное влияние на поведение цифровой СПС оказывает запаздывание, вносимое микроконтроллером, дискретизация сигнала ошибки по времени и квантование по уровню, а также то, что вместо производной от сигнала ошибки используется ее приближенное значение, определяемое через конечные разности.

Получены соотношения, позволяющие рассмотреть движение цифровой СПС с объектом управления, описываемым дифференциальным уравнением второго порядка, в каноническом пространстве состояния (фазовом пространстве). Это позволяет использовать принципы исследования идеальной СПС для определения условий существования квазискользя-

щего режима в цифровой системе. Полученные результаты предполагается адаптировать к проектированию специализированных систем управления нестационарными объектами (например, робототехническими комплексами [6]), для которых характерно значительное изменение параметров.

Библиографический список

1. Ким Д. П. Теория автоматического управления. Многомерные, нелинейные, оптимальные и адаптивные системы. М.: Издательство Юрайт, 2025. 331 с.

2. Utkin V. I. Sliding modes in control and optimization. New York, Springer-Verlag. 1991. 286 p.

3. Скворцов С. В., Хрюкин В. И., Скворцова Т. С. Параметрический синтез цифрового ПИД-регулятора на основе аналитико-графической модели системы управления // Вестник Рязанского государственного радиотехнического университета. 2025. № 91. С. 220-232.

4. Скворцов С. В., Хрюкин В. И., Скворцова Т. С. Аналитико-графическое моделирование систем управления на основе ПИД-регуляторов // Вестник Рязанского государственного радиотехнического университета. 2024. № 87. С. 78-88.

5. Виноградов Ю. Л. Определение допустимого времени запаздывания при формировании функции переключения в системах с переменной структурой // Приборостроение. 1987. № 6. С. 17-23.

6. Бобиков А. И., Корниенко М. Д. Оптимальное нестационарное управление многосвязными объектами // Вестник Рязанского государственного радиотехнического университета. 2023. № 84. С. 176-186.

УДК 004.023; ГРНТИ 20.01

АРХИТЕКТУРНЫЕ ОСОБЕННОСТИ ПАРАЛЛЕЛЬНОГО ГЕНЕТИЧЕСКОГО АЛГОРИТМА МНОГОКРИТЕРИАЛЬНОЙ QOS-МАРШРУТИЗАЦИИ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

А.Н. Сапрыкин, А.А. Тихонов

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, saprykin.a.n@rsreu.ru

Аннотация. В работе рассматривается вариант решения задачи многокритериальной QoS-маршрутизации в программно-конфигурируемых сетях с помощью параллельной модификации генетического алгоритма с применением композитных метрик. На основе предложенного алгоритма выполнена разработка вычислительного модуля с асинхронной реализацией генетических операторов с использованием языка программирования Go. Приведена оценка эффективности асинхронного подхода при условии соответствия числа рабочих потоков количеству аппаратных ядер процессора.

Ключевые слова: генетический алгоритм, эвристические методы, QoS-маршрутизация, программно-конфигурируемые сети.

ARCHITECTURAL FEATURES OF THE PARALLEL GENETIC ALGORITHM OF MULTICRITERIAL QOS ROUTING IN SOFTWARE-DEFINED NETWORKS

A.N. Saprykin, A.A. Tikhonov

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, saprykin.a.n@rsreu.ru

The summary. The paper considers a solution to the problem of multi-criteria QoS routing in software-defined networks using parallel modification of a genetic algorithm using composite metrics. Based on the proposed algorithm, a computational module with asynchronous implementation of genetic operators using the Go programming language was developed. An evaluation of the effectiveness of the asynchronous approach is given, provided that the number of operating currents corresponds to the number of processor hardware cores.

Keywords: genetic algorithm, heuristic methods, QoS routing, software-defined networks.

Программно-конфигурируемые сети представляют собой перспективную архитектурную парадигму, обеспечивающую гибкость, централизованное управление и динамическую

адаптацию сетевой инфраструктуры под меняющиеся требования приложений и пользователей. Одной из ключевых задач в программно-конфигурируемых сетях является обеспечение маршрутизации с гарантированным качеством обслуживания (Quality of Service, QoS), особенно в условиях роста трафика, разнообразия сервисов и требований к задержкам, пропускной способности и надёжности.

Основной проблемой многокритериальной QoS-маршрутизации является большая вычислительная сложность решающих эту задачу алгоритмов, а также существенное время их работы. Ввиду невозможности или неоптимальности классических подходов к решению данной задачи, появляется необходимость в применении эвристических методов, что может сильно сократить фактическую вычислительную нагрузку на систему и время расчётов. Одной из важнейших проблем многокритериальной QoS-маршрутизации является наличие множества метрик, которые необходимо в конечном итоге оптимизировать. Одним из вариантов её решения является компоновка набора из N метрик в одну, на подобие того, как это происходит в алгоритме Larac [3]. Варианты реализации применения такой компоновки представлены в работах [1] и [4]. Такой подход позволяет свести задачу многокритериальной оптимизации к оптимизации общей метрики, полученной методом предобработки данных, таким образом независимо от количества оптимизируемых метрик, вычислительная сложность основного алгоритма будет оставаться неизменной.

Таким образом, сведение многокритериальной задачи к однокритериальной за счёт предварительной агрегации метрик создаёт благоприятные условия для применения эвристических методов поиска, в частности генетических алгоритмов, которые способны эффективно работать с единой целевой функцией. Однако даже при упрощённой постановке задачи время выполнения таких алгоритмов может оказаться неприемлемым для динамических сетевых сред, где требуется оперативное принятие решений. В этой связи особую значимость приобретают подходы, направленные на снижение временной сложности за счёт распараллеливания вычислений.

В контексте применения генетических алгоритмов к задачам маршрутизации в программно-конфигурируемых сетях следует отметить работу [2], в которой рассмотрена многопутевая QoS-маршрутизация с использованием генетического алгоритма для балансировки потоков данных. В указанной работе, однако, не применяется агрегация множества метрик качества обслуживания в единую композитную целевую функцию, а оптимизация осуществляется по отдельным критериям в рамках многоцелевого подхода. Кроме того, реализация алгоритма выполнена в однопоточном режиме, что ограничивает его применимость в сценариях, требующих быстрого реагирования на изменения сетевой топологии или трафика.

Методология параллельной модификации генетического алгоритма для решения задачи маршрутизации

В работе [5] предложен подход к распараллеливанию генетического алгоритма, основанный на выполнении однотипных вычислительных операций независимо и одновременно на нескольких вычислительных ядрах. Данный метод позволяет сократить общее время выполнения алгоритма за счёт исключения необходимости синхронизации и обмена данными между потоками на этапах эволюционных преобразований. Указанный подход был взят за основу при разработке рассматриваемого варианта генетического алгоритма. Ниже приведено его алгоритмическое описание.

Пункт 1. Инициализация параметров алгоритма. Определение размера популяции, вероятности скрещивания и мутации, максимального число поколений MAX_GEN и порогового значения числа поколений без улучшения глобального решения EARLY_STOP.

Пункт 2. Асинхронная генерация начальной популяции, в которой особи формируются параллельно и независимо друг от друга.

Пункт 3. Пока текущее число итераций не превысило MAX_GEN:

Пункт 3.1. Асинхронный турнирный отбор родительских особей.

Пункт 3.2. Асинхронное скрещивание с заданной вероятностью.

Пункт 3.3. Асинхронная мутация с заданной вероятностью.

Пункт 3.4. Определение лучшей особи текущего поколения по значению функции приспособленности.

Пункт 3.5. Если найденная особь превосходит текущего глобального лидера (наилучшую особь за всё время выполнения), перейти к пункту 3.6, иначе – к пункту 3.7.

Пункт 3.6. Обновление глобального лидера.

Пункт 3.7. Если за последние EARLY_STOP поколений не произошло улучшения глобального решения, завершить цикл; в противном случае – продолжить выполнение с пункта 3.1.

Выбор языка программирования для реализации предложенного алгоритма определяется рядом факторов, среди которых наиболее значимыми являются поддержка эффективных механизмов параллелизма и практическая целесообразность развёртывания в среде программно-конфигурируемой сети.

Язык Java обладает развитыми встроенными средствами для асинхронного программирования, однако его использование требует наличия Java Virtual Machine, что может быть избыточным для размещения на ресурсоограниченном сервере контроллера программно-конфигурируемых сетей, особенно в случае изолированного вычислительного модуля. Языки C/C++ предоставляют низкоуровневый доступ к системным потокам, однако управление ими сопряжено со значительными накладными расходами как на этапе разработки, так и во время выполнения, что снижает общую эффективность распараллеливания. Интерпретируемый язык Python, несмотря на простоту использования, ограничен в возможностях истинного параллелизма из-за глобальной блокировки интерпретатора, что делает его малопригодным для CPU-интенсивных вычислений.

В отличие от перечисленных решений, язык Go (Golang) обеспечивает высокоуровневую абстракцию параллелизма посредством горутин – лёгковесных конкурентных единиц исполнения, управляемых планировщиком времени выполнения. Кроме того, Go является компилируемым языком, что исключает накладные расходы, характерные для интерпретируемых сред, и способствует повышению производительности вычислительного модуля. Эти особенности обусловили выбор Go в качестве основной платформы реализации предложенного алгоритма.

Для представления решений в генетическом алгоритме используется структура данных, инкапсулирующая маршрут и сопутствующие характеристики. Несмотря на отсутствие в языке Go классической объектно-ориентированной модели с наследованием и полиморфизмом, применение составных типов обеспечивает эффективную агрегацию связанных полей и удовлетворяет требованиям к представлению особи в рамках поставленной задачи. Структура особи, реализующая кодирование маршрута в графе сети, приведена ниже.

```
type Individual struct {
  Path []int // Последовательность узлов маршрута
  Weights []int // Веса рёбер между последовательными узлами
  Fitness int // Значение функции приспособленности
  IsValid_ bool // Флаг корректности маршрута
}
```

Генерация корректного индивида осуществляется по следующему алгоритмическому описанию:

Пункт 1. Инициализация текущего узла начальной вершиной маршрута и установка счётчика возвратов в нулевое значение.

Пункт 2. Определение множества соседних непосещённых узлов на основе матрицы смежности.

Пункт 3. Если множество соседей пусто, то при условии, что текущий узел не является начальным – возврат к предыдущему узлу маршрута с инкрементом счётчика возвратов. В противном случае – прерывание генерации и инициализация нового индивида.

Пункт 4. При превышении допустимого порога числа возвратов генерация маршрута прекращается как неудачная.

Пункт 5. Случайный выбор следующего узла из множества допустимых соседей.

Пункт 6. Пометка выбранного узла как посещённого и добавление его в последовательность Path.

Пункт 7. Если достигнута целевая вершина – завершение генерации; в противном случае осуществляется возврат к пункту 2.

Данный алгоритм гарантирует формирование ациклических маршрутов, соединяющих заданные начальную и конечную вершины, что является необходимым условием валидности решения в задаче маршрутизации.

Оператор турнирной селекции реализован в соответствии с классической схемой: из случайно выбранных трёх особей популяции (либо всех имеющихся особей при размере популяции менее трёх) в качестве родителя отбирается особь с максимальным значением функции приспособленности. Данный подход обеспечивает баланс между селективным давлением и сохранением генетического разнообразия в популяции.

Оператор кроссинговера реализован как модифицированное одноточечное скрещивание с обязательной нормализацией результирующих маршрутов. Для пары родительских особей определяется общая вершина, присутствующая в обоих путях, которая служит точкой разделения. Префикс одного родителя до данной вершины комбинируется с суффиксом другого родителя после неё, формируя потомка. Поскольку подобная комбинация может привести к образованию циклов, выполняется постобработка маршрута: при обнаружении повторяющихся вершин удаляется фрагмент между первым и вторым вхождением, что гарантирует ацикличность и корректность получаемого решения.

Оператор мутации предназначен для преодоления локальных оптимумов и предотвращения преждевременной сходимости алгоритма. С заданной вероятностью в хромосоме выбирается точка мутации – промежуточная вершина маршрута. Фрагмент пути, следующий после данной вершины, отбрасывается и заменяется новым участком, сгенерированным посредством стохастического обхода графа от точки мутации до целевой вершины при соблюдении ограничения на отсутствие циклов. Такой механизм обеспечивает локальное разнообразие решений без нарушения допустимости маршрутов.

Реализация асинхронного выполнения генетических операторов на основе горутин языка Go

Все описанные выше генетические операторы реализованы в асинхронном режиме с использованием легковесных конкурентных примитивов языка Go, известных как горутины, совместно с механизмом синхронизации sync.WaitGroup. Такой подход позволяет эффективно распараллеливать вычисления на уровне отдельных особей популяции без необходимости явного управления потоками операционной системы.

Ключевым преимуществом горутин по сравнению с традиционными потоками является их минимальная потребляемая память и управление планировщиком времени выполнения Go, который мультиплексирует большое число горутин на ограниченном пуле системных потоков. Это обеспечивает высокую масштабируемость и низкие накладные расходы даже при обработке тысяч параллельных задач, что особенно актуально для эволюционных алгоритмов с крупными популяциями.

Пример реализации асинхронной мутации представлен ниже.

```
func mutateParallel(offspring []*Individual, matrix [][]int, pMutation float64) []*Individual {
    var wg sync.WaitGroup
    for i := range offspring {
        wg.Add(1)
        go func(index int) {
            defer wg.Done() // Отложенное завершение элемента ожидания
            if rand.Float64() < pMutation {
                offspring[index] = mutate(offspring[index], matrix)
            }
        }(i)
    }
    wg.Wait()
    return offspring
}
```

Следует отметить, что достижение реального ускорения при таком распараллеливании возможно лишь при соблюдении следующих условий: объём вычислительной работы на одну задачу достаточен для компенсации накладных расходов на запуск горутины, общее число активных конкурентных задач не превышает аппаратные возможности системы, в частности количество логических ядер процессора. В противном случае параллелизм может не дать выигрыша во времени или даже привести к деградации производительности из-за избыточного переключения контекста. В рамках рассматриваемой задачи QoS-маршрутизации указанные условия выполняются, что подтверждается экспериментальной оценкой временных характеристик реализованного модуля.

Выводы

В работе описана архитектура параллельного генетического алгоритма для решения задачи многокритериальной QoS-маршрутизации в программно-конфигурируемых сетях с применением композитных метрик. Скаляризация множества метрик качества обслуживания в единую агрегированную функцию приспособленности позволило снизить размерность оптимизационной задачи и стабилизировать вычислительную сложность независимо от числа критериев. Организация параллельного выполнения генетических операторов на уровне отдельных особей популяции посредством горутин языка Go обеспечило эффективное использование многоядерных вычислительных ресурсов контроллера программно-конфигурируемых сетей без избыточных накладных расходов на синхронизацию.

Разработанная архитектура параллельного генетического алгоритма гарантирует корректность генерируемых маршрутов за счёт строгой валидации на этапе инициализации особей и обязательной нормализации после генетических операций, исключающей образование циклов и разрывов в путях. Применение легковесных конкурентных примитивов в сочетании с компилируемой природой языка Go позволило достичь значимого сокращения времени вычислений по сравнению с последовательными реализациями, что критически важно для обеспечения оперативного принятия решений в динамически изменяющейся сетевой среде. Полученные результаты подтверждают целесообразность использования эвристических методов с аппаратно-ориентированным распараллеливанием для решения вычислительно трудоёмких задач управления трафиком в программно-конфигурируемых сетях.

Библиографический список

1. Перепёлкин, Д.А. Многопоточная реализация генетического алгоритма для многокритериальной QoS-маршрутизации в программно-конфигурируемых сетях. / Д.А. Перепёлкин, А.Н. Сапрыкин, А.А. Тихонов // Вестник Рязанского радиотехнического университета. – 2025. № 94. – С.68-84.
2. Перепелкин Д.А., Нгуен В.Т. Исследование и анализ процессов многопутевой маршрутизации и балансировки потоков данных в программно-конфигурируемых сетях на основе генетического алгоритма / Д.А. Перепелкин, В.Т. Нгуен // Вестник Рязанского государственного радиотехнического университета. – 2022. № 79. – С. 31-48.
3. Корячко, В.П. Программно-конфигурируемые сети. Учебник для вузов. / В.П. Корячко, Д.А. Перепелкин // М.: Горячая линия – Телеком. – 2020. – 288 с.
4. Корячко, В.П. Теоретические основы САПР. / В.П. Корячко, В.М. Курейник, И.П. Норенков // Энергоатомиздат. – 1987. – 400 с.
5. Скворцов, С.В. Ускорение генетического алгоритма решения транспортной задачи средствами многопоточного программирования. / С.В. Скворцов, М.С. Дьяков // Вестник Рязанского радиотехнического университета. – 2023. № 84. – С.99-107.

УДК 004.896; ГРНТИ 28.23.29

РАЗРАБОТКА МОДУЛЬНОЙ СИСТЕМЫ РАСПОЗНАВАНИЯ РЕЧИ С ПОДДЕРЖКОЙ ДИАРИЗАЦИИ И ДООБУЧЕНИЯ МОДЕЛИ НА БАЗЕ VOSK

С.Н. Бурцева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, burtsevaaas@yandex.ru

Аннотация. В статье представлена архитектура и процесс разработки программного модуля для преобразования аудиоданных в текстовую форму. Система поддерживает обработку как предзаписанных аудиофайлов, так и потокового аудио с микрофона. Особое внимание уделено механизму дообучения модели для распознавания специализированных аббревиатур и терминов, а также реализации упрощённой диаризации для идентификации отдельных участников диалога. Результат работы модуля экспортируется в структурированный JSON-файл с временными метками и идентификаторами спикеров.

Ключевые слова: распознавание речи, Vosk, диаризация, дообучение модели, Python, PyQt5, транскрибация, аббревиатуры, JSON.

DEVELOPMENT OF A MODULAR SPEECH RECOGNITION SYSTEM WITH SUPPORT FOR DIARIZATION AND MODEL REFINEMENT BASED ON VOSK

S.N. Burtseva

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, burtsevaaas@yandex.ru

Abstract. The article presents the architecture and development process of a software module for converting audio data into a text form. The system supports processing of both pre-written audio files and streaming audio from a microphone. Special attention is paid to the mechanism of further training of the model for recognizing specialized abbreviations and terms, as well as the implementation of simplified diarization for identifying individual participants in the dialogue. The result of the module is exported to a structured JSON file with timestamps and speaker IDs.

Keywords: speech recognition, Vosk, diarization, model refinement, Python, PyQt5, transcription, abbreviations, JSON.

Введение

В современных условиях растёт потребность в автоматизации обработки аудиозаписей: расшифровка совещаний, создание субтитров, документирование телефонных переговоров и т.д. Из данных потребностей следует разработка алгоритмов и систем, способных ав-

томатически преобразовывать акустический речевой сигнал в текстовое представление, преодолевая при этом фундаментальные проблемы изменчивости человеческого голоса, влияния шумов и неоднозначности естественного языка. От первых экспериментов с ограниченными словарями до современных нейросетевых архитектур, лежащих в основе виртуальных ассистентов и систем транскрибации, эволюция этой технологии отражает не только прогресс в области вычислительной техники, но и стремление к созданию наиболее естественного интерфейса взаимодействия человека и машины [1].

Существующие облачные решения (Google Speech-to-Text, Yandex SpeechKit) требуют постоянного подключения к интернету и могут быть небезопасны для обработки конфиденциальной информации.

Данный проект представляет собой оффлайн-решение на базе открытой библиотеки Vosk, которое работает локально, не требует сетевого подключения и позволяет гибко настраивать словарь распознавания под конкретную предметную область.

Актуальность

Данный проект находит решение для следующих проблем:

1) конфиденциальность: полная локальная обработка без отправки на сервер;
2) специфическая лексика: механизм дообучения словаря аббревиатурами;
3) разделение спикеров: базовая диаризация по паузам в речи;
4) структурированный вывод: JSON с таймкодами и метаданными;
5) узкоспециализированная среда: работает без интернета, минимальные зависимости.

Проект особенно актуален для корпоративной среды (совещания, интервью), специализированных организаций (техническая документация, аббревиатуры), оффлайн-сценариев (удалённые локации, защищённые сети).

В основе системы лежит библиотека Vosk, использующая нейросетевую архитектуру Kaldi с глубокими нейронными сетями (DNN/HMM-гибрид). Это обеспечивает высокое качество распознавания даже на устройствах с ограниченными вычислительными ресурсами.

Этапы разработки

Этап 1: Прототипирование интерфейса

Создание базового GUI на PyQt5 с двумя кнопками: выбор файла и запись с микрофона.

Этап 2: Интеграция Vosk

Подключение библиотеки распознавания речи, настройка потоковой обработки аудио.

Этап 3: Модульная архитектура

Рефакторинг кода: разделение на логические модули (UI, аудио, модели, утилиты).

Этап 4: Дообучение модели

Реализация механизма добавления кастомных аббревиатур в словарь модели.

Этап 5: Диаризация и экспорт

Добавление разделения спикеров по паузам, сохранение результатов в JSON.

Этап 6: Тестирование и оптимизация

Проверка работы с различными аудиофайлами, настройка порогов диаризации.

Архитектура и алгоритм работы программы:

Архитектура программы представлена на рисунке 1:

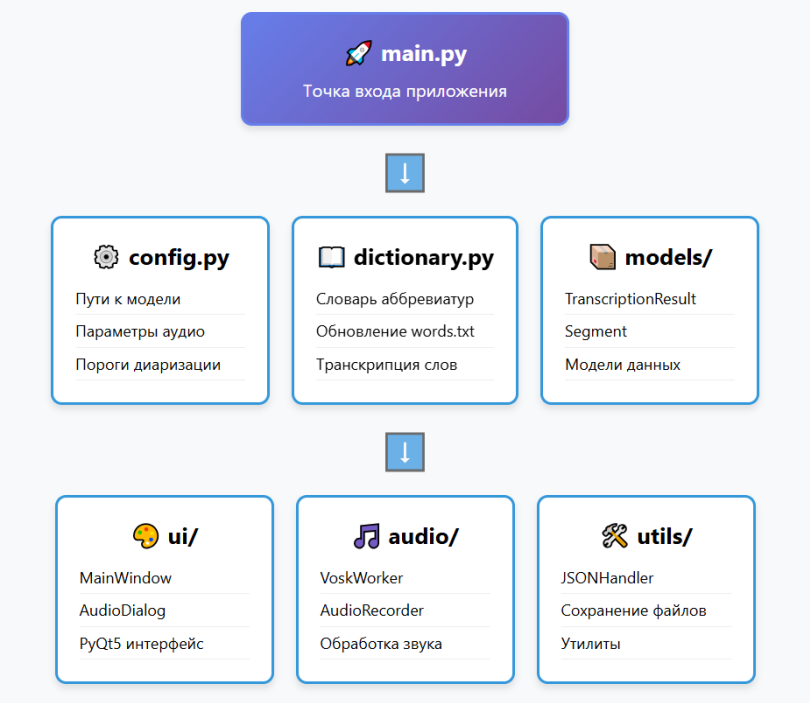


Рис.1. Архитектура программы

Алгоритм использования модуля представлен на рисунках 2-4:

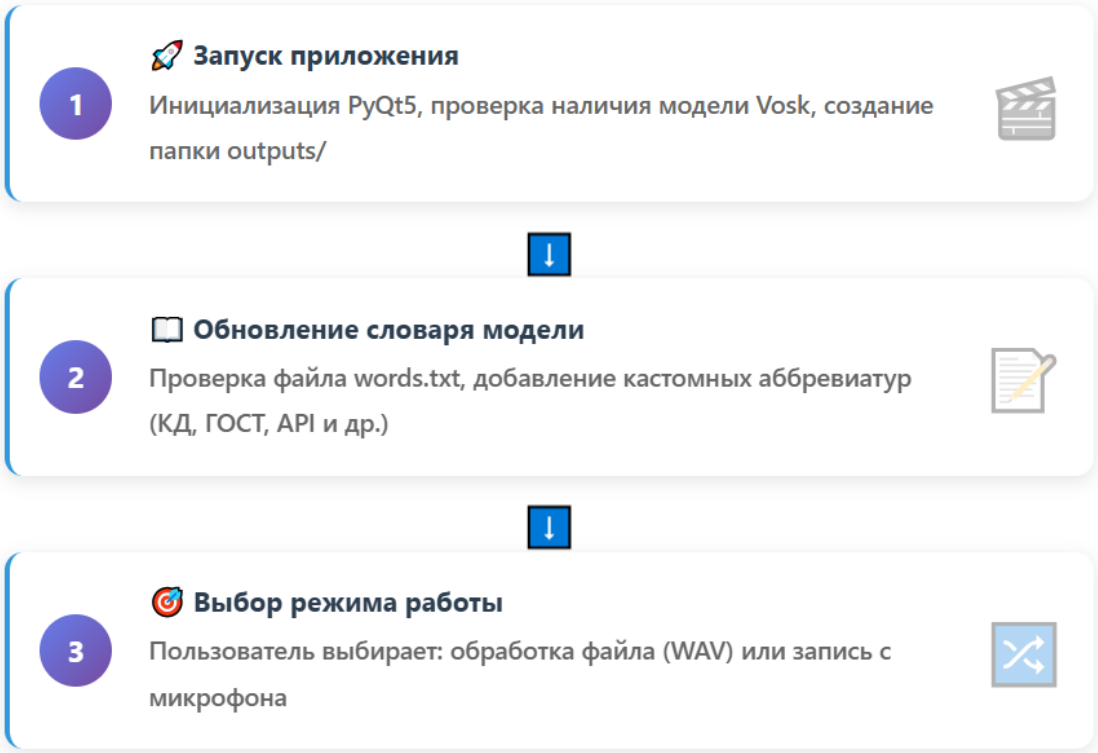


Рис. 2. Алгоритм работы программы

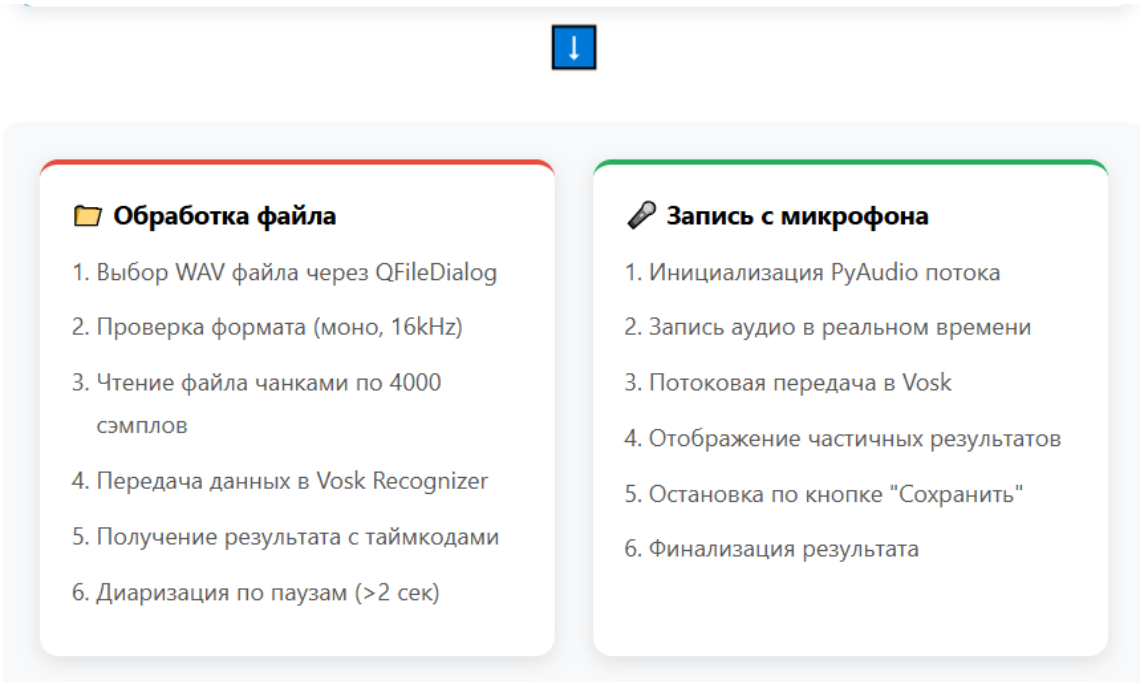


Рис.3. Алгоритм работы программы

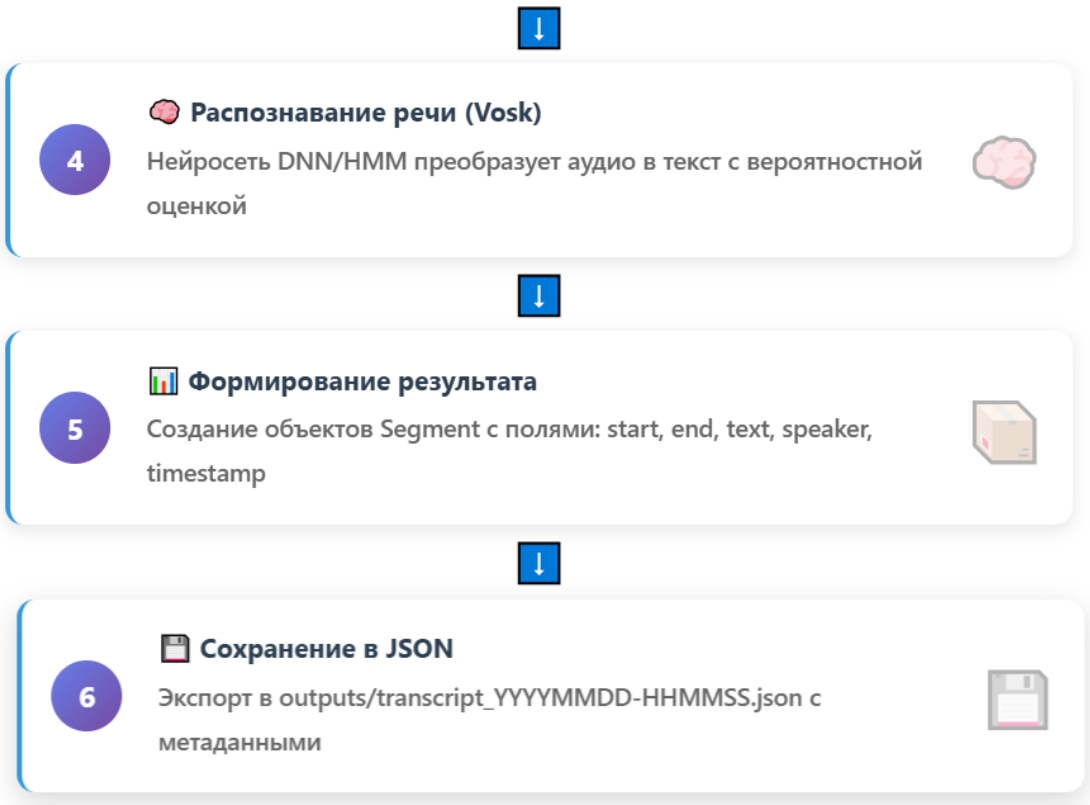


Рис. 4. Алгоритм работы программы

Формат словаря аббревиатур и формат выходных данных:

```
CUSTOM_ABBREVIATIONS = {
 "КД": "к э д э",        # Конструкторская документация
 "ГОСТ": "г о с т",      # Государственный стандарт
```

```
    "API": "а п и",         # Программный интерфейс
    "JSON": "джейсон",      # Формат данных
}
```

```
{
  "metadata": {
    "created_at": "2024-01-15 14:30:25",
    "timezone": "Europe/Moscow",
    "model": "vosk-model-small-ru-0.22",
    "source": "microphone"
  },
  "segments": [
    {
      "start": 0.5,
      "end": 3.2,
      "text": "открываем кд",
      "speaker": "SPEAKER_00",
      "timestamp": "2024-01-15 14:30:25"
    },
    {
      "start": 5.0,
      "end": 7.8,
      "text": "согласно гост требованиям",
      "speaker": "SPEAKER_01",
      "timestamp": "2024-01-15 14:30:27"
    }
  ]
}
```

Возможности улучшения программного модуля

В данный момент используется упрощённая диаризация по паузам (>2 секунд – новый спикер). Это не определяет голоса, а лишь предполагает смену говорящего [2].

В перспективе будет использоваться PyAnnote – библиотека на Python для анализа речи, которая специализируется на диаризации спикеров. Данная модель весит 2 ГБ (против 40 МБ у Vosk), в связи с этим требуется больше вычислительных ресурсов, использование GPU, требование RAM 8 ГБ.

Также в перспективе возможна реализация выполнения команд голосом: “модуль, начать запись”, “модуль, пауза”, “модуль, перезапуск”, “модуль, сохранить и завершить”. При обнаружении данных команд, модуль будет выполнять по очереди логику, прописанную для данных команд, а в данный момент логика прописана только для кнопок.

Заключение

Разработанный модуль демонстрирует возможность создания локальной системы распознавания речи с гибкой настройкой под предметную область. Модульная архитектура позволяет легко расширять функционал: добавлять поддержку других языков, интегрировать более точные модели диаризации (pyannote.audio), экспортировать в различные форматы (DOCX, TXT).

Библиографический список

1. Головко В.В., Горелик П.А., Игнатова А.Н. Теория и практика распознавания речи. СПб.: Наука и Техника, 2016. 320 с.
2. Шароватов Ю.С., Гладких А.М. Обработка естественного языка и распознавание речи. М.: Интернет-Университет Информационных Технологий, 2014. 240 с.

УДК 004.3; ГРНТИ 50.51

АРХИТЕКТУРНЫЕ РЕШЕНИЯ И МЕТОДЫ СИНТЕЗА КОНЕЧНЫХ АВТОМАТОВ НА VHDL В БАЗИСЕ ПЛИС

А.Н. Сапрыкин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, saprykin.a.n@rsreu.ru

Аннотация. В работе исследуются методологические аспекты проектирования и синтеза конечных автоматов для реализации в архитектуре программируемых логических интегральных схем. Проведен сравнительный анализ формальных моделей конечных автоматов и стратегий кодирования состояний, выявлена их зависимость от типа целевой платформы и требований к быстродействию. Обосновано преимущество двухпроцессорного стиля описания на языке VHDL перед монолитной однопроцессорной реализацией с точки зрения качества логического синтеза, читаемости кода и эффективности верификации.
Ключевые слова: конечный автомат, ПЛИС, VHDL, логический синтез.

ARCHITECTURAL SOLUTIONS AND METHODS FOR SYNTHESIS OF FINITE-STATE MACHINES IN VHDL BASED ON FPGA

A.N. Saprykin

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, saprykin.a.n@rsreu.ru

The summary. This paper examines the methodological aspects of designing and synthesizing finite-state machines for implementation in programmable logic integrated circuit architectures. A comparative analysis of formal finite-state machine models and state encoding strategies is conducted, revealing their dependence on the target platform type and performance requirements. The advantages of a dual-processor VHDL description style over a monolithic single-processor implementation are substantiated in terms of logic synthesis quality, code readability, and verification efficiency.
Keywords: finite state machine, FPGA, VHDL, logic synthesis.

Реализация конечных автоматов (КА) на программируемых логических интегральных схемах (ПЛИС) представляет собой стратегически значимое направление развития аппаратной архитектуры специализированных вычислительных систем. Высокая степень параллелизма, детерминизм временных характеристик и возможность динамической реконфигурации ПЛИС обеспечивают существенные преимущества при синтезе управляющих модулей реального времени, протоколов обмена данными и конвейерных обработчиков потоковой информации. В условиях роста требований к энергоэффективности и производительности встраиваемых систем, использование КА на базе ПЛИС позволяет достигать оптимального баланса между гибкостью программных решений и быстродействием аппаратных реализаций.

Особую актуальность приобретает интеграция КА-контроллеров в состав гетерогенных вычислительных кластеров на программируемой логике, где они выполняют функции координации межмодульного взаимодействия, управления конвейерными стадиями и обработки прерываний. Так, вопросы проектирования масштабируемых кластерных структур на базе ПЛИС, обеспечивающих эффективное распределение вычислительной нагрузки, рассмотрены в работе [1]. Методики оптимизации физического представления специализиро-

ванных вычислителей с конвейерной архитектурой, критически важные для минимизации задержек при переключении состояний КА, представлены в исследовании [2]. Кроме того, проблемы конфигурирования вычислительных кластеров на базе ПЛИС, включая аспекты динамического перепрограммирования управляющих автоматов в ходе выполнения задачи, детально проанализированы в работе [3].

Таким образом, практическая значимость реализации конечных автоматов в архитектуре ПЛИС обусловливает необходимость обращения к их теоретическому базису. Для обеспечения корректного синтеза и верификации управляющих модулей требуется строгая формализация моделей КА, позволяющая установить однозначное соответствие между функциональными требованиями и аппаратной реализацией. Систематизация подходов к описанию состояний и переходов, а также классификация архитектурных вариантов автоматов создают методологическую основу для выбора оптимальной стратегии проектирования, учитывающей как временные ограничения, так и ресурсные характеристики целевой платформы.

Формальные модели и классификация конечных автоматов в задачах цифрового проектирования

Конечные автоматы представляют собой специализированный метод формального моделирования последовательностных логических схем, применение которого обосновано при проектировании систем с жёстко детерминированной последовательностью выполнения операций. Ключевая область применения КА заключается в аппаратной реализации алгоритмов, функционирующих в виде упорядоченной последовательности дискретных шагов. В сложных цифровых системах, где алгоритмическая структура может быть декомпозирована на цепочку действий, зависимых от текущего состояния системы и внешних управляющих сигналов, конечный автомат выполняет функцию управляющего модуля, обеспечивающего координацию и синхронизацию работы функциональных блоков.

Архитектурная организация типовой структуры КА представлена на рисунке 1. Текущее состояние системы фиксируется в регистре памяти состояний, реализуемом на базе k триггеров, синхронизируемых единым тактовым сигналом. Логика формирования следующего состояния представляет собой комбинационную схему, выход которой определяется декартовым произведением вектора текущего состояния и входных сигналов. Функция выхода в автоматах Мили зависит как от вектора состояния, так и от входных воздействий, тогда как в автоматах Мура выходные сигналы детерминируются исключительно текущим состоянием.

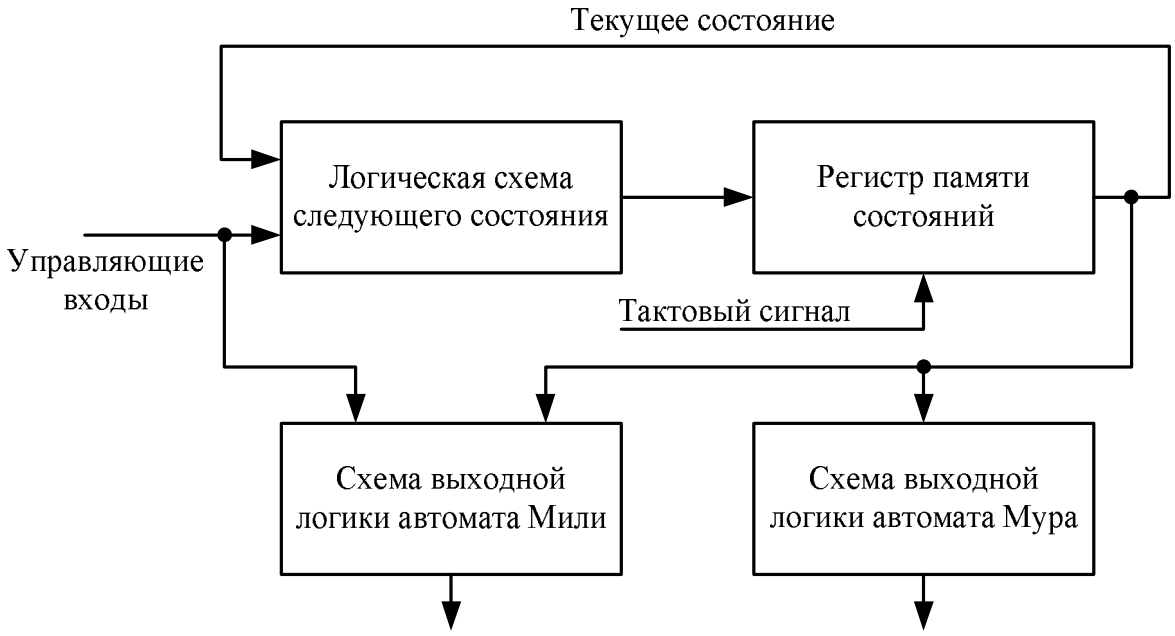


Рис. 1. Структурная схема конечного автомата

Формальная спецификация КА базируется на пяти фундаментальных элементах: множестве символьных состояний, входных и выходных сигналах, а также функциях переходов и выходов. Состояние идентифицирует уникальную внутреннюю конфигурацию системы; в процессе функционирования КА осуществляет дискретные переходы между состояниями. Вектор следующего состояния определяется функцией переходов, аргументами которой являются текущая конфигурация автомата и внешние входные воздействия [4].

Функция выхода детерминирует значения выходных сигналов. В случае зависимости исключительно от текущего состояния выход классифицируется как сигнал автомата Мура, тогда как зависимость от состояния и входных данных характеризует выход автомата Мили. Соответственно, автомат классифицируется как автомат Мура или Мили при наличии соответствующих типов выходов, однако сложные архитектуры могут комбинировать оба типа.

Для моделирования КА применяются различные подходы, включая диаграммы состояний, систему уравнений, таблицы переходов и алгоритмические схемы состояний. Методология синтеза предполагает трансформацию функционального описания в диаграмму состояний, что позволяет сформировать таблицы переходов и выходов для последующей аппаратной реализации. На этапе синтеза доступен широкий спектр методов оптимизации, направленных на улучшение метрик площади кристалла, быстродействия и энергопотребления.

Методы кодирования состояний при синтезе конечных автоматов

Выбор стратегии кодирования состояний является критическим этапом проектирования КА, определяющим баланс между быстродействием и аппаратными затратами. Базовым методом выступает двоичное кодирование, обеспечивающее минимальную ёмкость регистра памяти состояний (n триггеров для кодирования 2^n состояний). Однако данный подход требует реализации сложной комбинационной логики декодирования, что увеличивает задержки распространения сигнала и снижает быстродействие системы.

Альтернативным методом является кодирование «one-hot», при котором каждому состоянию соответствует отдельный триггер (n триггеров для n состояний), а активным является лишь один бит вектора состояния. Преимущества данной архитектуры включают повышенное быстродействие, зависящее от количества переходов в состояние, а так же универсальность и оптимальность для различных типов автоматов.

Промежуточным вариантом служит кодирование «two-hot», активирующее два бита на состояние, что позволяет закодировать до n(n−1)/2 состояний.

Выбор метода кодирования обусловлен архитектурой целевого устройства. Для ПЛИС типа FPGA, обладающих избыточным количеством триггерных ячеек, рекомендовано применение стиля one-hot вследствие его производительности и удобства реализации. В случае использования CPLD, где ресурсы триггеров ограничены, целесообразно применение двоичного кодирования или кодирования Грея для обеспечения максимальной плотности размещения логики и экономии доступных ресурсов.

Методологические принципы синтеза и верификации конечных автоматов на языке VHDL

Конечные автоматы служат фундаментальным компонентам архитектуры цифровых устройств. Корректность разработки их модели определяет функциональную надежность устройства и эффективность использования аппаратных ресурсов.

При синтезе КА на языке VHDL необходимо учитывать ряд таких ключевых архитектурных аспектов, как стилистика кодирования, архитектура процессного описания (количество процессов), методология кодирования состояний и тип организации выходных сигналов.

Существует несколько подходов к программной реализации логики автомата. Структурная организация VHDL-кода предполагает декомпозицию на три функциональных модуля: регистр текущего состояния, комбинационную логику переходов и схему формирования выходов. Несмотря на теоретическую возможность монолитного описания, синтез смешанной последовательностной и комбинационной логики в рамках единого процессного блока (process) является некорректным с точки зрения требований синтезаторов.

При использовании n триггеров памяти теоретическое пространство состояний составляет 2^n комбинаций, однако функциональная спецификация часто не требует задействования всего множества. В связи с этим для описания логики переходов целесообразно применять оператор выбора case. Данный подход обуславливает необходимость разделения модели на несколько процессов, однако обеспечивает высокую читаемость и надежность кода. Использование ветви по умолчанию (when others) в операторе case позволяет исключить явную спецификацию неиспользуемых состояний, обеспечивая корректность синтеза и предотвращая возникновение незапланированных логических элементов.

В общем случае описание любого конечного автомата на языке VHDL допускает реализацию посредством единого процессного блока либо совокупности двух раздельных процессов. Рассмотрим сопоставление структурных элементов исходного кода, соответствующих однопроцессорной и двухпроцессорной архитектурам моделирования.

Пример реализации КА одним процессом представлен ниже.

```
proc_one: process (clk, rst)
begin
if (rst='1') then  current_state <= st_id0;
elsif (clk'event and clk='1') then
  case current_state is
    when st_id0 =>
      if (din_serial ='0') then f<='0'; next_state <= st_id0;
      else f<='0';  next_state <= st_id1;
      end if;
    when st_id1 =>
      if (din_serial ='0') then f<='01';  next_state <= st_id2;
      else f<='0';  next_state <= st_id1;
```

```
      end if;
    when st_id2 =>
      if (din_serial ='0') then f<='1';next_state <= st_id0;
      else f<='0'; next_state <= st_id1;
      end if;
    when others =>
      current_state <= st_id0;
  end case;
end if;
end process proc_one;
```

Пример реализации КА двумя процессами представлен ниже.

```
proc_synch: process (clk, rst)
begin
if (rst='1') then  current_state <= st_id0;
elsif (clk'event and clk='1') then  current_state <= next_state;
end if;
end process proc_synch;
proc_comb: process (din_serial, current_state) begin
case current_state is
  when st_id0=>
    if (din_serial ='0') then f<='0';  next_state <= st_id0;
    else f<='0';  next_state <= st_id1;
    end if;
  when st_id1=>
    if (din_serial ='0') then f<='1';  next_state <= st_id2;
    else f<='0';  next_state <= st_id1;
    end if;
  when st_id2=>
    if (din_serial ='0') then f<='0';  next_state <= st_id0;
    else f<='0'; next_state <= st_id1;
    end if;
  when others =>
    current_state <= st_id0;
end case;
end process proc_comb;
```

В варианте реализации КА с одним процессом оператор case, моделирующий логику переходов, осуществляет мониторинг текущего состояния конечного автомата и анализирует входные сигналы на предмет наличия условий для смены состояния.

Аналогичная структура КА применяется для его реализации на базе двух VHDL процессов. Исходный код разделяется на два функциональных блока: процесс описания синхронных элементов (регистры памяти состояний) и процесс описания комбинационной логики (оператор case). Таким образом, формируется архитектурное разделение между тактируемым процессом, отвечающим за элементы хранения, и комбинационным процессом, реализующим функцию переходов. В рамках оператора case осуществляется верификация текущего состояния и анализ входных воздействий. При наличии условия перехода значения сигналов next_state и current_state различаются, и фиксация нового состояния в качестве текущего происходит по приходу следующего активного фронта тактового сигнала.

Однопроцессорное описание обладает большей наглядностью при внешнем наблюдении за динамикой состояний автомата за пределами VHDL-модуля. Графическое представ-

ление алгоритма структурно ближе к реализации в виде единого процесса, нежели к разделенной архитектуре.

Декомпозиция исходного VHDL кода на два независимых процесса является методологически обоснованной, поскольку она отражает фундаментальное архитектурное различие между комбинационными и последовательностными элементами схемы. Выделение отдельного процесса для регистров состояния и отдельного процесса для логики обеспечивает четкое разграничение временных доменов, что соответствует принципам модульного проектирования и упрощает верификацию структуры.

Применение двухпроцессорной архитектуры существенно повышает эффективность этапа симуляции. Четкое разделение процессов позволяет с высокой точностью локализовать момент возникновения ошибки и определить её источник, так как сбои в комбинационной логике и нарушения синхронизации проявляются в различных временных интервалах относительно тактового сигнала, что облегчает диагностику причин некорректного поведения системы на ранних стадиях разработки.

В настоящее время большинство современных инструментов логического синтеза демонстрируют более высокую эффективность при обработке двухпроцессорных описаний конечных автоматов. Такая структура позволяет синтезаторам точнее идентифицировать критические пути, эффективнее выполнять оптимизацию ресурсов и генерировать схемы с улучшенными показателями быстродействия и занимаемой площади кристалла по сравнению с монолитными однопроцессорными реализациями.

Выводы

Интеграция конечных автоматов в архитектуру программируемых логических интегральных схем выступает фундаментальным условием создания высокопроизводительных специализированных вычислительных систем с детерминированными временными характеристиками. Ключевым фактором, определяющим эффективность аппаратной реализации, является обоснованный выбор стратегии кодирования состояний, адаптированной под специфику целевой платформы. Для FPGA-архитектур, обладающих развитой ресурсной базой триггерных ячеек, целесообразно применения кодирования «one-hot», обеспечивающего минимизацию задержек распространения сигнала в комбинационной логике переходов. В противовес этому, для CPLD-устройств с дефицитом элементов памяти оптимальным решением остается использование компактных бинарных кодов или кодов Грея, позволяющих максимизировать утилизацию кристалла.

Одним из важнейших аспектов методологии проектирования является переход от монолитных однопроцессорных описаний к модульной двухпроцессорной архитектуре. Разделение синхронной и комбинационной логик не только устраняет риски возникновения скрытых ошибок синтеза, но и предоставляет инструментам автоматизированного проектирования возможности для глубокой оптимизации критических путей и снижения энергопотребления. Данный подход также существенно повышает прозрачность процесса верификации, облегчая локализацию дефектов на этапе функционального моделирования.

Библиографический список

1. Дуксин, Н.А. Проектирование вычислительных кластеров программируемой логики // Вестник Рязанского радиотехнического университета. – 2025. № 92. – С.92-99.

2. Люлява, Д.В. Применение методики оптимизации физического представления специализированного вычислителя с конвейерной архитектурой // Вестник Рязанского радиотехнического университета. – 2025. № 92. – С.77-91.

3. Щепухин, Д.О. Вопросы конфигурации вычислительных кластеров на базе ПЛИС // Вестник Рязанского радиотехнического университета. – 2025. № 92. – С.100-105.

4. Гилл, А. Введение в теорию конечных автоматов // М.: Наука. – 1966. – 272 с.

УДК 621.396.001.2; ГРНТИ 47.47.03

АЛГОРИТМЫ И ИНТЕРФЕЙСНЫЕ ПОДХОДЫ К РАЗМЕЩЕНИЮ КОМПОНЕНТОВ В СОВРЕМЕННЫХ САПР ПРОЕКТИРОВАНИЯ ПЕЧАТНЫХ ПЛАТ

А.М. Костяева

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, an.kostayeva@yandex.ru

Аннотация. В статье проводится сравнительный анализ методов и инструментов размещения электронных компонентов в современных системах автоматизированного проектирования (САПР) печатных плат (ПП). Рассматриваются как базовые, так и продвинутые стратегии размещения, включая ручное, интерактивное и автоматизированное размещение. Особое внимание уделено алгоритмической основе автоматических размещений, реализованных в таких пакетах, как Altium Designer, Cadence OrCAD/Allegro, Mentor PADS и Siemens NX (ранее Siemens EDA). Проведенный анализ выявляет ключевые тенденции в развитии данных систем, а именно: смещение в сторону гибридных подходов, сочетающих скорость автоматических алгоритмов и контроль со стороны инженера, а также глубокую интеграцию размещения со смежными этапами проектирования – трассировкой и анализом целостности сигналов.

Ключевые слова: САПР, печатная плата, размещение компонентов, автоматическое размещение, Altium Designer, Cadence Allegro, Siemens PADS, трассировка, DFM.

ALGORITHMS AND INTERFACE APPROACHES TO COMPONENT PLACEMENT IN MODERN CAD SYSTEMS FOR PRINTED CIRCUIT BOARD DESIGN

A.M. Kostyaeva

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, an.kostayeva@yandex.ru

The summary. This article provides a comparative analysis of electronic component placement methods and tools in modern printed circuit board (PCB) computer-aided design (CAD) systems. Both basic and advanced placement strategies are considered, including manual, interactive, and automated placement. Particular attention is paid to the algorithmic basis of automatic placement implemented in packages such as Altium Designer, Cadence OrCAD/Allegro, Mentor PADS, and Siemens NX (formerly Siemens EDA). The analysis reveals key trends in the development of these systems, namely, a shift toward hybrid approaches that combine the speed of automated algorithms with engineer control, as well as deep integration of placement with related design phases such as routing and signal integrity analysis.

Keywords: CAD, printed circuit board, component placement, automatic placement, Altium Designer, Cadence Allegro, Siemens PADS, routing, DFM.

Проектирование печатной платы является многоэтапным процессом, в котором размещение компонентов занимает одно из центральных мест. Качество размещения напрямую определяет такие критически важные параметры конечного изделия, как помехоустойчивость, тепловые режимы, надежность, а также сложность и выполнимость последующей трассировки соединений. Неоптимальное размещение может привести к увеличению количества слоев платы, использованию переходных отверстий, ухудшению электромагнитной совместимости (ЭМС) и, как следствие, к удорожанию продукта и увеличению сроков разработки.

Современные САПР предлагают широкий спектр инструментов для решения этой задачи, от классического ручного перемещения до сложных алгоритмов автоматической оптимизации. Однако реализация этих инструментов и их идеология существенно различаются в зависимости от целевой аудитории и исторического развития пакета. Целью данной работы является систематизация и сравнительный анализ подходов к размещению компонентов в ведущих коммерческих САПР ПП.

Классификация подходов к размещению

Условно все методы размещения можно разделить на три основные категории (рис. 1).

1. Ручное размещение. Инженер вручную перемещает компоненты на монтажное поле, руководствуясь схемой, монтажным эскизом и собственным опытом. Это наиболее гибкий метод, обеспечивающий полный контроль, но требующий значительного времени и подверженный человеческому фактору.

2. Интерактивное и полуавтоматическое размещение. Система предоставляет инструменты, которые ускоряют и упрощают ручное размещение. Сюда относятся:

2.1. Размещение по помещениям – группы компонентов ассоциируются с логическим помещением, которое можно перемещать и копировать целиком;

2.2. Размещение по схематике – выбор компонента на принципиальной схеме автоматически подсвечивает и выделяет его на плате;

2.3. Динамическая подсказка длины цепей – система в реальном времени отображает ожидаемую длину связи между контактами, что критично для высокоскоростных цепей.

3. Автоматическое размещение. САПР самостоятельно расставляет компоненты на плате согласно заданным правилам и критериям оптимизации.

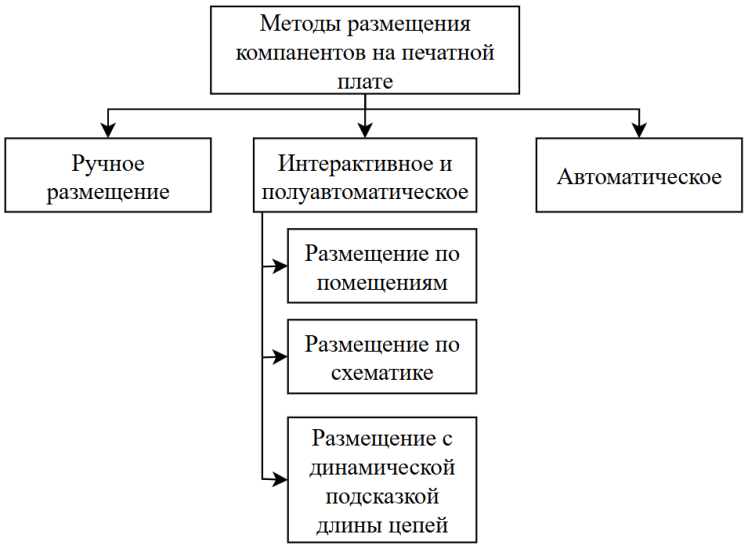


Рис. 1. Классификация методов размещения компонентов на печатной плате

Сравнительный анализ реализаций в различных САПР

Altium Designer

Altium Designer позиционируется как универсальный инструмент для широкого круга разработчиков, чей подход к размещению компонентов характеризуется гибкостью и удобством интерактивных методов. В программе реализованы базовые алгоритмы автоматического размещения, такие как кластерный метод (основанный на анализе электрических связей) и простые стратегии (например, размещение по окружности). Эти алгоритмы могут быть достаточно эффективны для предварительного, «чернового» размещения большого количества дискретных компонентов, однако зачастую они не справляются со сложными многоуровневыми ограничениями, характерными для высокоскоростных проектов.

Сильной стороной инструмента являются интерактивные методы, подкрепленные глубокой интеграцией с принципиальной схемой через режим Cross Select Mode. Активное использование инструмента «Помещения» позволяет разработчику задавать как жесткие, так и нежесткие правила для группового размещения компонентов. Кроме того, мастер размеще-

ния компонентов предоставляет пошаговый интерфейс, существенно упрощающий организацию массивов однотипных элементов, например, резисторов подтяжки.

Основная идеология продукта делает упор именно на интерактивное, управляемое инженером размещение, где автоматические функции играют вспомогательную роль, обеспечивая необходимый баланс между скоростью работы и контролем над проектом.

Cadence OrCAD / Allegro PCB Designer

Allegro является флагманским решением для профессиональной разработки сложных и высокоскоростных плат, и его подход к размещению отличается особой строгостью в сочетании с мощными автоматическими возможностями. В основе работы лежат сложные алгоритмы автоматического размещения, которые учитывают не только топологию электрических связей, но и множество физических и электрических ограничений, предварительно заданных через централизованный Constraint Manager. Благодаря этому алгоритм способен оптимизировать размещение компонентов для минимизации длины цепей, подавления перекрестных помех и точного обеспечения требуемых временных задержек.

Инструмент Autoplace предлагает тонкую настройку параметров трассировки, позволяя, например, игнорировать уже размещенные компоненты или учитывать тепловые факторы. Широкое применение находит механизм «Связок», который обеспечивает синхронное перемещение групп компонентов, критичных к взаимному расположению, таких как дифференциальные пары. В идеологии продукта размещение рассматривается как неотъемлемая часть процесса проектирования, подчиненная жестким правилам, где автоматические алгоритмы являются более продвинутыми и гибко настраиваемыми, однако их эффективное использование требует глубокой и тщательной предварительной настройки констрейнтов.

Siemens EDA (ранее Mentor PADS)

PADS, как и Altium, охватывает широкий рыночный сегмент, однако имеет более выраженный уклон в сторону корпоративных сред и традиционных отраслей промышленности. В версии PADS Professional реализован мощный алгоритм автоматического размещения, который отличается глубокой интеграцией с системами анализа, такими как HyperLynx. Это позволяет выполнять размещение компонентов с учетом результатов предварительного анализа целостности сигналов и электромагнитной совместимости, что критически важно для обеспечения качества разрабатываемых устройств.

Интерактивные инструменты программы отличаются высокой степенью автоматизации рутинных операций, где особую эффективность демонстрируют функции выравнивания, распределения и замены компонентов. Логика работы с «Помещениями» также присутствует в PADS и является стандартным подходом для организации повторного использования функциональных блоков. Основная идеология продукта строится на поиске баланса между автоматизацией процессов и сохранением контроля над ними, предлагая разработчику надежные и предсказуемые инструменты, ориентированные в первую очередь на повышение общей производительности, а не на предоставление максимальной гибкости.

Таблица 1. Сравнительный анализ систем автоматизированного размещения компонентов в САПР печатных плат

Критерий сравнения	Altium Designer	Cadence Allegro	Siemens PADS
Идеология проектирования	Интерактивный подход с приоритетом визуального контроля процесса размещения	Детерминированный подход на основе жесткого управления правилами	Гибридный подход, ориентированный на достижение баланса между автоматизацией и контролем

Продолжение таблицы 1

Метод автоматического размещения	Базовые алгоритмы (кластерный, групповой); рекомендуются для предварительной («черновой») расстановки компонентов	Продвинутые алгоритмы оптимизации с учетом физических и электрических ограничений, заданных в Constraint Manager	Алгоритмы средней сложности, интегрированные с системами предварительного анализа
Ключевые функциональные возможности	Динамическая связь со схемой; гибкое управление группами через инструмент «Помещения»	Мощный менеджер ограничений (Constraint Manager); синхронное перемещение согласованных групп	Развитые утилиты для рутинных операций; блочное проектирование с использованием «Помещений»
Область применения (целевая аудитория)	Широкий круг разработчиков, малые инновационные предприятия, образовательные учреждения	Профессиональная разработка сложной высокоскоростной электроники, телекоммуникационное оборудование	Корпоративный сектор, промышленная и автомобильная электроника, организации с регламентированным документооборотом

Проведенный анализ позволяет заключить, что в современной практике проектирования печатных плат не существует универсального «лучшего» подхода к размещению компонентов, а выбор конкретной САПР и соответствующей стратегии размещения детерминируется спецификой разрабатываемого проекта и требованиями к нему. Для проектов средней сложности и задач быстрого прототипирования оптимальным инструментом может оказаться Altium Designer, предоставляющий интуитивные интерактивные инструменты, обеспечивающие глубокую связь с принципиальной схемой и визуальный контроль процессов. В случае проектирования высокоскоростных устройств, предъявляющих жесткие требования к целостности сигналов и временным задержкам, безальтернативным лидером выступает Cadence Allegro, где процесс размещения неразрывно связан с всеобъемлющей системой правил и ограничений, задаваемых через Constraint Manager. Для корпоративного сектора и промышленной электроники предпочтительным решением является Siemens PADS, который предлагает надежное и сбалансированное решение, ориентированное на предсказуемость результатов и бесшовную интеграцию в общий производственный процесс.

Наблюдаемой тенденцией развития рассматриваемой предметной области является эволюция гибридных интеллектуальных систем, которые не заменяют инженера-проектировщика, а существенно усиливают его возможности, принимая на себя рутинные задачи оптимизации и верификации тысяч ограничений, оставляя за специалистом принятие стратегических решений. Дальнейшее развитие методологии размещения, вероятно, будет связано с активным внедрением методов машинного обучения для прогнозирования качества размещения на ранних этапах проектирования, а также с более тесной интеграцией инструментов трехмерного моделирования и учетом производственных требований на этапе разработки.

Библиографический список

1. Елшин Ю. М. Инновационные методы проектирования печатных плат на базе САПР P-CAD 200x: практическое пособие / Ю. М. Елшин. — М.: СОЛОН-Пресс, 2020. — 464 с. — ISBN 978-5-91359-196-8.

2. Иванова Н. Ю., Петров А. С., Поляков В. И., Романова Е. Б. Технология проектирования печатных плат в САПР P-CAD-2006: учебное пособие / Н. Ю. Иванова, А. С. Петров, В. И. Поляков, Е. Б. Романова. — СПб.: СПбГУ ИТМО, 2009. — 168 с.

3. Фетисов В. С. Самоучитель по автоматизированной разработке печатных плат: учебное пособие / В. С. Фетисов. — Уфа: ФОТОН, 2012. — 88 с. — ISBN 978-5-9903144-2-9.

УДК 621.317.18; ГРНТИ 90.27.35

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ ИЗМЕРЕНИЯ ЧАСТОТЫ: ОТ ПРЯМОГО СЧЁТА ДО ЦИФРОВОЙ ОБРАБОТКИ

К.И. Лейбович

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань

Аннотация. В работе представлен обзор методов измерения частоты электрических сигналов – от классических аналоговых до современных цифровых и фотонных технологий. Рассмотрены принципы работы, достоинства и ограничения резонансного метода, методов прямого счёта, измерения периода, а также методов на основе цифровой обработки сигналов (БПФ). Приведены структурные схемы и математические соотношения. Выполнен сравнительный анализ методов.

Ключевые слова: измерение частоты, прямой счёт, метод периода, цифровая обработка сигналов, быстрое преобразование Фурье.

OVERVIEW OF MODERN FREQUENCY MEASUREMENT METHODS: FROM DIRECT COUNTING TO DIGITAL PROCESSING

K.I. Leibovich

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan

The summary. This paper presents an overview of frequency measurement methods for electrical signals – from classical analog to modern digital and photonic technologies. The operating principles, advantages, and limitations of resonant method, direct counting, period measurement, as well as methods based on digital signal processing (FFT) are considered. Structural diagrams and mathematical relationships are provided. A comparative analysis is performed.

Keywords: frequency measurement, direct counting, period method, digital signal processing, fast Fourier transform.

Измерение частоты является одной из фундаментальных задач в электронике, радиотехнике и связи. За последние десятилетия методы измерения частоты прошли путь от простых резонансных схем до сложных цифровых систем, использующих алгоритмы цифровой обработки сигналов и фотонные технологии [1]. В данной статье представлен обзор основных методов измерения частоты, их сравнительный анализ и тенденции развития.

1. Классические методы измерения частоты

1.1 Резонансный метод

Резонансный метод основан на сравнении измеряемой частоты с собственной частотой настраиваемого колебательного контура. При совпадении частот наблюдается максимум амплитуды колебаний, фиксируемый индикатором. Общая структурная схема реализации метода приведена на рисунке 1.

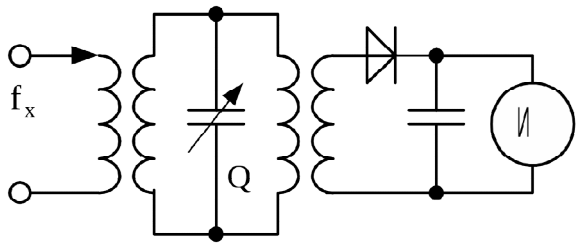


Рис 1. Структурная схема реализации резонансного метода

Погрешность метода в диапазоне СВЧ составляет $10^{-3}\% \ldots 10^{-4}\%$ [2]. В зависимости от диапазона частот конструкция резонансных частотомеров различается:

- в диапазоне от 50 кГц до 200 МГц применяются частотомеры с сосредоточенными параметрами (конденсатор переменной ёмкости и сменные катушки индуктивности);
- в диапазоне от 200 МГц до 1000 МГц используются контуры смешанного типа (ёмкость сосредоточенная, индуктивность распределённая);
- на частотах выше 1000 МГц (СВЧ) применяются коаксиальные и объёмные резонаторы с распределёнными параметрами, обеспечивающие высокую добротность (до 30 000) и малую погрешность [2].

Резонансный метод остаётся востребованным в тех областях, где требуется прямое измерение частоты с приемлемой точностью без сложной цифровой обработки.

2. Цифровые методы измерения частоты

С развитием микропроцессорной техники наибольшее распространение получили цифровые методы измерения частоты [2].

2.1 Метод прямого счёта (метод дискретного счёта)

Метод прямого счёта является основой работы большинства современных цифровых частотомеров. Его суть заключается в преобразовании непрерывного входного сигнала в последовательность импульсов и подсчёте их количества за строго фиксированный интервал времени [2]. Структурная схема, реализующая описанный принцип, приведена на рисунке 2 [2].

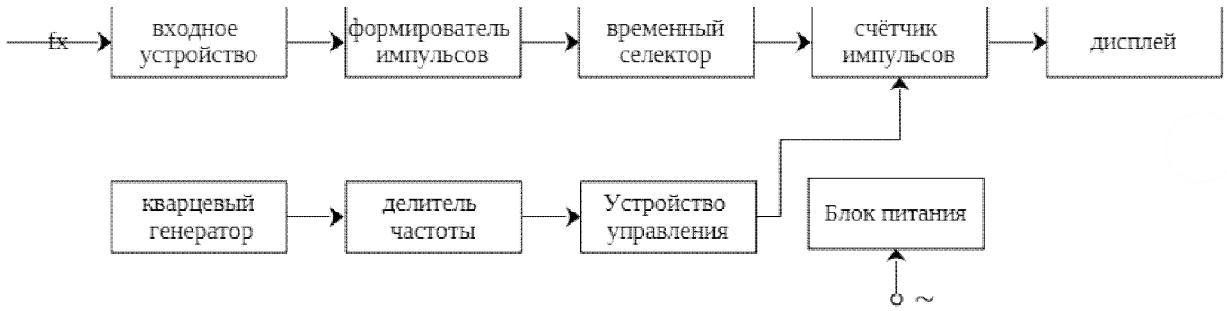


Рис. 2. Структурная схема цифрового частотомера с прямым счётом

Измеряемая частота вычисляется как:

$$f_x = \frac{N}{T} \tag{1}$$

где N – количество подсчитанных импульсов, T – время счета (например, 1 секунда) [6].

Основными достоинствами метода являются простота реализации и высокое быстродействие, особенно на средних и высоких частотах. Однако ему присущи и недостатки. Главный из них – погрешность дискретности, обусловленная возможной потерей или добавлением одного импульса (± 1 счёт) при открывании и закрывании ключа. Максимальная относительная погрешность измерения частоты описывается выражением:

$$\delta = \delta_{\text{кв}} + \frac{1}{N} = \delta_{\text{кв}} + \frac{1}{f_x \tau}, \tag{2}$$

где $\delta_{\text{кв}}$ – относительная погрешность опорного кварцевого генератора [2]. Из формулы (2) видно, что при измерении низких частот, когда число импульсов N невелико, погрешность дискретности становится значительной. Увеличение времени счёта τ для снижения этой погрешности не всегда целесообразно, так как ведёт к росту времени измерения. Для низких

частот (как правило, ниже 1 кГц) применяют метод измерения периода, свободный от этого недостатка.

2.2 Метод измерения периода

Для низких частот применяется метод, при котором измеряется длительность одного или нескольких периодов сигнала. Частота затем вычисляется как обратная величина. Временные диаграммы, иллюстрирующие метод, показаны на рисунке 3 [3].

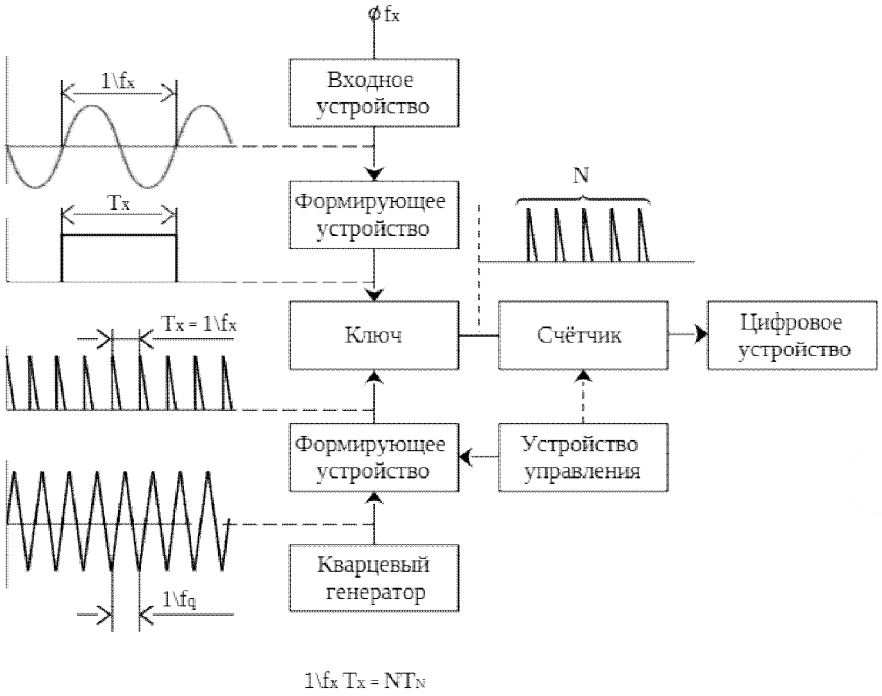


Рис. 3. Структурная схема и временные диаграммы цифрового частотомер, основанного на методе измерения периода

Частота вычисляется по формуле:

$$f_x = \frac{1}{T_x} \tag{3}$$

где T_x – измеренный период сигнала [2].

Достоинства метода: высокая точность на низких частотах. Недостатки: на высоких частотах время измерения становится слишком малым, что увеличивает погрешность [2].

3. Современные методы на основе цифровой обработки сигналов

3.1 Методы на основе преобразования Фурье

Быстрое преобразование Фурье (БПФ) позволяет определить частотный состав сигнала за один цикл измерений. Спектрограмма сигнала отображает зависимость частоты от времени [4]. Частотное разрешение БПФ определяется формулой:

$$\Delta f = \frac{f_s}{N} \tag{4}$$

где f_s – частота дискретизации, N – количество точек БПФ [4].

Современные анализаторы спектра сочетают супергетеродинную технологию с БПФ, обеспечивая широкий диапазон измерений и высокое разрешение [4].

4. Фотонные методы измерения частоты

Перспективным направлением являются фотонные методы, особенно актуальные для сверхвысокочастотного диапазона (СВЧ). Фотонные системы преобразуют электрический СВЧ-сигнал в оптическую область, где осуществляется обработка, а затем обратное преобразование. Выделяют три основных подхода: частотно-мощностной (FTPM), частотно-временной (FTTM) и частотно-пространственный (FTSM) [5]. Метод на основе стимулированного бриллюэновского рассеяния позволяет достигать точности до 1 МГц в диапазоне 6–38 ГГц [1].

5. Сравнительный анализ методов

В таблице 1 представлено сравнение основных методов измерения частоты.

Таблица 1. Сравнение методов измерения частоты

Метод	Диапазон частот	Точность	Быстродействие	Ограничения
Резонансный	50 кГц – сотни ГГц	Высокая в СВЧ	Среднее	Узкий диапазон перекрытия, ручная настройка, зависимость от внешних факторов
Прямой счёт	0,1 Гц – 500 МГц	Средняя	Высокое	Низкая точность на частотах ниже 1 Гц (требует большого времени измерения)
Измерение периода	0,001 Гц – 1 МГц	Высокая	Среднее	Не применим на высоких частотах (малая длительность периода)
БПФ-анализ	Зависит от АЦП	Зависит от АЦП	Зависит от длины выборки	Требует мощной цифровой обработки, избыточен для простых сигналов
Фотонные методы	СВЧ (1–100 ГГц)	Очень высокая	Мгновенное	Высокая сложность, дороговизна, лабораторное применение

Заключение

Эволюция методов измерения частоты идёт по пути повышения точности, расширения диапазона и увеличения быстродействия. От простых аналоговых методов развитие пришло к цифровым методам дискретного счёта, а сегодня – к сложным алгоритмам цифровой обработки и фотонным технологиям. Каждый метод имеет свою область применения: классический прямой счёт оптимален для большинства практических задач, а фотонные методы незаменимы в сверхвысокочастотной технике [1, 6].

Библиографический список

1. Zhang N., Ma J. Advances in frequency measurement techniques based on microwave photonics // Journal of Liaocheng University (Natural Science Edition). – 2025. – Vol. 38, No. 5. – P. 679-692.
2. Измерение частоты // НОУ ИНТУИТ. Метрология и электрорадиоизмерения. Лекция 10. – URL: https://intuit.ru/studies/professional_skill_improvements/16389/courses/684/lecture/16317?page=2.
3. Измерение частоты методом дискретного счета // StudFiles. – URL: https://studfile.net/preview/11704939/page:18/.
4. Основанный на БПФ анализ частоты времени // ЦИТМ Экспонента. – URL: https://docs.exponenta.ru/R2019a/signal/ug/fft-based-time-frequency-analysis.html.
5. Frequency meter // China Science Communication. – 2021. – URL: https://www.kepuchina.cn/.
6. Choosing a Method for Measuring Frequency // National Instruments Documentation. – 2025. – URL: https://www.ni.com/docs/en-US/bundle/pcie-pxie-6351/page/frequency-measurement-methods.html.

УДК 621.317.18; ГРНТИ 90.27.35

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ТОЧНОСТИ ИЗМЕРЕНИЯ ЕМКОСТИ КОНДЕНСАТОРОВ

К.И. Лейбович, Ю.М. Тобратов
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань

Аннотация. В работе рассматриваются современные методы повышения точности измерения емкости конденсаторов. Проведен анализ классических подходов (мостовых, резонансных, метода вольтметра-амперметра), цифровых методов компенсации погрешностей и перспективных методов на основе искусственного интеллекта. Выявлены основные источники погрешностей, характерные для каждого подхода. На основе сравнительного анализа в табличной форме обосновано, что применение технологий искусственного интеллекта позволяет минимизировать систематические и случайные погрешности за счет учета нелинейных зависимостей и влияния внешних факторов, обеспечивая принципиально новый уровень точности.
Ключевые слова: измерение емкости, точность измерений, мостовые методы, резонансные методы, метод вольтметра-амперметра, цифровая обработка сигналов, искусственный интеллект, нейронные сети.

COMPARATIVE ANALYSIS OF METHODS FOR IMPROVING THE ACCURACY OF CAPACITOR MEASUREMENTS

K.I. Leibovich, Tobratov Yu.M.
Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan

The summary. This paper examines modern methods for improving the accuracy of capacitance measurements of capacitors. An analysis of classical approaches (bridge methods, resonant methods, the voltmeter-ammeter method), digital error compensation techniques, and promising methods based on artificial intelligence is carried out. The main sources of errors inherent in each approach are identified. Based on a comparative analysis in tabular form, it is substantiated that the application of artificial intelligence technologies makes it possible to minimize systematic and random errors by accounting for nonlinear dependencies and the influence of external factors, thereby providing a fundamentally new level of accuracy.
Keywords: capacitance measurement, measurement accuracy, bridge methods, resonant methods, voltmeter-ammeter method, digital signal processing, artificial intelligence, neural networks.

Точность измерения емкости конденсаторов критически важна для работы электронных устройств. Это особенно актуально при разработке прецизионной измерительной аппаратуры и систем диагностики. Классические методы – мостовые, резонансные и метод вольтметра-амперметра – имеют ограничения из-за паразитных параметров, температурного дрейфа и внешних полей [1]. Цифровая обработка позволяет частично компенсировать эти погрешности, однако наиболее перспективным является применение искусственного интеллекта (ИИ), способного моделировать сложные нелинейные зависимости. Цель работы – сравнительный анализ методов повышения точности и обоснование эффективности ИИ.

1. Классические методы измерения и пути повышения их точности

1.1 Мостовые методы

Мостовые методы (мост Шеринга, Вина) считаются эталонными благодаря высокой точности и помехозащищенности. Условие равновесия моста исключает влияние нестабильности источника питания. На рисунке 1 приведена схема моста для измерения емкости методом сравнения.

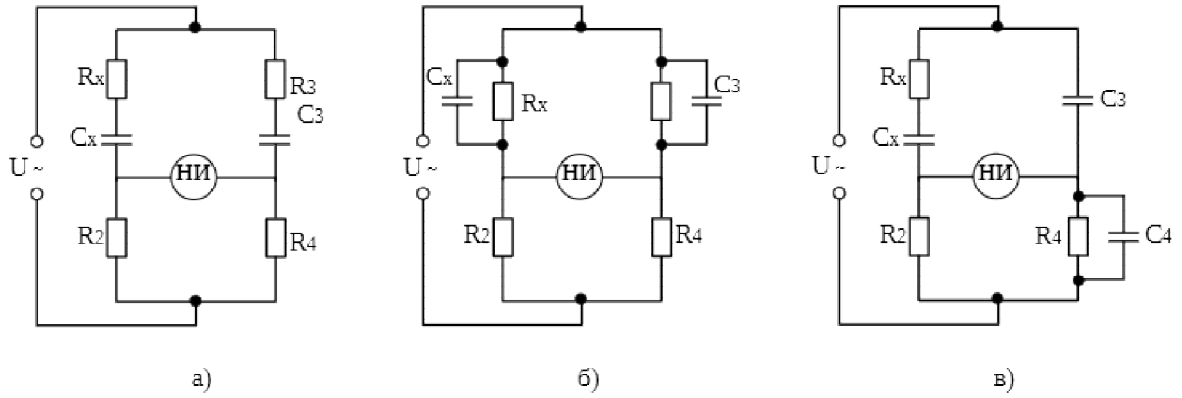


Рис. 1. Схема моста для измерения емкости методом сравнения

На рисунке 1 представлена схемы мостов для измерения емкости методом сравнения: а – для конденсаторов с малыми потерями (последовательная схема замещения); б – для конденсаторов с большими потерями (параллельная схема); в – мост Шеринга для точного определения емкости и тангенса угла потерь. R_2, R_3, R_4– плечи моста; C_3 – образцовый конденсатор; C_x – измеряемая ёмкость; R_x– сопротивление потерь конденсатора.

Для схемы с малыми потерями (рис. 1,а) условия равновесия:

$$C_x = \frac{C_3 R_4}{R_2}, R_x = \frac{R_2 R_3}{R_4}, \tan\delta = \omega C_3 R_3. \quad (1)$$

Для конденсаторов с большими потерями применяют параллельную схему (рис. 1,б). Мост Шеринга (рис. 1,в) позволяет одновременно измерять емкость и tgδ с высокой точностью. На практике чаще всего применяют именно мост Шеринга, так как он обеспечивает наилучшие результаты для широкого класса конденсаторов. Повышение точности достигаеся экранированием и использованием прецизионных компонентов [2].

1.2 Резонансные методы

Резонансные методы реализуются в измерителях добротности (куметрах). Структурная схема куметра (рис. 2) содержит генератор, колебательный контур и электронный вольтметр.

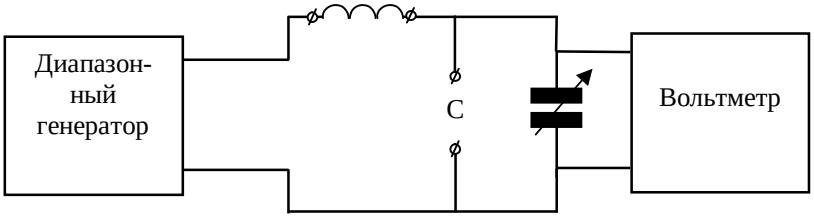


Рис. 2. Структурная схема измерителя добротности

Измерение емкости выполняется методом замещения. Сначала контур настраивают в резонанс без C_x, фиксируют C_1. Затем подключают C_x параллельно, уменьшают C_0 до нового резонанса C_2. Емкость вычисляется как $C_x = C_1 - C_2$ Это исключает влияние собственных параметров контура. Достоинства – широкий частотный диапазон, возможность определения паразитных параметров, таких как собственная межвитковая емкость катушки индуктивности и индуктивность выводов конденсатора [3].

1.3 Метод вольтметра и амперметра

Этот метод относится к косвенным измерениям. При измерении ёмкости на переменном токе в цепь с конденсатором включают амперметр и вольтметр, измеряют действующие значения тока I и напряжения U, после чего вычисляют ёмкость по формуле, вытекающей из закона Ома для емкостного сопротивления:

$$X_c = \frac{1}{2\pi f C} = \frac{U}{I}. \tag{2}$$

Выражаем ёмкость C:

$$C_x = \frac{I}{2\pi f U}. \tag{3}$$

Существуют две основные схемы включения приборов (рис. 3), которые различаются способом учёта внутренних сопротивлений амперметра и вольтметра. Эти схемы универсальны и применимы как для измерения активного сопротивления, так и для измерения ёмкости при замене R_x на емкостное сопротивление X_c.

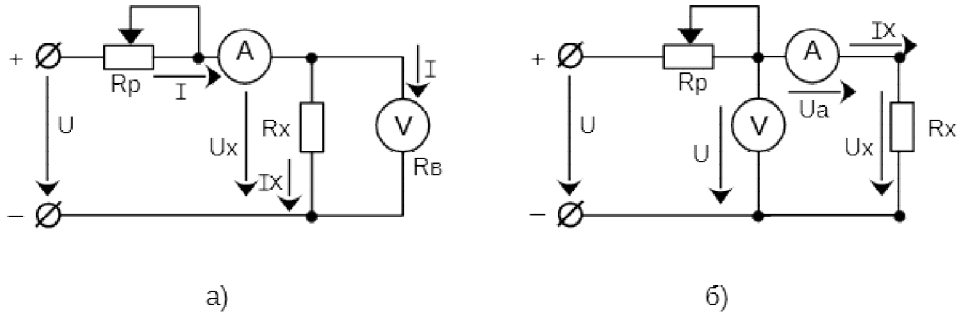


Рис 3 – Схемы включения приборов: а) для малых сопротивлений/больших ёмкостей; б) для больших сопротивлений /малых ёмкостей

В схеме на рисунке 3,*а* вольтметр измеряет напряжение непосредственно на конденсаторе, а амперметр – суммарный ток через конденсатор и вольтметр. В схеме рис. 3,*б* амперметр измеряет ток через конденсатор, а вольтметр – сумму напряжений на конденсаторе и амперметре [4]. Для получения точного результата необходимо вводить поправки, учитывающие сопротивления приборов. Первую схему предпочтительно использовать для относительно больших ёмкостей (малых емкостных сопротивлений), вторую – для малых ёмкостей (больших емкостных сопротивлений). При правильном выборе схемы и учёте инструментальных погрешностей метод позволяет проводить измерения с приемлемой для многих практических задач точностью.

2. Современные методы повышения точности

2.1 Цифровая обработка сигналов и калибровка

Современные измерители импеданса (LCR-метры) используют цифровую коррекцию для исключения систематических погрешностей.

Калибровка «Open/Short» основана на предварительном измерении паразитных параметров измерительных проводов и контактов. Сначала фиксируются показания при разомкнутых щупах (паразитная ёмкость), затем – при замкнутых (паразитные сопротивление и индуктивность). Эти данные вычитаются из результатов последующих измерений, что позволяет свести влияние монтажа к минимуму [1].

Многочастотные измерения позволяют разделить вклад собственно ёмкости (C), эквивалентного последовательного сопротивления (ESR) и индуктивности (ESL). Измеряя па-

раметры на нескольких частотах, прибор строит математическую модель двухполюсника и выделяет чистую ёмкость [2].

Алгоритмическая коррекция нелинейности компенсирует искажения, вносимые аналоговыми узлами (усилители, АЦП). Используются цифровые алгоритмы калибровки по эталонным мерам, что позволяет достичь погрешности 0,05–0,1% [3].

2.2 Методы на основе искусственного интеллекта

Искусственный интеллект (ИИ) позволяет прогнозировать ёмкость по косвенным признакам, учитывая нелинейные зависимости и внешние факторы.

Гибридные нейросетевые модели объединяют несколько алгоритмов. Например, в работе [4] модель на основе искусственной нейронной сети, градиентного бустинга и линейной регрессии (ANN-GB-LR) оценивала ёмкость конденсаторов в преобразователях ветроустановок с погрешностью всего 0,142%, что значительно лучше традиционных методов.

Трансферное обучение позволяет адаптировать модель, обученную на одном типе конденсаторов, для работы с другими типами, используя менее 5% новых данных. Это решает проблему нехватки размеченных данных для каждого типа изделий [5].

Вейвлет-преобразование в сочетании со свёрточными нейросетями применяется для анализа зашумленных сигналов. Метод выделяет частотные составляющие напряжения на конденсаторе и по ним одновременно определяет ёмкость и ESR с высокой точностью [6].

Таким образом, ИИ-методы не просто измеряют, а прогнозируют состояние конденсатора с учётом множества факторов, обеспечивая принципиально новый уровень точности.

3. Сравнительный анализ методов

Таблица 1. Сравнительная характеристика методов

Метод	Точность и условия	Преимущества	Недостатки
Мостовые	0,01–0,1% в лаборатории (1 пФ – 1 Ф)	Эталонная точность, помехозащищённость	Сложность, влияние монтажа
Резонансные	0,1–1% на ВЧ (0,1 пФ – 1 мкФ)	Широкий частотный диапазон	Косвенные измерения, зависимость от добротности
Вольтметра-амперметра	1–5% на НЧ (100 пФ – 1 Ф)	Простота, низкая стоимость	Низкая точность, чувствительность к приборам
Цифровая калибровка	0,05–0,2% [5] в автоматизированных системах	Автоматизация, компенсация погрешностей	Не устраняет нелинейные искажения
Методы на основе ИИ	0,14–0,3% [6] в работающем оборудовании	Прогнозирование, учёт нелинейностей	Зависимость от данных, сложность интерпретации

Заключение

Классические методы измерения ёмкости имеют фундаментальные ограничения из-за паразитных параметров. Цифровая калибровка повышает точность до 0,05–0,2%, но не устраняет нелинейные искажения и не прогнозирует деградацию.

Методы искусственного интеллекта обеспечивают точность до 0,14% в реальных условиях, позволяют одновременно оценивать ёмкость, ESR, импеданс и прогнозировать изменение параметров. Это делает их наиболее перспективными для систем диагностики и мониторинга в реальном времени.

Библиографический список

1. Почему портативные измерители емкости испытывают трудности с измерением малых емкостей [Электронный ресурс] // Honeytek. – 2025. – URL: https://honeytek.com/ (дата обращения: 04.03.2026).
2. Мостовые методы измерения емкости [Электронный ресурс] // Analogiu. – URL: https://analogiu.ru/4/4-3-2.html.
3. Резонансные методы измерения [Электронный ресурс] // ИНТУИТ. – URL: https://intuit.ru/studies/courses/3442/684/lecture/16315?page=2.
4. Метод вольтметра и амперметра [Электронный ресурс] // ИНТУИТ. – URL: https://intuit.ru/studies/courses/3442/684/lecture/16315?page=1.
5. Exponential-incremental quantization-based calibration for capacitor mismatch in high-precision SAR ADCs / Z. Zhang [et al.] // Microelectronics Journal. – 2025. – Vol. 158. – Art. 106634.
6. Capacitance estimation algorithm based on DC-link voltage ripples using hybrid machine learning techniques / [et al.] // Results in Engineering. – 2025. – Vol. 27. – Art. 106216.

УДК 004.716; ГРНТИ 50.41.25

РАЗРАБОТКА ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УСТРОЙСТВА КОММУНИКАЦИОННОГО ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ ПРОТОКОЛОВ ИНТЕРНЕТА ВЕЩЕЙ

С.В. Морозов, Е.М. Шаганов

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, morozov.sereoja2020@gmail.com

Аннотация. Разработано программное обеспечение устройства коммуникационного преобразования сетевых протоколов интернета вещей, обеспечивающее передачу данных с помощью различных транспортных протоколов и физических сред. Рассмотрены основные составляющие устройства и используемые технологии разработки. Также акцентируется внимание на возможностях устройства и особенностях программной реализации.

Ключевые слова: Интернет вещей, программно-конфигурируемые сети (ПКС), IP-сети, OpenFlow, устройство коммуникационного преобразования сетевых протоколов.

DEVELOPMENT OF EMBEDDED SOFTWARE FOR A COMMUNICATION DEVICE FOR CONVERTING IOT NETWORK PROTOCOLS

S.V. Morozov, E.M. Shaganov

V.F. Utkin Ryazan State Radio Engineering University, Russian Federation, Ryazan, morozov.sereoja2020@gmail.com

Abstract. Software has been developed for a communication device that converts Internet of Things network protocols, ensuring data transmission using various transport protocols and physical media. The main components of the device and the development technologies used are considered. Attention is also focused on the device's capabilities and features of the software implementation.

Keywords: Internet of Things, software-defined networking (SDN), IP networks, OpenFlow, communication device for converting network protocols.

В настоящее время по всему миру наблюдается активный рост количества устройств Интернета вещей, которые могут использовать различные протоколы передачи для обмена данными между собой и другими устройствами [1], но в большинстве случаев эти данные передаются через IP-сети.

Большой объем трафика, проходящего через IP-сети, может сказаться на стабильной работе этих сетей. Ввиду этого обстоятельства для предупреждения отказов необходимо исследовать новые подходы и алгоритмы управления сетями. Одним из таких подходов является использование программно-конфигурируемых сетей (ПКС) [2], которые позволяют гибко и централизованно управлять сетевыми ресурсами.

Разработанное устройство коммуникационного преобразования сетевых протоколов предназначено для сбора данных с датчика, имеющего интерфейс UART, и передачи собранных данных по IP-сети, используя различные протоколы и физические среды передачи. Устройство можно использовать для проведения экспериментальных исследований алгоритмов маршрутизации в ПКС, используя специальные устройства – коммутаторы OpenFlow для объединения наших устройств в одну локальную сеть под управлением контроллера ПКС.

Ядром устройства служит микроконтроллер ESP32-S3, выбранный благодаря своим характеристикам и производительности. Для микроконтроллера было разработано программное обеспечение (ПО) на языке программирования C++. ПО состоит из 3-х модулей: модуль визуального веб-интерфейса, модуль чтения данных с датчика, модуль сетевого взаимодействия. Изображение разработанного веб-интерфейса представлено на рисунке.

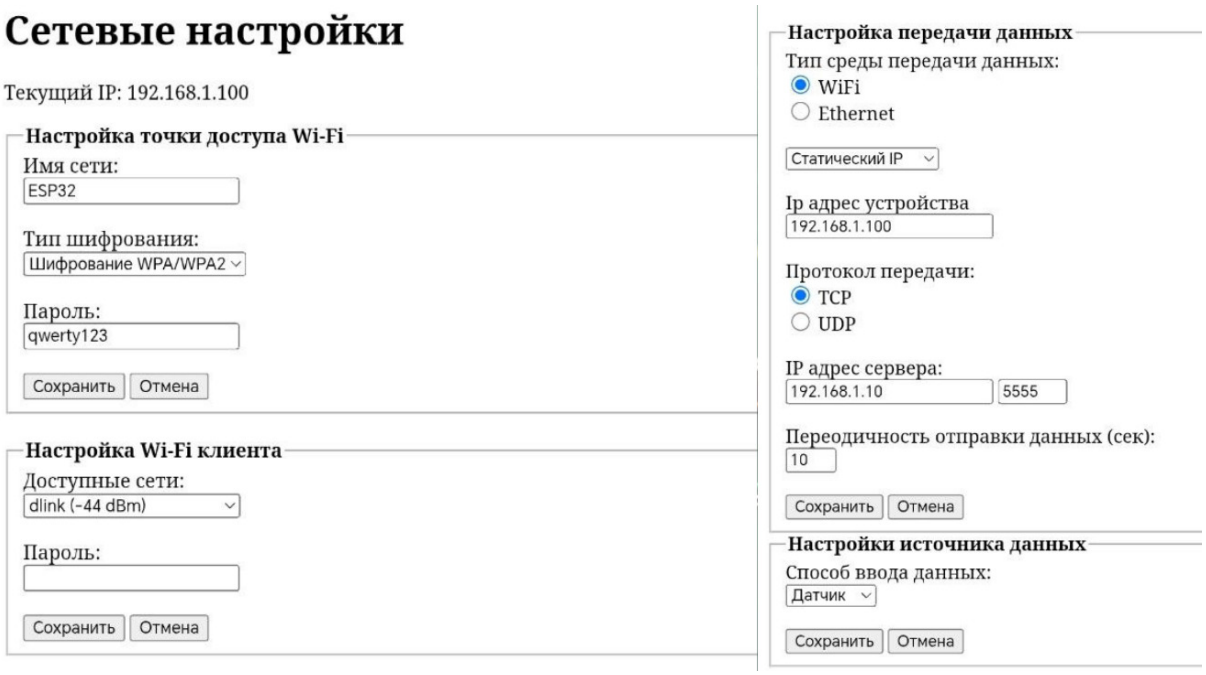


Рис. Изображение веб-интерфейса

Веб интерфейс реализован в виде класса WebConfig, который предназначен для хранения и установки настроек устройства. Он позволяет устанавливать следующие сетевые параметры преобразователя: вид среды передачи (проводная – Ethernet или беспроводная – Wi-Fi), данные точки доступа, к которой подключится устройство при выборе беспроводного вида среды передачи, протокол передачи данных на сервер (TCP или UDP), IP адрес самого преобразователя, IP адрес принимающего сервера. Имеется возможность выбора типа IP адреса преобразователя – статический (устанавливается вручную) или динамический (устанавливается маршрутизатором с помощью протокола DHCP). Помимо этого реализована функция выбора источника данных. Данные для передачи на сервер могут быть считаны из датчика или заданы пользователем вручную, что может быть удобно при проведении экспериментальных исследований.

Модуль чтения данных с датчика реализован в виде класса PulsarHandler, который предназначен для низкоуровневого взаимодействия с датчиком по интерфейсу UART. Модуль реализует полный цикл обмена информацией с датчиком: формирование бинарных запросов, отправка запросов на чтение данных, прием ответов, содержащих значения считанных параметров, проверка целостности данных. Класс хранит информацию о формате коммуникационного пакета с датчиком, сетевом адресе датчика, типе запроса, длине и идентификаторе коммуникационного пакета, контрольной сумме.

Модуль сетевого взаимодействия реализован в виде класса Sender, который предназначен для отправки данных на удаленный сервер. В зависимости от конфигурации модуль устанавливает соединение по выбранному транспортному протоколу (TCP или UDP) через заданную среду передачи, после чего осуществляет отправку данных на сервер. Класс хранит информацию о физических адресах сетевых интерфейсов устройства коммуникационного преобразования, параметрах сетевого клиента и типе соединения с IP-сетью (посредством Wi-Fi или Ethernet). Для получения данных с устройства были разработаны два сервера на языке Python – TCP сервер, UDP сервер.

Алгоритм работы устройства коммуникационного преобразования сетевых протоколов можно представить следующей последовательностью шагов.

Шаг 1. Этап инициализации. На данной стадии выполняются стартовые функции: загружаются параметры из постоянной памяти, производится сканирование доступных Wi-Fi сетей, активируется точка доступа и веб-сервер для конфигурации, а также устанавливается сетевое подключение через интерфейс Wi-Fi или Ethernet.

Шаг 2. Основной рабочий цикл. В этом режиме работы устройство выполняет следующие операции: обработка команд, поступающих на веб-интерфейс, сбор информации с датчика и ее последующая передача на удалённый сервер. Работа с датчиком и веб-интерфейсом происходит параллельно, за счет использования разных ядер процессора микроконтроллера.

Библиографический список

1. Перепелкин, Д. А. Анализ современных технологий Интернета вещей / Д. А. Перепелкин, К. В. Анисимов // Информационные технологии в прикладных исследованиях: Межвузовский сборник научных трудов. – Рязань: ИП Коняхин А.В. (Book Jet), 2024. – С. 208-220.

2. Корячко В. П., Перепелкин Д. А. Программно-конфигурируемые сети. Учебник для вузов. М.: Горячая линия-Телеком, 2020. 288 с.

УДК 004.896; ГРНТИ 28.23.37

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РАЗМЕЩЕНИИ КОМПОНЕНТОВ В САПР

В.В. Грошев

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, vitalag75@gmail.com

Аннотация. В работе рассматриваются вопросы автоматизации размещения компонентов в системах автоматизированного проектирования (САПР) на основе методов машинного обучения. Приводятся основные проблемы традиционных алгоритмов размещения, связанные с высокой вычислительной сложностью и ограниченной адаптивностью. Рассматриваются принципы построения интеллектуальной системы поддержки принятия решений, интегрированной в САПР, а также особенности взаимодействия модуля машинного обучения с существующей архитектурой проектной среды.

Ключевые слова: САПР, размещение компонентов, машинное обучение, искусственные нейронные сети, поддержка принятия решений, автоматизация проектирования.

INTELLIGENT DECISION SUPPORT SYSTEM FOR THE PLACEMENT OF COMPONENTS IN CAD

V.V. Groshev

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, vitalag75@gmail.com

The summary. The paper discusses the issues of automating the placement of components in computer-aided design (CAD) systems based on machine learning methods. It presents the main prob-

lems of traditional placement algorithms, which are associated with high computational complexity and limited adaptability. The paper also discusses the principles of building an intelligent decision support system integrated into CAD, as well as the features of the interaction between the machine learning module and the existing design environment architecture.
Keywords: CAD, component placement, machine learning, artificial neural networks, decision support, and design automation.

Одной из главных проблем современных систем автоматизированного проектирования является выбор, разработка или совершенствование алгоритма размещения компонентов на печатной плате или кристалле. От выбора конкретного алгоритма зависит качество топологической структуры устройства, длина межсоединений, уровень задержек сигналов, тепловые характеристики и электромагнитная совместимость. Инженер-проектировщик при этом ориентируется на поставленную задачу: минимизацию длины соединений, снижение уровня перекрёстных помех, обеспечение технологичности или сокращение времени проектирования. Качество получаемого размещения определяется рядом факторов, влияющих на процесс компоновки: количеством компонентов, плотностью монтажа, числом электрических связей между элементами, ограничениями по габаритам и требованиями к трассировке. В отличие от простых компоновочных задач, размещение в современных электронных устройствах носит сложный многокритериальный характер, где необходимо одновременно учитывать электрические, тепловые и технологические параметры. Наиболее перспективным направлением повышения эффективности процесса размещения является применение методов машинного обучения. Интеллектуальные алгоритмы способны анализировать структуру электрических связей, выявлять закономерности компоновки и формировать рекомендации по размещению компонентов. Использование таких методов позволяет повысить качество проектных решений, сократить длину межсоединений и снизить влияние человеческого фактора. В рамках данной статьи будут рассмотрены основные подходы к автоматизации размещения компонентов в САПР, а также принципы построения интеллектуальной системы поддержки принятия решений на основе методов машинного обучения [2].

С формальной точки зрения задача размещения может быть представлена следующим образом.

Пусть имеется множество компонентов

$$C = \{c_1, c_2, \dots, c_n\} \quad (1)$$

и множество электрических соединений

$$E = \{e_{ij}\} \quad (2)$$

где e_{ij} – соединение между компонентами c_i и c_j.

Каждому компоненту соспоставляются координаты размещения (x_i, x_j). Одной из типовых целевых функций является минимизация суммарной длины межсоединений:

$$F = \sum_{(i,j)\in E} w_{ij} * d_{ij} \quad (3)$$

где w_{ij} – вес соединения, d_{ij} – расстояние между компонентами.

В простейшем случае используется манхэттенская метрика:

$$d_{ij} = |x_i - x_j| + |y_j - y_j| \quad (4)$$

Таким образом, задача раземещения сводится к задаче многокритериальной оптимизации с ограничениями.

Классические алгоритмы размещения

Классические алгоритмы размещения компонентов в САПР формируют основу большинства существующих систем автоматизированного проектирования. Их основная задача заключается в определении координат элементов схемы в пределах заданной области с ми-

нимизацией целевой функции, чаще всего связанной с суммарной длиной межсоединений, числом пересечений или плотностью размещения [1].

Одним из базовых подходов являются последовательные алгоритмы, при которых компоненты размещаются поочерёдно в соответствии с заданным порядком и установленными правилами. Принцип работы заключается в поэтапном формировании структуры компоновки с учётом уже размещённых элементов. Достоинством данного подхода является простота реализации и предсказуемость результата, однако качество размещения во многом зависит от выбранной стратегии упорядочивания компонентов.

Широко применяется также двухуровневый подход, включающий этапы глобального и детального размещения. На этапе глобального размещения определяется общее распределение элементов по области проектирования без точной фиксации координат, после чего выполняется детальное уточнение позиций с учётом локальных ограничений и технологических требований. Такой метод позволяет сократить вычислительные затраты и обеспечить более равномерную структуру компоновки [6].

Анализ классических алгоритмов показывает, что они формируют основу большинства современных САПР и обеспечивают базовый уровень автоматизации процесса размещения. Однако их эффективность ограничена жёсткостью алгоритмических правил и отсутствием механизмов адаптации к особенностям конкретной схемы, что особенно проявляется при увеличении сложности проектируемых систем.

Эвристические алгоритмы размещения

С увеличением сложности электронных устройств и ростом числа компонентов применение строго детерминированных алгоритмов стало недостаточным для получения качественных решений. В связи с этим в САПР получили широкое распространение эвристические и метаэвристические методы размещения, ориентированные на поиск близких к оптимальным решений в условиях большой размерности задачи. В отличие от классических алгоритмов, эвристические методы не гарантируют нахождение глобального оптимума, однако позволяют эффективно исследовать пространство возможных конфигураций. Их принцип работы основан на итерационном улучшении текущего решения с использованием правил или стратегий поиска.

Одним из наиболее известных методов является алгоритм имитации отжига, при котором размещение компонентов последовательно изменяется путём случайных перестановок. Решения, ухудшающие целевую функцию, могут приниматься с определённой вероятностью, что позволяет избежать преждевременной фиксации в локальном минимуме. Метод демонстрирует высокое качество решений, однако требует значительных вычислительных затрат при больших размерах схем.

Алгоритм основан на вероятности принятия ухудшающего решения:

$$P = \exp\left(-\frac{\Delta F}{T}\right) \quad (5)$$

где ΔF – приращение целевой функции, T – параметр «температуры».

Параметр T постпенно уменьшается в процессе работы алгоритма в соответствии с заданным законом охлаждения $T_{k+1} = \alpha T_k$, где $0 < \alpha < 1$.

На начальных этапах при высокой температуре система допускает переходы к менее оптимальным состояниям, что обеспечивает исследование пространства решений. По мере уменьшения темературы вероятность принятия ухудщающих изменений снижается, и алгоритм концетрируется на уточнении текущего решения. Таким образом, метод реализует баланс между глобальным поиском и локальной оптимизацией [3].

Также применяются генетические алгоритмы, основанные на моделировании процессов естественного отбора. Набор вариантов размещения рассматривается как популяция, внутри которой выполняются операции скрещивания и мутации. В результате происходит

постепенное улучшение качества решений. Данный подход отличается гибкостью, но требует корректного выбора параметров и критериев отбора.

Каждое размещение представляется хромосомой:

$$X = \{x_1, y_1, x_2, y_2, \dots, x_n, y_n\} \quad (6)$$

Функция приспособленности определяется как:

$$Fit(X) = \frac{1}{F(X)} \quad (7)$$

Эволюционный процесс включает операции селекции, скрещивания и мутации. Селекция обеспечивает отбор наиболее приспособленных решений для формирования следующего поколения. Оператор скрещивания объединяет фрагменты двух размещений, создавая новые конфигурации, а мутация вносит случайные изменения координат отдельных компонентов, что предотвращает преждвременную сходимость к локальному минимуму. Итерационное применение данных операторов приводит к постепенному улучшению среднего значения целевой функции в популяции [4].

К эвристическим методам также относят алгоритмы локального поиска, при которых производится последовательное улучшение размещения путём анализа соседних конфигураций. Такие методы обладают высокой скоростью работы, однако могут застревать в локальных оптимумах.

Анализ эвристических алгоритмов показывает, что они обеспечивают более высокое качество размещения по сравнению с классическими методами, особенно при работе со сложными схемами. Вместе с тем их эффективность существенно зависит от выбора параметров, начальной конфигурации и критериев оптимизации. Кроме того, данные методы не обладают механизмами обучения на накопленных проектных данных, что ограничивает их адаптивность.

Методы машинного обучения в задачах размещения компонентов

Развитие методов машинного обучения открыло новые возможности для решения задач автоматизированного проектирования, включая задачу размещения компонентов в САПР. В отличие от классических и эвристических алгоритмов, методы машинного обучения ориентированы не только на поиск решения в заданном пространстве вариантов, но и на формирование модели, способной выявлять закономерности в структуре схем и учитывать накопленный опыт проектирования.

Применение машинного обучения в задачах размещения основано на представлении схемы в формализованном виде. Наиболее распространённым является графовая модель, в которой компоненты рассматриваются как вершины графа, а электрические соединения – как рёбра. Такое представление позволяет учитывать топологическую структуру схемы и использовать алгоритмы, способные анализировать взаимосвязи между элементами. В зависимости от способа постановки задачи используются различные подходы машинного обучения. Один из них предполагает формирование регрессионной модели, прогнозирующей качество размещения по заданным параметрам конфигурации. Другой подход ориентирован на генерацию координат компонентов на основе анализа структуры соединений. Также возможна реализация рекомендательных моделей, предлагающих проектировщику оптимальные варианты размещения с учётом заданных критериев.

Задача обучения может быть представлена как минимизация функции потерь:

$$L(\theta) = \frac{1}{N}\sum_{k=1}^{N} l(f_\theta(G_k), Y_k) \quad (8)$$

где f_θ – модель с параметром θ, G_k – граф схемы, Y_k – эталонное размещение.

Минимизация функции потерь осуществляется с использоанием градиентных методов оптимизации, например стохастического градиентного спуска. В процессе обучения пара-

метры θ корректируются таким образом, чтобы минимизировать расхождение между предсказанным размещением и эталонной конфиграцией. В качестве функции ошибки может использоваться среднеквадратичное отклонение координат компонентов либо функционал, связанный с длиной междсоединений.

Особый интерес представляют искусственные нейронные сети, включая графовые нейронные сети, которые позволяют учитывать сложные структурные зависимости между элементами схемы. Такие модели способны обучаться на базе ранее реализованных проектов и формировать решения, учитывающие особенности конкретного класса устройств. В отличие от эвристических методов, нейросетевая модель после обучения может быстро формировать рекомендации без необходимости полного перебора конфигураций.

Важным аспектом является интеграция модели машинного обучения в архитектуру САПР. Интеллектуальный модуль может функционировать как подсистема поддержки принятия решений, анализируя текущую компоновку и предлагая улучшения, либо как автоматизированный генератор первичного размещения. При этом сохраняется возможность участия проектировщика в корректировке решений, что повышает надёжность итогового результата.

Анализ применения методов машинного обучения показывает, что их использование позволяет повысить адаптивность алгоритмов размещения, сократить время проектирования и улучшить качество получаемых решений. В то же время эффективность таких методов зависит от качества обучающих данных, выбора архитектуры модели и корректной интеграции в существующую среду САПР [5].

Для наглядной иллюстрации сравнительной зависимости вычислительных затрат различных методов размещения от сложности проекта на рисукнке 1 представлена качественная оценка роста выичслительной трудоёмокстии при увеличении числа компонентов.

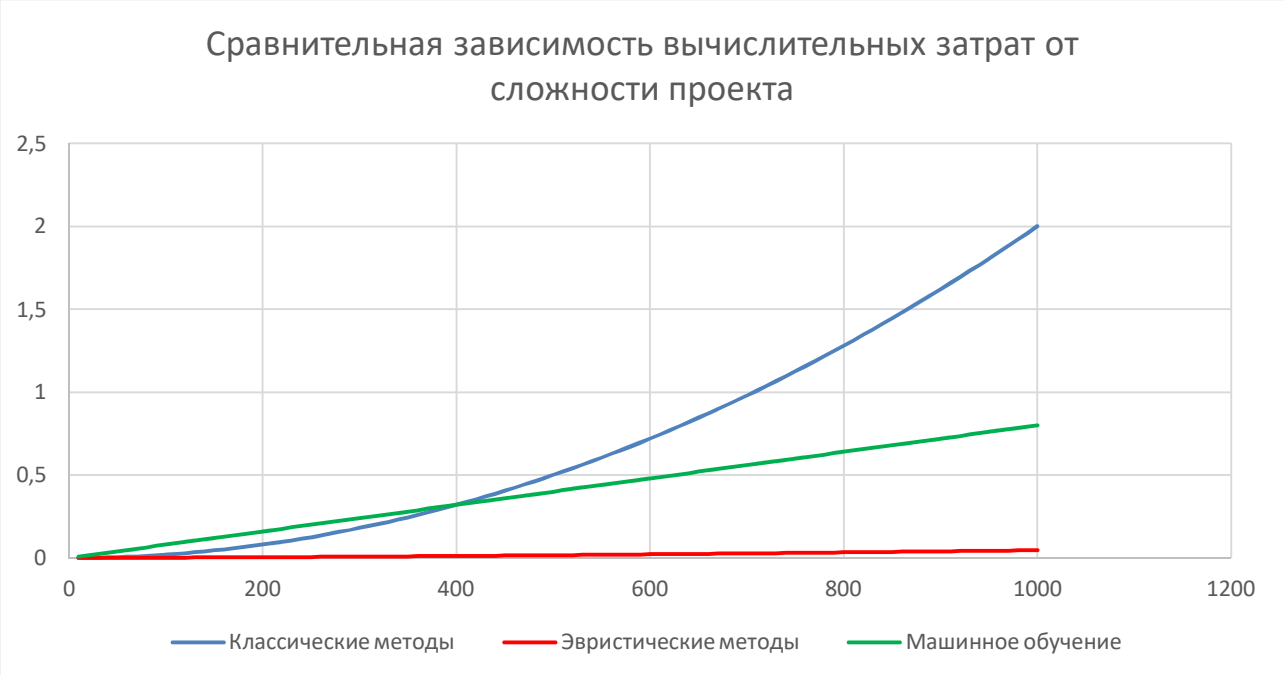


Рис. 1. Сравнительнный график

Представленная зависимость отражает теоретическую оценку вычислительной сложности алгоритмов. Для классических методов характерен квадратичный рост затрат вследствие необходимости учёта большого числа взаиомдействий между компонентами ($O(n^2)$ или $O(n^2 \log n)$, где n – число компонентов). Эвристические алгоритмы демонстрируют более умеренную зависимость, обсуловленную ограничением числа итераций поиска

($O(k * n)$, где k – число итераций). Методы машинного обучения после этапа обучения обеспечивают близкую к линейной зависимость времени формирования решения от числа компонентов (два этапа: обучение $O(N * n)$ и инференс $O(n)$), что делает их перспективными при работе со сложными проектами.

Архитектура интеллектуальной системы поддержки принятия решений при размещении компонентов в САПР

Интеллектуальная система поддержки принятия решений (ИСППР) при размещении компонентов представляет собой программный модуль, интегрируемый в структуру САПР и взаимодействующий с её базовыми подсистемами. Основной задачей системы является анализ проектных данных и формирование рекомендаций по оптимальному размещению компонентов с учётом заданных критериев.

С функциональной точки зрения архитектура системы может быть представлена в виде следующих основных модулей:

1. Модуль подготовки и представления данных.

Данный модуль обеспечивает получение информации из САПР: перечень компонентов, параметры посадочных мест, список электрических соединений (netlist), ограничения по габаритам и технологические требования.

На этом этапе выполняется:

- формирование структурированной модели схемы;
- преобразование данных в формат, пригодный для обработки алгоритмами машинного обучения;
- построение графового представления системы.

Корректность и полнота подготовки данных напрямую влияют на качество последующих рекомендаций.

2. Модуль машинного обучения.

Центральным элементом системы является модель машинного обучения, обученная на базе ранее выполненных проектов либо синтетически сгенерированных данных.

В зависимости от выбранного подхода модель может:

- прогнозировать качество текущего размещения;
- предлагать корректировку отдельных компонентов;
- генерировать первичное размещение с учётом структуры соединений.

В случае использования нейронных сетей модель получает на вход структурированные характеристики схемы и формирует координаты компонентов либо рекомендации по их перераспределению.

3. Модуль оценки и оптимизации.

Полученные от модели варианты размещения проходят дополнительную проверку на соответствие ограничениям САПР. Производится расчёт целевых показателей:

- суммарной длины соединений;
- плотности размещения;
- соответствия технологическим требованиям.

При необходимости выполняется итерационное уточнение решения.

4. Интерфейсный модуль взаимодействия с проектировщиком.

Особенностью интеллектуальной системы является её рекомендательный характер. Пользователь получает:

- визуальное отображение предложенного размещения;
- количественную оценку улучшений;
- возможность принять или отклонить изменения.

Таким образом, система не заменяет инженера, а выступает инструментом поддержки принятия решений.

Интеграция интеллектуального модуля может быть реализована в виде:

1. Встроенного расширения существующей САПР.
2. Внешнего вычислительного сервиса с обменом данными через API.
3. Облачного модуля анализа проектных решений.

Предложенная архитектура обеспечивает модульность, масштабируемость и возможность адаптации к различным типам электронных проектов. Она соответствует концепции интеллектуальной поддержки проектировщика и позволяет объединить алгоритмические методы оптимизации с возможностями машинного обучения.

Библиографический список

1. Бонч-Бруевич М.А., Черников Б.В., Черникова Е.А. Анализ методов размещения элементов при проектировании специализированных БИС // Управление развитием крупномасштабных систем. MLSD’2020: труды XIII международной конференции. – М.: ИПУ РАН, 2020. – С. 792–798.

2. Канг А.Б., Линиг Й., Марков И.Л., Ху Ц. Физическое проектирование БИС: от разбиения графа до временной оптимизации. – М.: Техносфера, 2022. – 317 с.

3. Киркпатрик С., Гелатт К., Векки М. Оптимизация методом имитации отжига // Science. – 1983. – Т. 220, №4598. – С. 671–680.

4. Кухон Дж.П., Пэрис У.Д. Генетическое размещение // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 1987. – Т. 6, №6. – С. 956–964.

5. Кахани И., Штимер М. Математическая оптимизация и машинное обучение для идентификации топологии печатных плат // Advances in Radio Science. – 2023. – Т. 21. – С. 25–38.

6. Чан Т.Ф. и др. Улучшенный многоуровневый алгоритм размещения схем // Материалы конференции ICCAD-2003. – IEEE, 2003. – С. 299–306.

СЕКЦИЯ «ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ В ОБРАЗОВАНИИ»

УДК: 37.018.43:004(575.1); ГРНТИ: 14.35.07

НАЦИОНАЛЬНЫЕ ОСОБЕННОСТИ ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ: ОПЫТ РЕСПУБЛИКИ УЗБЕКИСТАН

Л.С. Махмутходжаева
Филиал Российского экономического университета имени Г.В. Плеханова в г. Ташкенте, Республика Узбекистан, г. Ташкент, food-system@yandex.ru

Аннотация. В статье представлен комплексный анализ воздействия процессов цифровизации на современную систему образования. Рассматриваются научные подходы к оценке влияния цифровых технологий на образовательную сферу, выявляются их положительные и отрицательные аспекты. Особое внимание уделено анализу ключевых тенденций и перспектив цифрового развития образования в Республике Узбекистан
Ключевые слова: цифровизация, система образования, университеты, Узбекистан, цифровое обучение, цифровые технологии.

NATIONAL FEATURES OF DIGITALIZATION OF EDUCATION: THE EXPERIENCE OF THE REPUBLIC OF UZBEKISTAN

L.S. Makhmutkhodjaeva
Branch of the Plekhanov Russian University of Economics in Tashkent, Republic of Uzbekistan, Tashkent
E-mail: food-system@yandex.ru

The summary. The article presents a comprehensive analysis of the impact of digitalization processes on the modern education system. Scientific approaches to assessing the influence of digital technologies on the educational sphere are examined, and their positive and negative aspects are identified. Particular attention is paid to the analysis of key trends and prospects for the digital development of education in the Republic of Uzbekistan.
Keywords: digitalization, education system, universities, Uzbekistan, digital learning, digital technologies.

Современный этап развития общества характеризуется ускоренным внедрением цифровых технологий во все сферы социально-экономической жизни. В этой связи образование как ключевой институт формирования человеческого капитала неизбежно оказывается в центре цифровых преобразований. Процессы цифровизации образования носят системный характер и обусловлены не только технологическим прогрессом, но и изменением запросов общества, рынка труда и глобальных экономических тенденций. Цифровая трансформация образования представляет собой сложный многоуровневый процесс, включающий внедрение информационно-коммуникационных технологий, изменение педагогических подходов, развитие новых форм обучения и трансформацию управленческих механизмов в образовательных организациях. В этих условиях особую актуальность приобретает анализ тенденций, рисков и перспектив цифровизации образовательной системы, в том числе на национальном уровне.

Методологической основой исследования послужил комплексный междисциплинарный подход, объединяющий положения теории человеческого капитала, концепции цифровой трансформации образования и системного анализа социально-экономических процессов. В ходе исследования использовались для обобщения теоретических подходов к цифровизации образования – методы научного познания, сравнительный анализ при сопоставлении национальных и международных тенденций цифрового развития образовательных систем; для выявления роли цифровых технологий в трансформации образовательного процесса – структурно-функциональный метод; а также статистический анализ и контент-анализ. Информационную базу исследования составили государственные стратегии и программы цифрового

развития Республики Узбекистан [1–2, 10–11], статистические данные по охвату высшим образованием и числу образовательных учреждений [8], материалы международных организаций (World Bank, UNESCO), а также результаты научных исследований отечественных и зарубежных авторов [3, 6–7, 9]. Применение совокупности указанных методов позволило обеспечить объективность выводов и комплексность анализа процессов цифровизации образования.

Современный образовательный процесс требует постоянного обновления в условиях изменения социальных ценностей и приоритетов. Научно-технический прогресс все в большей степени рассматривается как средство удовлетворения растущих потребностей личности и развития ее интеллектуального и духовного потенциала. Применение компьютерных технологий и интерактивных обучающих программ способствует формированию навыков самостоятельной работы, расширяет возможности самоконтроля и повышает мотивацию обучающихся. При этом IT-образование в последние годы стало одним из наиболее востребованных направлений на мировом рынке труда, что актуализирует задачу подготовки высококвалифицированных специалистов.

Интерес к проблематике цифрового образования возник задолго до современных этапов цифровой трансформации. Уже в начале 2000-х годов зарубежные исследователи начали анализировать влияние технологий на процессы преподавания и обучения. В частности, в 2002 году Д. Джонсон и Л. Бакер опубликовали одно из первых исследований, посвященных оценке роли технологий в образовании [1]. Современные научные подходы условно можно разделить на две группы: сторонники цифровизации, подчеркивающие ее преимущества и активно внедряющие цифровые инструменты (Г. Гейбл, Д. Седера, М. Веллер и др.), и критики, указывающие на возможные риски и ограничения (Р. Мустафаоглы, Я. Алдхамди и др.). В научной литературе цифровизация образования рассматривается в контексте теории постиндустриального общества, концепции экономики знаний и теории человеческого капитала. Согласно данным подходам, уровень развития образования напрямую определяет конкурентоспособность государства в глобальном пространстве. Исследователи подчеркивают, что цифровизация образования не сводится исключительно к использованию электронных платформ и дистанционных форм обучения. Речь идет о формировании новой образовательной парадигмы, ориентированной на непрерывное обучение, развитие цифровых компетенций, критического мышления и способности адаптироваться к быстро меняющимся условиям внешней среды. Научные дискуссии в данной области условно можно разделить на два направления. Представители первого направления рассматривают цифровизацию как инструмент повышения доступности и качества образования, расширения образовательных возможностей и демократизации знаний. Представители второго направления акцентируют внимание на социальных, психологических и когнитивных рисках чрезмерной цифровизации, включая снижение уровня социализации и утрату традиционных педагогических ценностей. Таким образом, цифровизация образования остается дискуссионным и многогранным процессом.

В Узбекистане реализуется комплекс мер, направленных на ускоренное развитие цифровой экономики и внедрение современных технологий в ключевые сферы общественной жизни – государственное управление, здравоохранение, сельское хозяйство и образование. В рамках данных преобразований запущены проекты по развитию рынка программных продуктов, информационных технологий и подготовке квалифицированных кадров. Согласно стратегическим установкам Президента Ш. Мирзиёева, планируется рост ВВП на душу населения до 2800 долларов США к 2026 году и до 4000 долларов США к 2030 году [2]. Достижение этих целей напрямую связано с модернизацией системы образования, развитием конкуренции и обеспечением доступности качественного обучения.

В Республике цифровая трансформация образования осуществляется в рамках долгосрочных стратегических документов. Стратегия «Цифровой Узбекистан – 2030» [3] опреде-

ляет образование как одно из приоритетных направлений цифрового развития, подчеркивая необходимость интеграции цифровых технологий на всех уровнях образовательной системы. Дополняют данную стратегию Стратегия инновационного развития и Стратегия развития Нового Узбекистана на 2022–2026 годы [4], направленные на формирование благоприятной инновационной среды, развитие цифровых навыков населения и повышение качества подготовки специалистов. Важным шагом стало принятие стратегии развития искусственного интеллекта [5], ориентированной на создание национальных онлайн-баз данных и популяризацию ИИ-технологий, прежде всего среди молодежи. Государственная политика в сфере образования в Узбекистане направлена на повышение охвата высшим образованием, развитие конкурентной среды между образовательными учреждениями, привлечение иностранных инвестиций и интеграцию национальной образовательной системы в международное пространство.

Цифровые технологии сегодня являются одним из ключевых факторов трансформации высшего образования, превращая традиционный учебный процесс в более гибкую, интерактивную и ориентированную на индивидуальные образовательные траектории среду. Использование цифровых платформ позволяет отказаться от жесткой привязки к аудиториям, единому темпу обучения и стандартному объему учебного материала, расширяя возможности для самостоятельных исследований, виртуального взаимодействия и доступа к глобальным источникам знаний [6]. В этой связи цифровизация высшей школы становится стратегическим приоритетом как для национальных, так и для зарубежных образовательных систем.

Цифровые технологии оказывают многоаспектное влияние на систему высшего образования. Они способствуют формированию гибких образовательных траекторий, индивидуализации обучения и развитию самостоятельной познавательной деятельности студентов. Использование цифровых платформ и онлайн-курсов позволяет расширить доступ к образовательным ресурсам ведущих мировых университетов и научных центров. Цифровизация учебного процесса также трансформирует роль преподавателя, который все чаще выступает не только источником знаний, но и модератором, наставником и координатором образовательной деятельности. Это требует пересмотра традиционных педагогических методов и повышения цифровой компетентности профессорско-преподавательского состава. Особое значение приобретает развитие смешанных форм обучения, сочетающих очное и дистанционное взаимодействие. Данный подход позволяет сохранить преимущества традиционного образования и одновременно использовать потенциал цифровых технологий.

К числу основных преимуществ цифровизации системы образования относятся отказ от бумажного документооборота, сокращение финансовых затрат образовательных учреждений и обучающихся, экономия времени, снижение транспортной нагрузки и уменьшение негативного воздействия на окружающую среду [7]. Таким образом, цифровизация требует взвешенного и системного подхода, направленного на минимизацию рисков и сохранение качества образования.

Рассматривая современные тенденции развития образования в Узбекистане мы видим, что анализ статистических данных показывает устойчивый рост интереса к образованию и профессиональной переподготовке. Увеличение числа высших учебных заведений и рост охвата высшим образованием свидетельствуют о формировании конкурентной образовательной среды. Среди ключевых тенденций можно выделить:

- персонализацию образовательных траекторий;
- рост частного и корпоративного образования;
- развитие дистанционных и смешанных форм обучения;
- активное внедрение цифровых платформ и аналитических систем;
- приток иностранных преподавателей и образовательных программ.

Особое внимание уделяется подготовке кадров в сфере информационно-коммуникационных технологий, что соответствует стратегической задаче превращения Узбекистана в региональный IT-хаб.

Опыт массового перехода к дистанционному обучению в период пандемии показал готовность образовательной системы Узбекистана к цифровым вызовам. Наличие развитой телекоммуникационной инфраструктуры, образовательных платформ и цифровых ресурсов создало основу для дальнейшего развития дистанционного образования. В перспективе ключевыми направлениями развития станут внедрение искусственного интеллекта и адаптивных обучающих систем; использование технологий виртуальной и дополненной реальности; развитие геймификации и проектного обучения; а также создание единых цифровых образовательных экосистем. В то же время цифровая трансформация сопровождается рядом проблем, включая риск снижения качества образования, особенно в технических и практико-ориентированных направлениях, возможное ослабление когнитивных способностей, дефицит социальной коммуникации и негативное влияние на здоровье при длительной работе за компьютером (см. таблицу 1). Цифровизация образования носит двойственный характер, требующий баланса между технологическими инновациями и сохранением качества образовательного процесса.

Таблица 1. Преимущества и риски цифровизации системы образования

Параметр	**Положительное влияние**	**Потенциальные риски**
Организация обучения	Гибкость форматов, дистанционный доступ	Снижение практико-ориентированного обучения
Экономический эффект	Снижение затрат, оптимизация ресурсов	Высокие первоначальные инвестиции
Социальный аспект	Расширение доступа к образованию	Ослабление социальной коммуникации
Качество подготовки	Индивидуализация обучения	Риск формализации знаний
Здоровье	Сокращение перемещений	Рост нагрузки на зрение и опорно-двигательный аппарат

Анализ образовательных тенденций в Узбекистане показывает устойчивый рост интереса к обучению и переобучению. За последние пять лет количество университетов в Узбекистане достигло 160 и согласно Концепции развития системы высшего образования Республики Узбекистан до 2030 года это число вырастет до 200. Рассмотрим динамику развития высшего образования в Узбекистане (таблица 2). Данные таблицы свидетельствуют о стремительном росте институциональной базы высшего образования и увеличении доступности образовательных услуг. Параллельно наблюдается рост доли цифровых дисциплин, что подтверждает системный характер цифровой трансформации образования.

Таблица 2. Динамика развития высшего образования в Республике Узбекистан (2015–2025 гг.)[1]

Показатель	**2015 г.**	**2020 г.**	**2022 г.**	**2024 г.**	**2025 г. (примерно)**
Количество вузов	65	131	198	>200	≈210–215
Охват высшим образованием, %	9	25	38	~40	42–45
Количество частных вузов	0	25	42	>50	55–60
Доля цифровых дисциплин в учебных планах, %	10	25	40	50	55–60

[1] составлено автором на основе официальных данных Министерства высшего образования Республики Узбекистан, аналитических обзоров Всемирного банка и национальных стратегических документов.

В Республике создана единая интегрированная электронная система (HEMIS), которая включает базу данных всех студентов по республике (в том числе частные и международные вузы). Формируется конкурентная среда между государственными и частными вузами, активно развиваются IT-направления и обучение иностранным языкам. Среди ключевых трендов выделяются персонализация образования, рост частного сектора, развитие корпоративного обучения, цифровизация учебного процесса и приток иностранных преподавателей. Наряду с этим, налажена подготовка кадров со стороны зарубежных вузов - в Университете Инха, университете Амити, были открыты смешанные цифровые частные вузы Japan Digital University и International Digital University. В Ташкентском филиале Российского экономического университета им. Г.В. Плеханова также уделяется большое внимание внедрению цифровых технологий – в филиале запущены и функционируют совместные проекты и цифровые лаборатории: научная лаборатория исследований зеленой экономики «Green EcoHub», цифровая медиа-студия «МедиаТехРэу», ИКТ Академия HUAWEI, интеллектуальный модуль IM REU Tashkent и др.

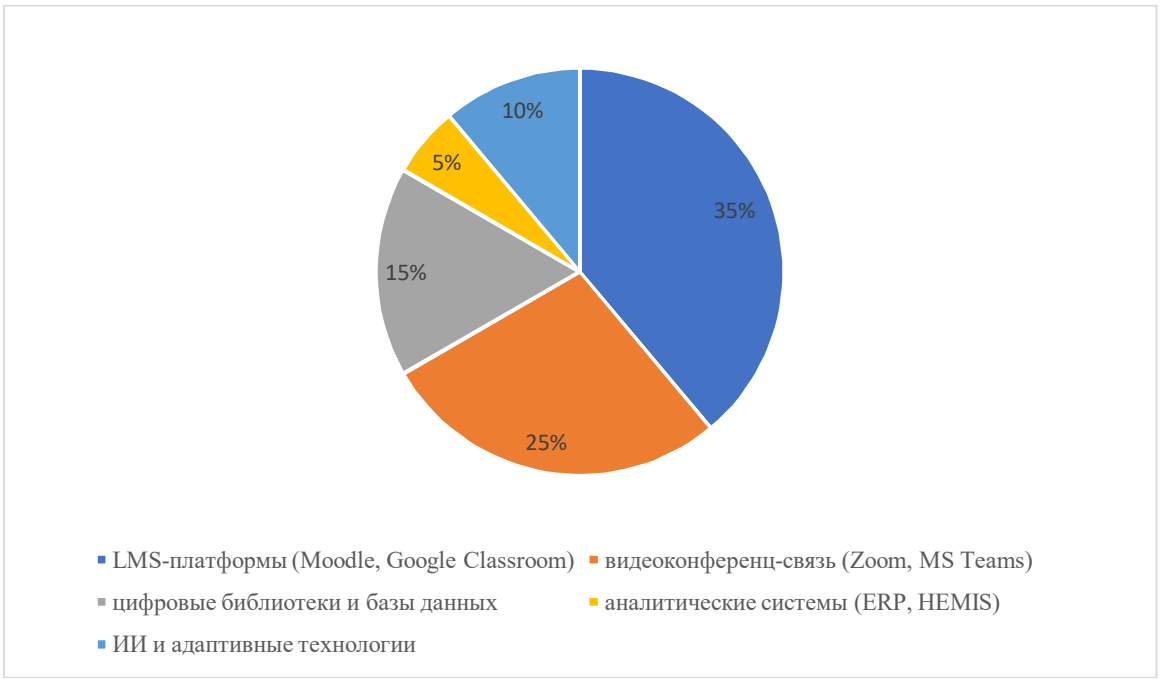


Рис. 2. Структура цифровых образовательных технологий в вузах

Опыт перехода к дистанционному обучению в 2020 году продемонстрировал готовность страны к масштабным образовательным трансформациям. Существенную роль сыграли развитая телекоммуникационная инфраструктура, доступность цифровых платформ и высокий удельный вес молодежи в структуре населения. В системе высшего образования реализуются стратегические реформы [8], направленные на повышение качества подготовки кадров, расширение охвата обучающихся и интеграцию в международное образовательное пространство [9].

Важное место в развитии цифрового образования занимает подготовка IT-кадров. Совместно с частным сектором правительство запустило платформу RoboTech для преподавания робототехники в государственных школах. Реализация проектов «Один миллион программистов», развитие IT-школ, техникумов и профильных университетов, а также деятельность IT-Park создают основу для формирования конкурентоспособного человеческого капитала [10].

Подводя итог, следует отметить, что цифровизация образования является объективной необходимостью современного этапа развития общества. Несмотря на существующие

ограничения и вызовы, цифровая образовательная среда не заменяет традиционную систему, а дополняет и обогащает ее, делая обучение более гибким, открытым и ориентированным на индивидуальные потребности. Уровень развития цифрового образования во многом будет определять качество подготовки специалистов и их конкурентоспособность на глобальном рынке труда [11]. Цифровизация представляет собой объективную и неизбежную тенденцию современного этапа развития общества, при этом она не является альтернативой традиционной системе образования, а выступает инструментом её модернизации и качественного обновления. Формирование эффективной цифровой образовательной среды требует комплексного подхода, включающего развитие инфраструктуры, повышение квалификации преподавателей и совершенствование нормативно-правовой базы. В условиях глобальной конкуренции именно уровень развития цифрового образования во многом определит качество человеческого капитала и конкурентоспособность выпускников на международном рынке труда, а для Республики Узбекистан цифровая трансформация образования становится одним из ключевых факторов устойчивого социально-экономического развития.

Библиографический список

1. Johnston J., Barker L. T. Assessing the impact of technology in teaching and learning: A sourcebook for educators. Institute of Social Research, University of Michigan, 2002. с. 119–137.
2. Итоги: 7 трендов в образовании в Узбекистане в 2022 году. 23 декабря 2022 г., URL: https://www.spot.uz/ru/2022/12/23/education/ (дата обращения: 31.01.2023)
3. Указ Президента Республики Узбекистан, от 05.10.2020 г. № УП-6079, «Об утверждении стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации, URL: https://lex.uz/ru/docs/5031048 (дата обращения: 31.01.2023)
4. Указ Президента Республики Узбекистан, от 28.01.2022 г. № УП-60, «О стратегии развития нового Узбекистана на 2022 – 2026 годы», URL: https://lex.uz/ru/docs/5841077 (дата обращения: 31.01.2023)
5. Постановление от 14.10.2024 г. № ПП-358 «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года». https://www.norma.uz/novoe_v_zakonodatelstve/utverjdena_strategiya_razvitiya_tehnologiy_iskusstvennogo_intellekta_do_2030_goda
6. Мирзиёев Ш.М. О том, какие перемены ожидаются в экономике Узбекистана в ближайшие пять лет. 9 сентября 2021, URL: https://www.spot.uz/ru/2021/09/09/program/ (дата обращения: 31.01.2023)
7. Такиуллин, Т.Р. Влияние цифровизации на систему образования / Т. Р. Такиуллин. – Текст : непосредственный // Молодой ученый. – 2021. – № 47 (389). – С. 5-8., URL: https://moluch.ru/archive/389/85723/ (дата обращения: 15.01.2023).
8. Указ Президента Республики Узбекистан, от 08.10.2019 г. № УП-5847 Об утверждении концепции развития системы высшего образования республики Узбекистан до 2030 года. URL: https://lex.uz/ru/docs/4545887 (дата обращения: 31.01.2023)
9. Концепция развития системы высшего образования Республики Узбекистан до 2030 года (Приложение №1 к Указу Президента РУз от 08.10.2019 г. №УП-5847). URL: https://nrm.uz/contentf?doc=602370_&products=1_vse_zakonodatelstvo_uzbekistana (дата обращения: 31.01.2023)
10. Налажена система непрерывной подготовки кадров в сфере ИКТ, URL: https://mitc.uz/ru/pages/ict_education (дата обращения: 31.01.2023)
11. Abdurakhmanov K.K., Khakimov N.K., Ruzieva R.H., Makhmutkhodjaeva L.S., Tozhaliev A.A. Higher education as a significant factor of Uzbekistan's sustainable development, Espacios. 2019. Т.40, № 9, С.15.

УДК 378.147:004.8; ГРНТИ 14.35:28.23

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ СИСТЕМ ДЕТЕКЦИИ ИИ-КОНТЕНТА В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

Ю.С. Кострова

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, julia-alpha@rambler.ru

Аннотация. Исследование посвящено проблеме верификации в образовательной среде посредстовм различных систем детекции ИИ-контента. Представлен сравнительный анализ эффективности ИИ-детекторов (GPTZero, Plagiat AI, AIChecker, Decopy AI, ZeroGPT, Originality AI) в контексте разных научных областей. Выявлена нестабильность работы ИИ-детекторов: высокий процент ложных срабатываний, низкая чувствительность к семантическому содержанию тестируемых текстов. Сделан вывод о необходимости комплексного подхода, сочетающего техническую проверку с экспертным мнением преподавателя.

Ключевые слова: искусственный интеллект, ИИ-детектор, академическая нечестность, верификация авторства, антиплагиат.

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF AI-CONTENT DETECTION SYSTEMS IN AN EDUCATIONAL ENVIRONMENT

Y.S. Kostrova

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, julia-alpha@rambler.ru

The summary. This study focuses on the problem of content verification within the educational environment using various AI detection systems. A comparative analysis of the effectiveness of AI detectors (GPTZero, Plagiat AI, AIChecker, Decopy AI, ZeroGPT, Originality AI) across different scientific disciplines is presented. The analysis reveals significant instability in the performance of AI detectors, characterized by a high rate of classification errors and low sensitivity to the semantic content of the tested texts. It is concluded that a comprehensive approach is necessary, combining technical verification with the expert judgment of instructors.

Keywords: artificial intelligence, AI detector, academic dishonesty, authorship verification, antiplagiarism.

Стремительное развитие языковых моделей таких, как ChatGPT, Qwen, DeepSeek и др., в течение последних лет кардинально изменило способы создания текстового контента. Доступность для широкой пользовательской аудитории породила новые вызовы для системы образования. Если до 2022 года основной угрозой являлось академическое мошенничество, заключавшееся в неправомерном заимствовании чужих работ, то сегодня на первый план выходит проблема верификации авторства: поиск возможностей отличить текст, созданный человеком от сгенерированного.

Для системы образования данная проблема актуальна, так как использование сгенерированных работ обесценивает учебный процессе, приводит к познавательной пассивности учащихся, снижает их когнитивные способности. Ответом на данный вызов является появление разнообразных систем детекции ИИ-контента (ИИ-детекторов). Вместе с тем эффективность таких систем остается предметом научных дискуссий. Алгоритмы детекции опираются на оценку повторяющихся паттернов, наличие субъектной авторской позиции, стилистическое и лексическое разнообразие, шаблонность, преобладание пассивных конструкций, преобладание обобщенных формулировок [1]. Однако, как отмечается рядом авторов [2], [3], [4], точность детекции зависит от предметной области и типа текста. Например, текст по физико-математическим наукам обладает строгой структурой, терминологической насыщенностью, отсутствием личной авторской позиции и не предполагает лексическое разнообразие. Это отличельная черта научных текстов в целом. В этой связи алгоритмы могут ошибочно интерпретировать эти признаки, как показатели генерации. В тоже время тексты по гуманитарным дисциплинам могут обладать большей вариативностью, что будет восприниматься ИИ-детекторами, как «человеческий» текст.

В настоящее время отсутствует единое мнение относительно достоверности конкретных ИИ-детекторов. Для системы образования это означает, что доверие ИИ-детекторам без личного критического анализа проверяемого текста со стороны преподавателя может привести, как к несправедливому обвинению студента в ИИ-плагиате, так и, наоборот, принятие сгенерированного текста за самостоятельный труд.

Цель исследования: сравнительный анализ эффективности ИИ-детекторов в контексте разных предметных областей.

Для тестирования систем детекции были выбраны три текста: 1) педагогические науки [5]; 2) физико-математические науки [6]; 3) полностью сгенерированная нейросетью Qwen статья без последующего редактирования на тему «О влиянии изучения математики на развитие когнитивных функций учащихся». Отсутствие генерации в первых двух статьях подтверждается датами их опубликования: 2011 и 2019 год соответственно.

В качестве ИИ-детекторов были выбраны: GPTZero, Plagiat AI, AIChecker, Decopy AI, ZeroGPT, Originality AI.

Ниже представлены результаты предоставления информации после проверки текста Decopy AI (рис. 1) и GPTZero (рис. 2).

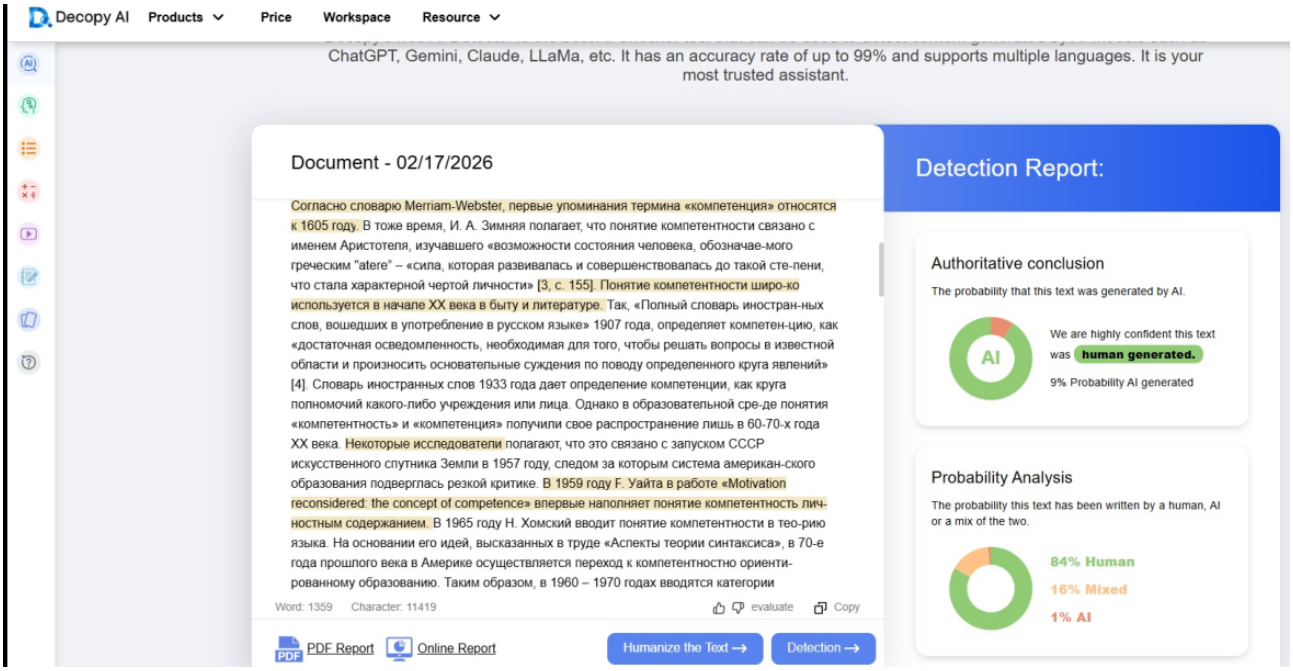


Рис. 1. Проверка текста ИИ-детектором Decopy AI

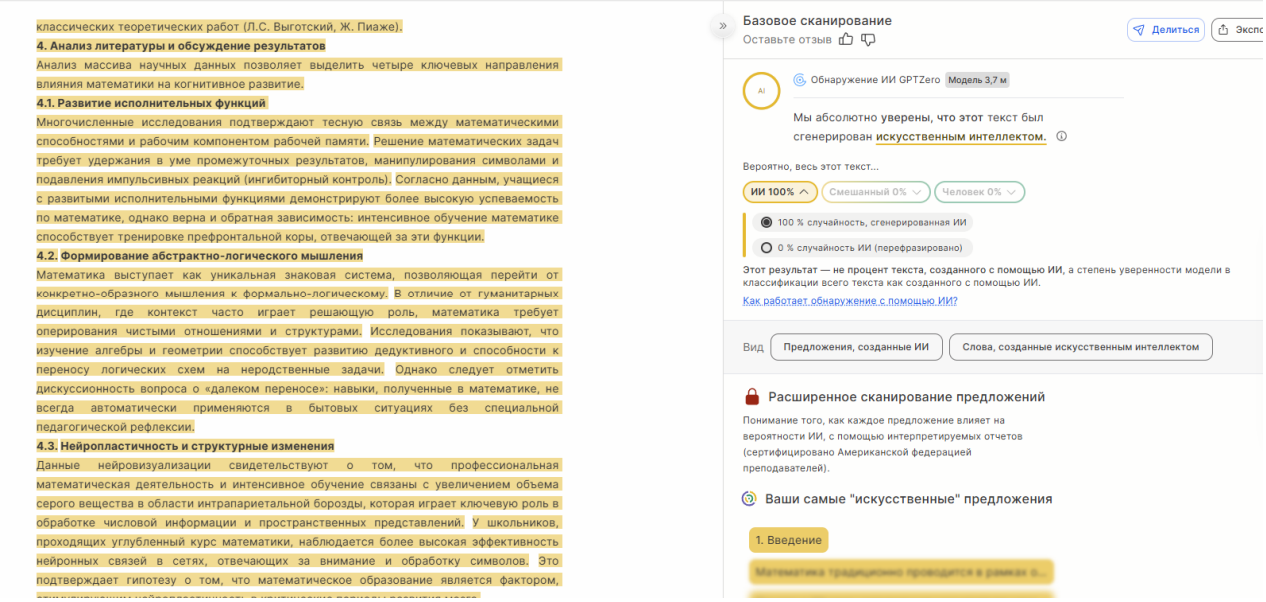


Рис. 2. Проверка текста ИИ-детектором GPTZero

Ниже представлена сводная таблица результатов тестирования (табл.1.). В ней отражен процент вероятности генерации ИИ, определенный каждой из систем для трех типов текстов.

Таблица 1. Эффективность ИИ-детекторов.

ИИ-детектор	Текст 1 (пед. науки)	Текст 2 (физ.-мат. науки)	Текст 3 (сгенерированный)
GPTZero	100% человек	100% человек	100% ИИ
Plagiat AI	86% человек 14% ИИ	96% человек 4% ИИ	91% человек 9% ИИ
AIChecker	18% человек 82% ИИ	32% человек 68% ИИ	22% человек 78% ИИ
Decopy AI	84% человек 16 % комбинация ИИ и человека 1% ИИ	84% человек 13 % комбинация ИИ и человека 3% ИИ	97% человек 3 % комбинация ИИ и человека 0% ИИ
ZeroGPT	51% человек 49% ИИ	51% человек 49% ИИ	4% человек 96% ИИ
Originality AI	100% человек	99% человек 1% ИИ	99% человек 1% ИИ

Результаты исследования позволяют сформировать объективное представление о возможностях и ограничениях современных ИИ-детекторов. В результате сравнительного анализа был выявлен ряд проблем.

1. Высокий процент ложных срабатываний. Сервисы Originality AI, Decopy AI и Plagiat AI определили текст, полностью сгенерированный ИИ, как человеческий с вероятностью 91 – 99 %. В образовательном контексте это означает, что предоставленная студентом работа (не зависимо от того, написана она самостоятельно или сгенерирована) будет признана данными системами за авторскую. Противоположный подход продемонстрировал AIChecker, определив все виды текстов, как сгенерированные. Использование данного инструмента может привести к несправедливому обвинению студента в ИИ-плагиате. Сложившаяся ситуация ставит под сомнение эффективность применения ИИ-детекторов в качестве гаранта академической честности.

2. Низкая чувствительность тестируемых систем к семантическому содержанию. Высокая точность совпадений оценки для текстов из разных областей знаний может говорить о поверхностном анализе, который учитывает лишь структуру абзацев, длину предложений, терминологическое разнообразие. Текущие версии алгоритмов не учитывают стилистические особенности различных научных направлений.

Единственным ИИ-детектором, верно распознавшим все три текста, стал GPTZero. Однако, 100% результат уверенности, который продемонстрировал данный сервис для каждого образца текста может привести к ошибкам в случаях, когда текст, сгенерированный ИИ, редактируется человеком. Для анализа данной возможности, мы отредактировали Текст №3 и снова пропустили его через ИИ-детектор GPTZero. Текст со значительными изменениями человеком (были добавлены ссылки на исследовательские работы, переформулированы сложные предложения, добавлено личное авторское мнение), был определен, как 100% сгенерированный.

Таким образом, результаты, предоставляемые современными системами детекции ИИ-контента, не могут служить надежным основанием для выявления сгенерированных учебных работ. Исследование подчеркивает необходимость комплексного подхода, где техническая проверка дополняется экспертной оценкой преподавателя.

Библиографический список

1. Weber-Wulff D, Anohina-Naumeca A, Bjelobaba S, Foltýnek T, Guerrero-Dib J, Popoola O. Testing of detection tools for AI-generated text // Int J Educ Integr. - 2023. - №19(1). P. 1-39.
2. Anderson N, Belavy DL, Perle SM, Hendricks S, Hespanhol L, Verhagen E, Memon AR. AI did not write this manuscript, or did it? Can we trick the AI text detector into generated texts? The potential future of ChatGPT and AI in sports & exercise medicine manuscript generation // BMJ Open Sport Exerc Med. – 2023. - № 9(1).
3. Erol G, Ergen A, Gülşen Erol B, Kaya Ergen Ş, Bora TS, Çölgeçen AD, Araz B, Şahin C, Bostancı G, Kılıç İ, Macit ZB, Sevgi UT, Güngör A. Can we trust academic AI detective? Accuracy and limitations of AI-output detectors // Acta Neurochir (Wien). – 2025. № 167(1). P. 214.
4. Hua H, Yao CJ. Investigating generative AI models and detection techniques: impacts of tokenization and dataset size on identification of AI-generated text // Front Artif Intell. – 2024. - №7.
5. Кострова Ю. С. Генезис понятий «компетенция» и «компетентность» // Молодой ученый. — 2011. — № 12 (35). — Т. 2. — С. 102-104.
6. Кострова Ю.С. Моделирование динамики популяции русской выхухоли в бассейне Оки // Современные технологии в науке и образовании – СТНО-2020. Сборник трудов международного научно-технического форума: в 10 томах. Под общ. ред. О.В. Миловзорова. Рязань, 2020. - С. 5 – 8.

УДК 378.241; ГРНТИ 14.35.09

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТРЕНИРОВКАХ ПРОФЕССИОНАЛЬНЫХ НАВЫКОВ НАЧИНАЮЩИХ ПСИХОЛОГОВ

О.П. Малая
Мелитопольский государственный университет,
Российская Федерация, Мелитополь, olpeta37@gmail.com

Аннотация. В данной статье были рассмотрены возможности использования искусственного интеллекта (ИИ) в тренировках профессиональных навыков начинающих психологов. В работе были сформулированы основные направления применения ИИ в подготовке будущих психологов. Проанализированы этические и технические вызовы применения ИИ в психологическом образовании.

Ключевые слова: искусственный интеллект (ИИ), программы искусственного интеллекта LLM (Large Language Models), технологии Augmented Intelligence (технологии дополненного интеллекта), психология, профессионализм, тренировки профессиональных навыков психологов.

USING ARTIFICIAL INTELLIGENCE IN PROFESSIONAL SKILLS TRAINING FOR BEGINNING PSYCHOLOGISTS

O.P. Malaya
Melitopol State University,
Russian Federation, Melitopol, olpema37@gmail.com

Abstract. This article examined the potential of using artificial intelligence (AI) in professional skills training for beginning psychologists. The paper outlined the key areas for applying AI in the training of future psychologists. The ethical and technical challenges of using AI in psychological education were analyzed.
Keywords: artificial intelligence (AI), LLM (Large Language Models) artificial intelligence programs, augmented intelligence technologies, psychology, professionalism, professional skills training for psychologists.

Актуальность исследования по теме использования ИИ в подготовке начинающих психологов обусловлена стремительной цифровизацией отрасли, которая в 2025-2026 годах перешла из стадии «экспериментов» в стадию «клинического стандарта».

Традиционное образование страдает от разрыва между теорией и практикой: студент не может тренироваться на реальных людях без риска нанести вред. Использование продвинутых LLM (Large Language Models, программ искусственного интеллекта, которые могут распознавать и генерировать текст) позволяет создавать симуляторы с реалистичным «цифровым пациентом». Это обеспечивает выпускнику безопасную среду для совершения первых 100 ошибок, не нарушая этический принцип «Primum non nocere» (не навреди) [1].

Согласно данным ВОЗ и профильных исследований 2025 года, спрос на психологическую помощь продолжает расти, опережая темпы подготовки специалистов. ИИ позволяет масштабировать процесс обучения. Выпускник, тренировавшийся на ИИ-тренажерах, выходит в практику с более высокой «насмотренностью» и готовностью к интенсивному приему, что критически важно для системы здравоохранения.

Традиционная супервизия субъективна и зависит от личности наставника. ИИ-аналитика позволяет проводить «Супервизию 2.0» – беспристрастный аудит сессий выпускника. Система фиксирует микро-ошибки (директивность, закрытые вопросы, пропуск эмоциональных маркеров), которые человек может не заметить. Исследование помогает внедрить эти объективные метрики в образовательный стандарт [2].

В 2026 году владение инструментами ИИ стало обязательной компетенцией (Hard Skill) для психолога. Начинающий психолог должен уметь работать в цифровой среде. Тренировки на ИИ-моделях естественным образом развивают навыки дистанционного консультирования, понимание специфики текстовой эмпатии и работы с цифровым следом клиента. Данное исследование актуально, так как оно обучает выпускника не просто психологии, а эффективному и безопасному содружеству с ИИ-ассистентами, что предотвращает профессиональное выгорание в будущем. Исследование отвечает на вызов времени: как превратить «теоретического выпускника» в «практикующего профессионала» в кратчайшие сроки, минимизируя риски для клиентов и повышая качество психологической помощи за счет технологий Augmented Intelligence (дополненного интеллекта) [3].

Исследованием применения искусственного интеллекта в тренировках профессиональных навыков начинающих психологов занимались такие ученые, как А.О. Лаврова, А.Р. Газизов, А. Сычева, А. Хаттенлохер, Б. Ву, Г. Киссинджер, Д.В. Альжев, И. Бенджио, Л.А. Беляева, М. Митчелл, М. Тегмарк, П. Норвиг, П. Панда, С. Вольфрам, С. Рассел, Ч. Аггарвал, Ш. Зубков, Э. Шмидт, Я. Гудфеллоу и другие.

Цель данного исследования – рассмотреть направления использования искусственного интеллекта в тренировках профессиональных навыков начинающих психологов.

Использование ИИ в подготовке будущих психологов – это переход от теории к «безопасному полигону», где цена ошибки равна нулю, а опыт накапливается в геометриче-

ской прогрессии. Искусственный интеллект в образовании психологов – это не замена человеческого наставничества, а создание «тренажерного зала высокого разрешения». Он позволяет выпускнику совершить свои первые 100 ошибок в безопасной среде, чтобы к первому реальному клиенту прийти уже не испуганным новичком, а подготовленным профессионалом с устойчивыми мета-навыками.

Вот основные направления применения ИИ в подготовке будущих психологов:

1. ИИ как интерактивный «симулятор пациента». Это направление является фундаментальным, так как оно решает главную проблему выпускника – дефицит реальной практики и страх перед «живым» клиентом. ИИ превращает пассивное обучение (чтение учебников) в активное формирование нейронных связей через действие:

– отработка различных психотипов – возможность программирования ИИ-агентов с конкретными радикалами (истероид, нарцисс, параноид и т.д.) для тренировки навыка диагностики «на лету» [4];

– симуляция сложных кейсов – моделирование острых состояний (панические атаки, суицидальный риск, сопротивление), с которыми начинающему специалисту страшно столкнуться в реальной практике;

– вариативность сценариев – отработка одной и той же ситуации с разными исходами в зависимости от выбранной стратегии терапевта [5].

2. Аналитическая поддержка и Супервизия 2.0. Это направление раскрывает ИИ не как собеседника, а как высокоточный измерительный прибор. В традиционном обучении супервизия субъективна и ограничена памятью студента. «Супервизия 2.0» предлагает беспристрастный, поминутный аудит профессионального поведения [6].

– Мгновенная обратная связь: нейросети могут анализировать транскрипт сессии и указывать на ошибки: закрытые вопросы, нарушение этики, навязывание мнения или пропуск важных маркеров в речи клиента.

– Анализ невербалики: использование компьютерного зрения для фиксации микромимики, тембра голоса и пауз (как терапевта, так и симулируемого клиента), что критически важно для развития эмпатии.

– Объективизация прогресса: составление «карты навыков» студента на основе данных сотен тренировочных сессий [7].

3. Развитие мета-навыков (Soft Skills). В контексте подготовки начинающих психологов использование ИИ для развития Soft Skills (мета-навыков, навыков социально-психологического реагирования специалиста) – это тренировка психологических компетенций в условиях, где студент может позволить себе быть несовершенным, чтобы в итоге стать профессионалом [8].

– Тренировка выдержки: использование ИИ для имитации агрессивных или провокативных клиентов, что помогает выпускнику выстроить «внутреннюю опору» и личные границы.

– Навык концептуализации: ИИ помогает студенту синтезировать данные сессии в стройную терапевтическую гипотезу, предлагая альтернативные взгляды на кейс [9].

– Преодоление «страха чистого листа»: использование чат-ботов для ролевых игр, где студент может бесконечно пробовать разные техники (КПТ, гештальт, психоанализ) без риска навредить живому человеку [10].

4. Этические и технические вызовы. Это направление исследований уравновешивает технологический оптимизм и переводит дискуссию в плоскость профессиональной ответственности. Внедрение ИИ в подготовку психологов – это не только технический прогресс, но и зона высокого этического риска [11].

– Риск алгоритмических искажений: проблема «галлюцинаций» ИИ и возможность формирования у студента неверных паттернов поведения.

– Эмпатический разрыв: дискуссия о том, может ли машина полноценно обучить человеческой сопричастности.

– Конфиденциальность данных: защита учебных кейсов и персональных данных студентов при использовании облачных ИИ-платформ [12].

Таким образом, развитие Soft Skills через ИИ превращает обучение из «заучивания техник» в формирование терапевтической идентичности. Студент выходит на первую встречу с реальным клиентом уже имея опыт «столкновения» с самыми разными человеческими проявлениями. ИИ не заменяет супервизора-человека, но становится высокотехнологичным тренажерным залом, который позволяет выпускнику выйти в реальную практику не с «чистыми руками», а с наработанными часами «налета» в виртуальной среде. Использование ИИ-симуляторов позволяет внедрить объективный структурированный клинический экзамен (ОСКЭ). Вместо билетов студент заходит в чат или голосовой интерфейс с «незнакомым пациентом», а система оценивает его навыки по четким критериям: эмпатия, удержание структуры сессии, этичность. Актуален «умный» дашборд супервизора, где вместо долгого прослушивания записи он видит «тепловую карту» сессии: красным отмечены зоны этического риска, зеленым – удачные интервенции, синим – моменты потери контакта. Это делает обучение в десятки раз плотнее и эффективнее.

Этические вызовы требуют создания «Цифрового кодекса психолога-педагога», который бы регламентировал использование нейросетей в учебном процессе. Основной задачей остается сохранение гуманистической сути профессии при использовании мощных аналитических инструментов ИИ.

Библиографический список

1. Газизов, А.Р. Цифровые инструменты психолога: от симуляторов до нейросетей / А.Р. Газизов. – Казань: Казанский университет, 2023. – 188 с.
2. Панда, П. ChatGPT. Мастер подсказок: руководство по эффективному взаимодействию с ИИ / П. Панда, А. Сычева. – СПб.: Питер, 2024. – 224 с.
3. Митчелл, М. Искусственный интеллект: подходы, вызовы, перспективы / М. Митчелл. – М.: КоЛибри, 2023. – 368 с.
4. Вольфрам, С. Как устроен ChatGPT? / С. Вольфрам. – М.: Альпина Паблишер, 2024. – 160 с.
5. Беляева, Л.А. Технологии искусственного интеллекта в профессиональном образовании: учебное пособие / Л.А. Беляева. – Екатеринбург: УрГПУ, 2024. – 154 с.
6. Зубков, А. Нейросеть на пальцах: как работает ИИ и как его использовать / А. Зубков. – М.: АСТ, 2024. – 256 с.
7. Woo, B. Artificial Intelligence in Cognitive Behavioural Therapy: A Guide for Mental Health Professionals / B. Woo. – London: Routledge, 2025. – 229 p.
8. Киссинджер, Г. Генезис: искусственный интеллект и человеческое будущее / Г. Киссинджер, Э. Шмидт, Д. Хаттенлохер. – М.: Альпина Паблишер, 2022. – 312 с.
9. Тегмарк, М. Жизнь 3.0. Быть человеком в эпоху искусственного интеллекта / М. Тегмарк. – М.: Корпус, 2020. – 560 с.
10. Рассел, С. Искусственный интеллект: современный подход / С. Рассел, П. Норвиг. – 4-е изд. – М.: Вильямс, 2021. – 1104 с.
11. Гудфеллоу, Я. Глубокое обучение / Я. Гудфеллоу, Й. Бенджио, А. Курвилль. – 2-е изд. – М.: ДМК Пресс, 2023. – 652 с.
12. Аггарвал, Ч. Нейронные сети и глубокое обучение: учебник / Ч. Аггарвал. – М.: Вильямс, 2020. – 496 с.

УДК: 378.1/004.8; ГРНТИ 14.15.15/28.23

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ

М.А. Федулов

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, fmikhail1199@gmail.com

Аннотация. В статье рассматривается влияние искусственного интеллекта (ИИ) на образование как социальный институт и на образовательный процесс. Анализируются риски безопасности данных, авторского права и нормативной базы, а также технологические изменения: рост спроса на IT-специалистов, персонализация и адаптивность учебных сред, оптимизация административных функций. Выделяются пять ключевых направлений применения ИИ: персонализация обучения, снижение нагрузки на преподавателей, генерация контента, поддержка самообразования и автоматизация оценивания. Описываются преимущества и сложности каждого направления, включая проблемы проверки творческих работ и отсутствие живого общения. В заключение подчеркивается, что ИИ трансформирует образование, но требует дальнейших исследований для улучшения качества обучения.

Ключевые слова: искусственный интеллект, образование, персонализация обучения, автоматизация оценивания, риски безопасности данных, нормативно-правовая база, этика ИИ.

POSSIBILITIES FOR THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN EDUCATION

M.A. Fedulov

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, fmikhail1199@gmail.com

The summary. The article examines the influence of artificial intelligence (AI) on education as a social institution and on the educational process. It analyzes risks related to data security, copyright, and regulatory frameworks, as well as technological changes such as the growing demand for IT specialists, personalization and adaptability of learning environments, and optimization of administrative functions. Five key directions of AI application are identified: personalized learning, reduced teacher workload, content generation, support for self-learning, and automated assessment. The advantages and challenges of each direction are described, including issues with evaluating creative work and the lack of live interaction. In conclusion, it is emphasized that AI is transforming education, but further research is required to improve the quality of learning.

Keywords: artificial intelligence, education, personalized learning, automated assessment, data security risks, regulatory framework, AI ethics.

Введение

В настоящее время технологии искусственного интеллекта (ИИ) широко проникли в большинство значимых сфер человеческой жизни, включая образование. В связи с этим возникает необходимость систематически отслеживать и анализировать изменения, которые возникают в результате внедрения ИИ в образовательный процесс в социальную структуру образовательных институтов.

Для первичной классификации влияния ИИ на образование предлагается разделить его на две основные области:

1. Влияние ИИ на образовательный институт;
2. Влияние ИИ на непосредственный образовательный процесс.

Целью данной статьи является рассмотрение возможностей и влияния использования ИИ на этих двух уровнях.

Влияние искусственного интеллекта на образование как социальный институт

Прежде чем приступать к рассмотрению возможностей ИИ непосредственно в практический деятельности, необходимо в целом оценить влияние данных технологий на образо-

вание. Современная действительность такова, что влияние ИИ охватывает всю систему образования: управление учреждениями, государственное регулирование, доступность, финансирование, развитие инфраструктуры, общественные и культурные аспекты.

При этом стоит отметить следующие риски [3]:

1. Взлома или изъятия баз данных;
   Системы ИИ часто хранят большие объёмы персональных данных, включая оценки, медицинскую информацию и планы обучения. Это делает их привлекательными целями для хакеров, которые могут использовать полученные данные для кибершпионажа или финансовых преступлений. Необходимо внедрять многоуровневые механизмы шифрования и регулярно проводить аудиты безопасности.
2. Нарушение авторских прав;
   Алгоритмы ИИ обучаются на больших корпусах текстов, изображений и видео, которые могут быть защищены авторским правом. При генерации новых материалов ИИ иногда заимствует фрагменты оригинальных источников без явного указания, что приводит к конфликтам с правообладателями. Важно использовать лицензированные наборы данных и разрабатывать системы отслеживания источников.
   Нарушение авторских прав также может возникать и из-за взлома баз данных ИИ. Хакеры, получив доступ к хранимым материалам, могут использовать их в обход лицензий, распространяя нелегальный контент или создавая копии защищённых работ без согласия владельцев.
3. Необходимость создания нормативно-правовой базы, контролирующей обеспечение защиты данных.
   Текущие законы часто не учитывают особенности ИИ, такие как автономное принятие решений и ответственность за ошибки. Для обеспечения справедливости и защиты прав участников образовательного процесса требуется разработка чётких регуляций, которые определяют ответственность за утрату данных, нарушения авторских прав и недобросовестное использование ИИ.

Технологии искусственного интеллекта уже сейчас трансформируют образовательный сектор, внося значительные изменения в потребности кадров, методы обучения и административные процессы.

- Рост потребностей в квалифицированных IT-специалистах.
  С увеличением интеграции ИИ в образовательные системы растёт спрос на специалистов, умеющих разрабатывать, внедрять и поддерживать модели управления ИИ и машинного обучения.
- Акцент на персонализированное обучение.
  ИИ способен анализировать успеваемость и стиль обучения каждого студента, предлагая индивидуальные траектории и материалы, что теоретически повышает эффективность усвоения знаний.
- Адаптивность учебной среды.
  Учебная среда с внедренным ИИ автоматически подстраивает материал под особенности каждого ученика, поддерживая инклюзивное образование, учитывая наличие инвалидности, языковые барьеры, разные уровни подготовки и стили обучения.
- Управление образовательными учреждениями.
  ИИ может использоваться для оптимизации расписания, распределения ресурсов, прогнозирования потребностей и улучшения административных процессов, тем самым повышая общую эффективность школ и вузов.

Возможности использования технологий искусственного интеллекта в образовательном процессе

Данной области уделено намного большее внимание, и она фокусируется на инструментах и процессах, которые непосредственно используют учителя и студенты: персонализация обучения, разработка новых образовательных материалов, оценивание результатов, обработка обратной связи и уровня мотивация. Если систематизировать примеры использования ИИ, описанные в различных статьях [1, 2, 4, 5], можно выделить следующие пять ключевых направлений:

- персонализация образования;
- снижение рабочей нагрузки на преподавателей;
- генерация контента для обучающихся;
- помощь обучающемуся в самообразовании;
- помощь в выполнении оценочных процедур.

Однако данное разделение является достаточно общим и требует конкретизации.

1. Персонализация образования

Данное направление отмечают многие авторы [1, 4, 5]. Обычно ими отмечаются следующие варианты использовании ИИ:

- адаптация учебной программы под конкретного обучающегося. Персонализированные учебные планы формируются на основе анализа успеваемости, предпочтений и стиля обучения студента. Такой подход повышает вовлечённость и ускоряет усвоение материала, позволяя каждому студенту продвигаться в собственном темпе;
- создание уникальных образовательных траекторий. Модели рекомендательного характера строят индивидуальные пути обучения, учитывая, как академические цели, так и личные интересы. Система предлагает последовательность курсов, проектов и практических заданий, которые оптимально сочетаются с предыдущим опытом и будущими карьерными планами. Это позволяет студентам более эффективно развивать нужные навыки и достигать профессиональных целей;
- индивидуальная обратная связь на основе собранных данных. Обратная связь генерируется в реальном времени, включающая конкретные примеры ошибок, советы по повторению и ресурсы для самостоятельного изучения. Такой персонализированный подход ускоряет исправление ошибок и повышает качество усвоения материала;
- адаптируемый доступ. Текст учебного материала может быть автоматически переведен на удобный для обучающегося язык, а также перефразирован простыми словами, чтобы сложные концепции становились более доступными. ИИ-технологии автоматически регулируют сложность и формат контента в зависимости от текущего уровня студента, обеспечивая плавный переход от простых к более сложным задачам.

Используя эти варианты преподавателю будет легче осуществлять индивидуальный подход к обучению, что способствует повышению качества усвоения учебного материала.

2. Снижение рабочей нагрузки на преподавателей

Это направление в рассмотренных источниках не озвучено непосредственно, но неоднократно встречается в форме следующих возможностей применения технологий искусственного интеллекта:

1. Автоматизация рутинных задач.

ИИ может автоматически проверять орфографию и грамматику сданных, что экономит время на ручной корректуре. Системы распознавания образов позволяют быстро сканировать и сортировать документы, а также генерировать отчёты о посещаемости;

2. Автоматический подбор материалов для студентов в отдельных темах.

На основе анализа учебных планов и предыдущих оценок ИИ предлагает персональные списки чтения и видеолекции. Алгоритмы рекомендаций учитывают интересы студента, тем самым повышая мотивацию и эффективность обучения. Подобранные материалы автоматически обновляются, когда в курсе появляются новые исследования или актуальные кейсы. ИИ-модели прогнозируют, какие темы потребуют дополнительного внимания, и автоматически подбирают материалы, которые соответствуют текущему уровню знаний;

3. Помощь в повышение квалификации. ИИ анализирует карьерные цели и текущие знания преподавателя, предлагая курсы, вебинары и литературу, соответствующую его уровню. Система автоматически уведомляет об обновлениях в области методики преподавания и новых технологий. Персонализированные планы развития помогают преподавателям эффективно использовать свободное время для самосовершенствования;

4. Анализ результатов обучения. ИИ обрабатывает данные о результатах, выявляет тренды и предоставляет интерактивные дашборды, которые помогают принимать решения. Система генерирует отчёты о производительности групп, а также рекомендации по улучшению методик и контента. Аналитические выводы позволяют быстро реагировать на проблемы в обучении и адаптировать учебный процесс.

3. Генерация контента для обучающихся

Данное направление может стать удобным инструментом, позволяющим быстро адаптировать учебные материалы под меняющиеся условия работы. Она повышает доступность и качество образования, делая его более персонализированным, интерактивным и ориентированным на практические навыки.

- Создание образовательного контента
  ИИ может автоматически генерировать учебные материалы на основе заданных тем и уровней сложности. С помощью генеративных моделей можно быстро обновлять контент, интегрируя новые исследования, актуальные кейсы и мультимедийные элементы.
- Создание “умного” контента
  “Умный” контент адаптируется под конкретные потребности студента, используя данные о его успеваемости, интересах и стиле обучения. Системы могут предлагать персонализированные задания, интерактивные симуляции и мгновенную обратную связь, повышая вовлечённость и эффективность усвоения материала. Интеграция с LMS позволяет автоматически отслеживать прогресс и корректировать контент в реальном времени.
- Создание образовательных приложений
  Генеративные модели могут автоматически создавать прототипы мобильных и веб-приложений, включая пользовательские интерфейсы, сценарии взаимодействия и базовые функции. Приложения могут включать чат-ботов, которые отвечают на вопросы студентов, предоставляют вспомогательные ресурсы и фиксируют успеваемость.
- Создание безопасных и децентрализованных систем обучения
  Интеграция блокчейн-технологий обеспечивает прозрачность и неизменность записей о достижениях, дипломах и сертификатах, защищая их от фальсификации. Децентрализованные платформы позволяют хранить учебный контент и данные студентов на распределённых узлах, повышая устойчивость к единой точке отказа и обеспечивая конфиденциальность.

Применение этих технологий позволит преподавателям экономить время на подготовке лекций и создавать более динамичные и актуальные учебные ресурсы. В результате

преподаватели освобождаются от рутинной подготовки, а студенты получают более динамичные и актуальные ресурсы для эффективного обучения.

4. Помощь обучающемуся в самообразовании

Использование ИИ позволяет студентам самостоятельно планировать учебный путь, предлагая персонализированные ресурсы и задания, которые соответствуют их интересам и целям.

- Анализ интересов студентов
  ИИ может собирать и обрабатывать данные о том, какие темы, форматы и ресурсы привлекают внимание студента. На основе этих данных система генерирует персонализированные рекомендации по материалам, курсам и проектам, которые соответствуют индивидуальным интересам.
- Выявление проблемных зон у обучающихся
  Анализируя ответы на тесты, домашние задания и активность в LMS, ИИ может ранжировать области, где студент испытывает трудности. Система способна автоматически предлагать дополнительные упражнения, объяснительные видео или живые сессии с наставником, фокусируясь на конкретных слабых местах.
- Чат-боты - виртуальные помощники
  Чат-боты, основанные на диффузионных LLM, способны вести диалог на естественном языке, отвечать на вопросы и предоставлять ресурсы в режиме реального времени. Они могут интегрироваться с учебными платформами, чтобы автоматически выдавать ссылки на лекции, раздаточные материалы и задания. Такой помощник повышает доступность информации и снижает нагрузку на преподавателей, позволяя студенту получать ответы в любое время.
- Помощь в профориентации
  ИИ может анализировать навыки, интересы и академические достижения студента, сопоставляя их с требованиями различных профессий и отраслей. На основе этой информации система предлагает индивидуальные карьерные траектории, курсы развития навыков и возможные стажировки.

Данное направление способно повысить мотивацию и вовлечённость, позволяя студенту самостоятельно строить учебный путь, который ему действительно интересен. Это позволяет сократить время, затрачиваемое на исправление ошибок, и ускоряет процесс усвоения материала.

5. Помощь в выполнении оценочных процедур

Это направление отмечается достаточно редко в силу своей новизны.

- Проверка экзаменов
  Автоматизированные системы используют алгоритмы машинного обучения для оценки письменных ответов, проверяя грамматику, логическую структуру и соответствие ключевым идеям. Это позволяет сократить время, затрачиваемое на ручную проверку, и обеспечивает более объективные результаты.
- Мониторинг нарушений в процессе сдачи онлайн-экзаменов
  Интеграция видеокамер и микрофонов с системами распознавания речи и лиц позволяет отслеживать подозрительные действия, такие как копирование с интернета, использование внешних устройств или смена местоположения. Алгоритмы аномалий сигнализируют о возможных нарушениях в реальном времени, обеспечивая справедливость оценивания.
- Инструменты, измеряющие внимание, эмпатию и эмоции
  Использование датчиков движения глаз, анализа голоса и распознавания эмоциональных выражений позволяет оценивать вовлеченность студента и его эмоциональное состояние во время экзамена. Эти данные помогают преподавателям адаптировать во-

просы, выявлять потенциальные трудности и обеспечивать более персонализированную обратную связь.

В целом, автоматизированная помощь в оценочных процедурах повышает точность, скорость и справедливость оценивания, одновременно предоставляя преподавателям инструменты для более глубокого анализа ответов и адаптации образовательных программ. Эти технологии позволяют сфокусироваться на педагогическом взаимодействии, освобождая время от рутинных проверок и улучшая качество образовательной обратной связи.

Сложности, возникающие при использовании технологий ИИ

Внедрение искусственного интеллекта в образовательный процесс открывает новые возможности, но также сопряжён рядом сложностей, которые необходимо учитывать для эффективного использования технологий.

- Проверка выполнения заданий
  В случае автоматической проверки заданий ИИ иногда не способен адекватно оценить творческие и контекстуальные ответы, что приводит к ошибочным оценкам. Помимо этого, сам обучающийся может использовать ИИ для получения готового ответа, вместо самостоятельного поиска решения.
- Отсутствия живого общения
  При передаче ИИ роли учителя возникает недостаток живого общения, исчезает возможность непосредственного взаимодействия, что снижает мотивацию студентов.
- Отсутствие эмпатии
  ИИ не способен распознавать эмоциональное состояние учащихся, поэтому не может адаптировать подход к индивидуальным потребностям.
- Разделение педагогического сообщества
  Существуют явные разделения между сторонниками и критиками использования ИИ, что затрудняет консенсус по методикам.
- Отсутствие воспитательной составляющей
  Важные аспекты нравственного и личностного развития могут быть упущены при автоматизации образовательных процессов.
- Трудность объяснения решений ИИ
  Преподаватели и студенты часто испытывают сложности в понимании того, как ИИ принимает решения, что приводит к недоверию.

Заключение

В статье рассматриваются как социальные, так и практические аспекты внедрения искусственного интеллекта (ИИ) в образовательный процесс.

Основные выводы:

1. ИИ трансформирует управление учреждениями и культурные аспекты образования, создавая при этом риски, связанные с безопасностью данных, авторским правом и отсутствием нормативной базы;
2. ИИ способствует росту потребностей в IT-специалистах, персонализации обучения, адаптивности учебных сред и оптимизации административных процессов.

Ключевые направления использования технологий ИИ:

- персонализация образования;
- снижение нагрузки преподавателей;
- генерация контента;

- поддержка самообразования;
- автоматизация оценивания.

Каждое из этих направлений имеет свои преимущества и сложности, такие как риск недостоверной оценки творческих работ, потеря живого общения и трудности в объяснении решений ИИ.

Основные выявленные сложности:

- вопросы безопасности и этики;
- отсутствия эмпатии и воспитательных аспектов.

Дальнейшая научная работа будет сосредоточена на анализе возможностей искусственного интеллекта в области генерации образовательного контента. Это включает:

- разработку моделей, автоматически создающих адаптивные учебные материалы, интерактивные задания и оценочные инструменты;
- исследование эффективности этих материалов в реальных образовательных средах;
- разработку механизмов контроля качества генерируемого контента.

Ожидается, что результаты исследований внесут вклад в создание более доступных, персонализированных и эффективных методов обучения.

Библиографический список

1. Еськин Д.Л. Использование технологий искусственного интеллекта в обучении. Журнал «Мир науки, культуры, образования», 2023, № 6(103), с. 329–331.

2. Канатьев П. В., Филатова О. Н., Зиновьева С. А. Применение нейросетей в образовательном процессе среднего и высшего профессионального образования. В: Проблемы современного педагогического образования. Ялта: РИО ГПА, 2024, вып. 84, ч. 4, 467с. с. 67–69.

3. Рафикова А.И. О возможностях использования технологий искусственного интеллекта в сфере образования // Образование. Наука. Научные кадры. 2022. № 2. С. 252-254. doi: 10.24412/2073-3305-2022-2-252-254.

4. Руденко М. Б.; Голодков Ю. Э.; Карелин А. Г. Искусственный интеллект в образовании: возможности и риски. Образование и право, 2023, №10, с. 363 366.

5. Шобонов Н. А.; Булева М. Н.; Зиновьева С. А. Искусственный интеллект в образовании. В: Проблемы современного педагогического образования. Ялта: РИО ГПА, 2023. Вып. 79, Ч. 4, 332 с. с. 288–290.

УДК 372.853; ГРНТИ 14.25.07

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ НЕЙРОСЕТИ DEEPSEEK УЧИТЕЛЕМ НА УРОКАХ ФИЗИКИ

В.Н. Семыкина, О.Р. Шефер

Южно-Уральский государственный гуманитарно-педагогический университет, Россия, Челябинск semykinavn@inbox.ru, shefer-olga@yandex.ru

Аннотация. В статье рассматривается особенности применения нейросети DeepSeek в образовательном процессе. Предложены методические приемы использования ряда ее возможностей на уроках физики, и при разработке учителем сценариев проведения учебных занятий и организации внеурочной деятельности по предмету «Физика».

Ключевые слова: нейросети, уроки физики, методические приемы, учитель.

POSSIBILITIES OF USING THE DEEPSEEK NEURAL NETWORK BY A TEACHER IN PHYSICS LESSON

V.N. Semykina, O.R. Shefer

South Ural State Humanitarian Pedagogical University, Russia, Chelyabinsk, semykinavn@inbox.ru, shefer-olga@yandex.ru

Annotation. The article examines the features of using the DeepSeek neural network in the educational process. Methodological techniques are proposed for using a number of its capabilities in

physics lessons, and for the teacher's development of scenarios for conducting training sessions and organizing extracurricular activities in the subject of Physics.
Keywords: neural networks, physics lessons, methodological techniques, teacher.

Нейронная сеть – вычислительная модель, созданная по аналогии со структурой и принципами работы биологических нейронных сетей (например, человеческого мозга). Нейросеть состоят из взаимосвязанных элементов – искусственных нейронов, объединенных в слои, которые обрабатывают информацию путем передачи сигналов между собой, а алгоритм, лежащий в ее основе, имитируя работу человеческого мышления, может выполнять сложные задачи и обучаться на примерах (хоть и без понимания смысла, как такового).

Учитывая популярность нейросетей среди учащейся молодежи, проанализируем особенности и возможности одной из них – нейросеть DeepSeek [7].

Преимущества DeepSeek:

- бесплатный доступ к нейросети;
- отсутствие ограничений по количеству запросов;
- возможность получения помощи в понимании сложных тем на основе объяснения одной и той же темы разными методами (аналогии, схемы, упрощения), иллюстрация на подробных примерах, связанных с реальной жизнью;
- возможность выполнять при объяснении процесса решения задачи и подбора при необходимости (наличии) различных методов ее решения роль «Репетитора».
- возможность загружать запрос (условие задания) в виде фотографии;
- наличие оптимальной скорости обработки запросов по отношению к другим бесплатным полностью или демоверсиям нейросетей;
- возможность генерации игровых и творческих форматов (квесты, головоломки и др.)
- наличие безопасной среды для несовершеннолетних пользователей (строгие фильтры гарантируют вежливый ответ на поставленный вопрос, без оскорблений и недопониманий);
- возможность работать с нейросетью на разных устройствах без скачивания через браузер, мобильные приложения;
- наличие поддержки работы с различными файлами (PDF, Word, Excel, PowerPoint, содержащими изображения, текст;
- возможность локальной поддержки и адаптации под российский контекст;
- отсутствие ограничений на использование в России (на момент написания статьи).

Недостатки DeepSeek:

- ограниченная интеграция с популярными образовательными платформами и нейросетями, для преодоления этого недостатка необходимо использовать API;
- отсутствует офлайн-режим, требуется постоянное Интернет-соединение;
- возможны ошибки в интерпретации сложных тем;
- мало инструментов для совместной работы, т.к. нейросеть ориентирована на индивидуальное использование ее возможностей.

Использование нейросетей в образовании имеет свои серьезные плюсы и минусы. С одной стороны нейросети помогают разбираться в разной сложности материале ученикам, учиться искать нужный материал, замечать ошибки в формулировках, формулах и объяснениях простых процессов, но с другой стороны ученики часто применяют нейросети для списывания [4; 6] (контрольные работы, самостоятельные работы и пр.), выполнения домашних заданий, не пытаясь разобраться в материале самим, создания докладов и т.д. [1] Учителям приходится подстраиваться и применять новые методы в обучении в новых реалиях. Рассмотрим особенности применения нейросети DeepSeek [3] в учебном процессе и методической деятельности учителя физики.

1. Нейросеть, как инструмент подготовки к учебным занятиям.

Основная часть профессиональной деятельности учителя – методическая работа: подбор или разработка дидактического материала, разработка сценариев учебных занятий, и работа с нормативными документами. С помощью нейросетей процесс выполнения задач, лежащих в основе достижения результатов этой деятельности, можно оптимизировать за счет их детализации, минимизируя тем самым временные затраты учителя на подготовку учебных занятий.

Разработка конспектов и технологических карт учебных занятий, занятий в рамках внеучебной деятельности, дополнительных занятий.

На основе полученных файлов и запроса пользователя DeepSeek выдает таблицы, поэтапные решения проблем и возможные варианты, идей. Учитель может задать запрос на генерацию нейросетью нескольких идей – основы для методических разработок. Но дорабатывать и собирать в единый сценарий учебного процесса учителю придется самому с опорой на свои профессиональные компетенции, исправляя возможные ошибки, которые выдает нейросеть, в том числе и за счет корректности в запросах.

2. Оптимизация действий с нормативными документами.

С помощью нейросети DeepSeek можно создавать документы. Стоит лишь задать нейросети необходимую информацию и пример исполнения задания (если такой имеется), что оптимизирует работу учителя с документацией по образовательному процессу.

3. Проверка и оценка заданий контрольных и диагностических работ учащихся, требующих развернутого ответа.

В некоторых отчетах по контрольным и диагностическим работам встречаются не совсем корректные ответы учащихся, которые учитель не знает, как оценивать или ему требуются дополнительные материалы, чтобы понять, о чем пишет ученик. На основе запроса и фото самой работы, нейросеть внесет ясность в работу.

4. Применение нейросети на учебных и внеурочных занятиях [2; 5]:

- организация работ учащихся с понятийным аппаратом, изучаемого материала. Этот методический подход позволяет так организовывать учебно-познавательную деятельность учащихся, что бы они могли увидеть возможные неточности формулировок понятий и понять ключевые аспекты понятия. Реализация приема -на уроке на экран выводят интерфейс нейросети DeepSeek, которой задается задание оценить правильность формулировки понятия, ученик приводит определение понятия, которое он выучил на уроке или дома. Независимое оценивание ответа учащегося нейросетью DeepSeek позволяет увидеть неточности в приведенной им формулировке и понять за что учитель снижает оценку. Но, при этом учитель должен знать, что нейросеть может без ошибочно интерпретировать полученные данные от ученика (рис.1);

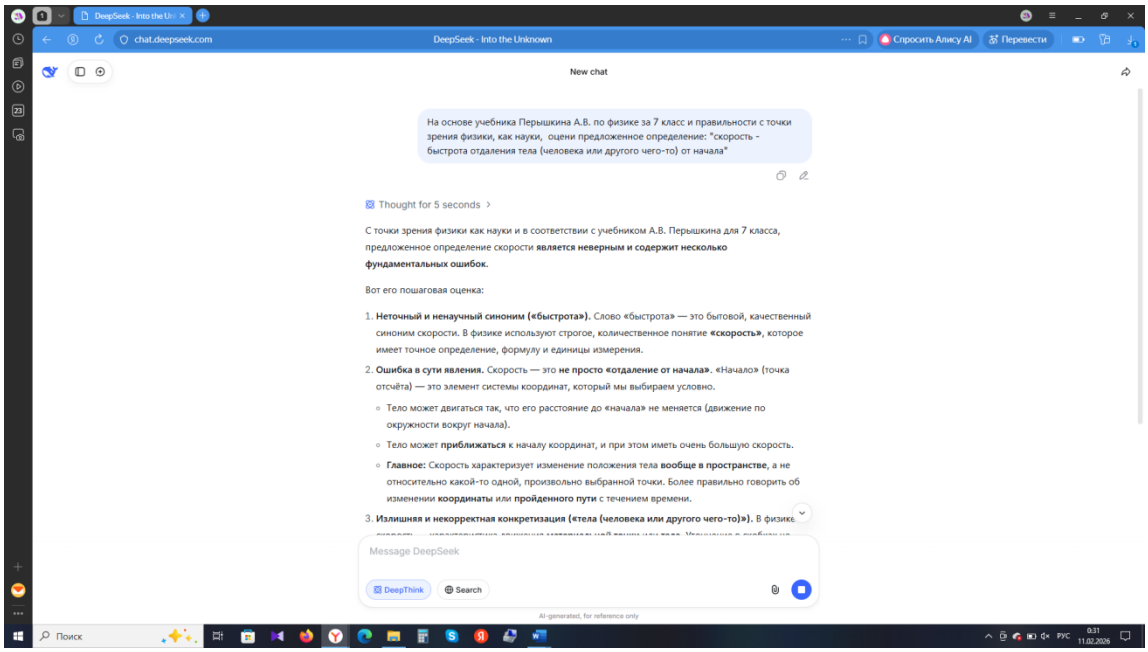


Рис. 1. Пример запроса в нейросеть определения «скорости», названного учеником 7 класса

- организация работы учащихся с моделированными нейросетью DeepSeek учебными ситуациями. Нейросеть DeepSeek способна моделировать нелинейные, многовариантные и междисциплинарные ситуации. С помощью нейросети можно моделировать эксперименты, невозможные для реализации в школьных лабораториях или противоречащие интуиции. Пример: «Смоделируй диалог между Ньютоном и Эйнштейном, где они обсуждают, что увидит наблюдатель, падающий в черную дыру. Ньютон опирается на классическую механику, Эйнштейн – на ОТО. В конце диалога выдели 3 ключевых физических противоречия». Одним из ответвлений данного пункта можно считать моделирование исторических научных открытий в «режиме реального времени» или «мира с иными законами физики». Оба метода позволят с интересом изучать физику, а не просто «зубрить» физические законы. Отметим, что модели, генерируемые нейросетью – это правдоподобный нарратив, а не точный расчет;

- организация работы учащихся по решению физических задач. Многие ученики в решении не соблюдают оформление физических задач – одного из компонентов правильно решенной задачи. Чтобы показать ученикам как нужно и как не нужно оформлять задачи, можно показать оба варианта одной задачи через нейросеть и попросить учеников оценить оба варианта (рис. 2);

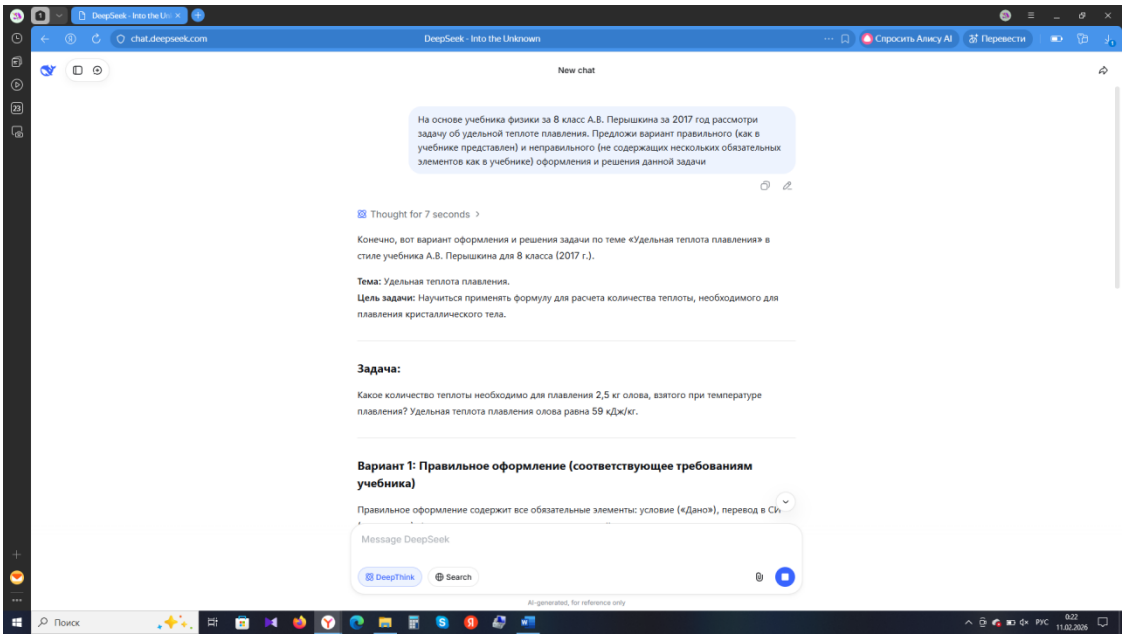


Рис. 2. Пример запроса нейросети DeepSeek «Как правильно оформить отчет по решению задачи»

- организация работы учащихся по освоению функциональной грамотностью на основе отработки навыков аргументации при освоении теории. На занятиях в средней школе нередко могут возникать дискуссии по использованию в технике или повседневной жизни человека, изучаемого физического материала. При нехватке аргументов учитель может предложить обратиться за помощью к нейросети DeepSeek;

- организация работы учащихся на физическом практикуме требует выдвижение гипотезы исследования, что не всегда корректно могут они сделать. Для формирования данного умения учитель может попросить учеников озвучить свои гипотезы, а выбор оптимальной предоставить нейросети DeepSeek, задач ей запрос: «Оцени гипотезу для школьного эксперимента: «..». Верна ли она с точки зрения формулы? Предположи, как будут выглядеть графики зависимости. Какие источники погрешностей могут исказить результат в школьной лаборатории?». Класс сравнит прогноз нейросети с реальным исходом эксперимента. Это учит критически оценивать информацию и планировать эксперимент с учетом погрешности;

- организация рефлексии учащихся в конце учебного или внеурочного занятия. В конце занятия можно попросить нейросеть задать ученикам вопросы по изучаемой теме для проверки остаточных знаний учащихся, с целью выявления сильных и слабых точек в понимании темы и даст возможность проработать их как ученикам, так и учителю в дальнейшем. Также можно попросить учеников задать вопросы по теме занятия нейросети, формулировка вопросов и понимания нейросетью DeepSeek их содержания позволят так же судить о результативности работ учащихся на занятии.

Учитывая неограниченные информационные возможности нейросети DeepSeek, учителю стоит придерживаться нескольких правил при ее использовании в учебном процессе, в частности [8]:

- цифровая гигиена и критическое мышление – нейросеть DeepSeek может неправильно интерпретировать запрос пользователя, из-за чего возникает необходимость в точности формулировок и проверке выданной информации;

- проверка корректности ответов с учетом педагогической этики – запретить нейросети DeepSeek определенные формулировки, которые могут быть оскорбительными или бессмысленными по отношению к ученикам;

- сохранение центральной роли учителя в учебном процессе на учебном и внеурочном занятии – нейросеть DeepSeek – помощник в учебном процессе, но не один из главных его представителей. Это демонстрационный материал, источник анализа и критического мышления, тренажер

Таким образом, нейросеть DeepSeek является помощником в развитии у обучающихся знания и умения необходимые для овладения учебным материалом, позволяет оптимизировать методическую работу учителя, сокращая время на подготовку к занятиям, помогая систематизировать применяемый в учебном процессе материал, но в то же время развивает профессиональные компетенции за счет критического оценивания материала, предоставляемого нейросетью.

Библиографический список

1. Искусственный интеллект в российском образовании: тренды 2024-2025/ Аналитический центр НИУ ВШЭ. – М.: ВШЭ, 2024. – 72 с.

2. Крайнева, С.В. Анализ влияния кластера педагогических технологий на формирование учебно-профессиональной мотивации студентов бакалавриата / С. В. Крайнева, О. Р. Шефер // Педагогический журнал Башкортостана. – 2019. №5(84). – С. 22-29.

3. . DeepSeek AI. DeepSeek Technical Report [Электронный ресурс] / DeepSeek AI. – 2024. – Режим доступа: https://github.com/deepseek-ai (дата обращения: 3.02.2026).

4. Белолобова, А. А. Искусственный интеллект в образовании: проблема его недобросовестного использования обучающимися / А. А. Белолобова // Инженерное образование. – 2025. - №37. – С. 86-98. – DOI 10.54835/18102883_2025_37_8.

5. Москалевич, Р. Д. Применение нейросетей в обучении физике/ Р. Д. Москалевич, П. А. Хорошевич // Физико-математическое образование: традиции, инновации, перспективы: Материалы Международной научно-практической конференции, Минск, 26-27 октября 2023 года. – Минск: Учреждение образования «Белорусский государственный педагогический университет имени Максима Танка», 2023. – С. 149-151.

6. Сайфутдинова, Г. С. Использование нейросетей в обучении физике: польза или вред / Г. С. Сайфутдинова, С. Р. Оразова, К. А. Таращанский //Наука, образование, транспорт: актуальные вопросы, приоритеты, векторы взаимодействия: Материалы II Международной научно-методической конференции. В 3-х частях, Оренбург, 08-09 ноября 2023 года. – Оренбург: Самарский государственный университет путей сообщения, 2023. – С. 95-98.

7. Перова, М. В. Технологии искусственного интеллекта в образовательной сфере / М. В. Перова, М. В. Прокопенко, Е. К. Головкина // Новые научные исследования и разработки: актуальные вопросы, достижения и инновации: Монография. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2025. – С. 6-21.

8. Кирилова, В. В. Нейросети – цифровой помощник для учителя/ В. В. Кириллова // Фундаментальные и прикладные аспекты развития современной науки : Сборник научных статей по материалам XVIII Международной научно-практической конференции, Уфа, 30 сентября 2025 года. – Уфа: ООО «Научно-издательский центр «Вестник науки»», 2025. – С. 46-50.

УДК 681.3+78:378; ГРНТИ 20.01.45

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КУЛЬТУРЕ И ОБРАЗОВАНИИ: ОТ ТЕОРИИ К ПРАКТИКЕ (ЧЕГО НАМ ОЖИДАТЬ И ЧЕГО ОПАСАТЬСЯ)

Э.А. Кадырова, А.В. Севастьянов

Крымский университет культуры искусств и туризма,
Российская Федерация, Республика Крым, Симферополь,
elvira_k2004@mail.ru, spu.crimea@gmail.com

Аннотация. В работе рассматриваются перспективные направления и проблемы внедрения искусственного интеллекта в сферы культуры и образования. Приводится обзор популярных AI-инструментов. Обобщены проблемы их практического освоения основными группами пользователей, возможные риски и перспективы их массового применения.

Ключевые слова: искусственный интеллект (ИИ), нейронные сети, цифровизация культуры, цифровизация образования, электронное обучение (ЭО)

ARTIFICIAL INTELLIGENCE IN CULTURE AND EDUCATION: FROM THEORY TO PRACTICE (WHAT TO EXPECT AND WHAT TO FEAR)

E.A. Kadyrova, A.V. Sevastianov
Crimean University of Culture, Arts and Tourism
Russian Federation, Republic of Crimea, Simferopol
elvira_k2004@mail.ru, spu_crimea@mail.ru

The summary. This paper examines promising areas and challenges in implementing artificial intelligence in culture and education. It provides an overview of popular AI-tools, summarizes the challenges of their practical adoption by key user groups, and discusses the potential risks and prospects of their widespread use.
Keywords: artificial intelligence (AI), neural networks, digitalization of culture, digitalization of education, e-learning (EL*)*

Введение

Разработка и внедрение технологий искусственного интеллекта (ИИ) в различные сферы деятельности является одним из главных трендов современного развития. Уже в ближайшей перспективе по прогнозам исследователей ИИ не только сравняется с интеллектом человека, но и превзойдет его. Достигнув определенного уровня, ИИ и нейросети смогут совершенствовать сами себя, без участия разработчиков. Накопленный опыт применения систем и технологий ИИ в сфере культуры и образования свидетельствует о все возрастающем интересе со стороны пользователей. ИИ продолжает интегрироваться в область искусства, предлагая новые возможности для творчества и расширяя его границы. Вместе с тем, исследователи и эксперты отмечают, что потенциал его использования в рассматриваемых сферах еще не до конца изучен, а вопросы легализации и изучения условий интеграции инструментов и программных решений ИИ до сих пор остаются дискуссионными [4; 7; 9; 15; 17]. Возрастающие возможности ИИ и нейросетей способствуют заметной трансформации традиционных моделей культурного и образовательного процессов, но они содержат также определенные риски и угрозы для их последующего развития. Масштабность распространения технологий ИИ в различных сферах с последующим активным освоением и практическим применением делает их предметом изучения для целого ряда научных дисциплин. Анализ теоретических работ и практических примеров использования ИИ и нейросетей в рассматриваемых областях позволяет выявить имеющиеся ключевые тенденции и противоречия.

Определение понятий

ИИ – одна из самых обсуждаемых в современных публикациях IT-областей; разрабатываемые здесь алгоритмы и модели позволяют компьютерам выполнять задачи, которые традиционно считались прерогативой интеллекта человека. При этом усилия разработчиков направлены на создание компьютерных программ/устройств и интеллектуальных систем, которые работают с имитацией когнитивных функций человека, в т. ч., мышления, творчества и т. д. Современные системы ИИ уже во многом превосходят возможности человека, реализуя недоступные ему сложнейшие операции, несопоставимые по скорости обработки данных, масштабу анализа информации и способности работать непрерывно.

Существует множество трактовок понятия «искусственный интеллект», среди которых в качестве рабочего определения в контексте данной статьи, приведем следующее: «*искусственный интеллект (ИИ) – алгоритмы, которые имеют способность самообучаться, чтобы применять полученные знания для достижения поставленных человеком целей*» [20]. В отечественных источниках термин «искусственный интеллект» часто заменяют аббревиатурой AI, как сокращение его английского эквивалента *Artificial Intelligence.* В профессиональной среде оба обозначения - ИИ и AI - считаются равнозначными и используются параллельно. Также, как синонимы часто используются термины «искусственный ин-

теллект» и «нейросети», однако понимание их различия критически важно как для разработчиков, так и для пользователей. Сопоставляя содержание данных терминов, отметим, что *искусственный интеллект представляет собой обширную область, включающую множество подходов и методов*, в то время как *нейронные сети - это мощный, но специфический инструмент в этом наборе*. Для построения действительно эффективных ИИ-систем необходимо владеть всем спектром доступных технологий и уметь выбирать оптимальное решение для каждой конкретной задачи (рисунок 1). Профессионалы, которые выходят за рамки «нейросетевого мышления» и осваивают весь арсенал ИИ, получают значительное преимущество на рынке и способны создавать более гибкие, эффективные и устойчивые решения.



Рис. 1. Классификация методов ИИ

В условиях реализации проектов цифровой трансформации общества ИИ играет все более важную роль во всех сферах жизни. В Российской Федерации - это один из самых значимых проектов программы «Цифровая экономика». В 2020 году стартовал федеральный проект «Искусственный интеллект», основной целью которого является создание условий для организаций и граждан России использовать преимущественно отечественные технологии ИИ [19]. В отраслевом разрезе наблюдаются существенные различия в активности внедрения ИИ: пока одни организации и компании успешно их используют, другие лишь начинают эксперименты по их применению [1]. Последние достижения стали возможны благодаря росту вычислительных мощностей и усовершенствованию методов обработки данных. Характерно, что многие передовые разработки искусственного интеллекта проникли в общие приложения, часто не называясь искусственным интеллектом. На практике ИИ чаще всего функционирует в фоновом режиме, повышая удобство, точность и персонализацию сервисов, не требуя от пользователей специальных знаний или дополнительных действий.

В настоящее время технологии ИИ являются важнейшим направлением, обеспечивающими эффективность и действенность процессов цифровизации, которые охватывают различные сферы жизни и деятельности современного общества, в том числе, отрасли культуры и образования. В контексте рассматриваемой проблематики термин «цифровизация» трактуется не просто отказ от бумажных носителей и дигитализация (англ.: digitalization), или оцифровка, но как *комплексный подход к внедрению современных цифровых технологий, в том числе ИИ.* На фоне стремительного развития ИИ как в мире, так и в России, всё более

актуальным становится вопрос практического применения этих технологий в рассматриваемых отраслях.

Обзор популярных инструментов ИИ для сферы культуры

Как и другие отрасли, в эпоху цифровых технологий сфера культуры и искусства, воспринимает передовые нововведения, более того, генерирует их. Применение систем и технологий ИИ – неизбежный процесс, создающий новая форму цифрового искусства (**ИИ-искусство**) как видимый результат, преобразующий и наполняющий данную сферу новыми смыслами, расширяющий границы понятия креативности и того, как может создаваться современное искусство вообще. По мнению куратора годового он-лайн курса «Арт-менеджмент в современном искусстве» А. Лисовской, «ИИ-искусство - это коллаборация креативщика (художника) и ИИ-системы, однако, уровень участия художника может сильно варьироваться, влияя на результат и качество произведения [18].

С конца 1950-х годов на заре компьютерного искусства визуальные художники (например, Манфред Мор - Германия, Вера Мольнар - Венгрия), проводили свои первые эксперименты с компьютерной графикой. Попытки разработать набор алгоритмов для создания визуальных образов с применением компьютерных технологий осуществляли Фридер Наке (Германия) в 1967 году, Гарольд Коэн (Великобритания) в 1973 году, и другие специалисты. В последнее время в сфере ИИ-искусства наметился прорыв, благодаря появившимся возможностям оперативно обрабатывать большие массивы данных и разрабатывать новые алгоритмы. Первое творческое применение нейросети *GAN* состоялось в 2015 году сотрудником Google Александром Мордвинцевым при изучении вопроса о том, как машины обучаются на визуальных образах (фотографиях, картинах художников). Публикация Google исходного кода алгоритма и возрастающая доступность открытых хранилищ изображений позволили художникам генерировать новые визуальные образы на уже натренированных нейросетях.

ИИ может помочь в сохранении и восстановлении произведений искусства; например, алгоритмы машинного обучения могут использованы для восстановления поврежденных или утраченных частей художественного произведения, а также для улучшения качества изображений и видео.

Компания OpenAI (США, https://openai.com), которая разрабатывает и лицензирует технологии на основе машинного обучения, в 2021 году представила нейросеть DALL-E, предназначенная для создания изображений по их текстовому описанию. Связь между смысловым значением текста и визуальным представлением обеспечивает модель CLIP. На ее основе осуществляется анализ релевантности изображений и фрагментов текста в процессе обучения на огромном массиве изображений и связанных с ним описаний.

Одной из самых популярных платформ в 2022 году, стала нейросеть Midjourney (Разработчик: Лаборатория MidJourney; https://www.midjourney.com/), на базе которой возможно создание реалистичных изображений. Midjourney работает по приглашению через Discord и использует модель Clip, где методы генерации изображений постоянно меняются. Бесплатно пользователям доступно 25 условных gpu-минут работы нейросети в месяц. Отметим, что платные подписки для РФ временно недоступны.

Нейронная сеть, выпущенная командой SberDevices и Sber AI при содействии SberCloud, входящей в экосистему Сбера (Центр исследований и разработки Сбера, г. Санкт-Петербург, https://developers.sber.ru/), генерирует изображения на основе текстового описания на русском языке. Работает через бот в Discord, также было выпущено приложение «Салют», где можно также создавать изображения по голосовому запросу.

Первые проекты, обеспечившие интеграцию ИИ и **музыкального творчества**, предоставили музыкантам и продюсерам безграничную палитру звуков, стилей и новых возможностей. ИИ-технологии в музыке позволяют создавать уникальные, сложные композиции с невиданной ранее скоростью и относительной легкостью. ИИ-музыка - сфера сочине-

ния музыки на основе систем искусственного интеллекта, а также разработка цифровых платформ, позволяющих использовать ИИ для создания музыкальных произведений. Изначально такие специализированные программы обучаются на больших массивах музыкальных баз данных, включающих партитуры и аудиозаписи множества произведений. Затем алгоритмы программы анализируют структуру, гармонию, мелодию и ритм произведений, что позволяет генерировать новые композиции в заданном стиле [11].

Известно, что российский исследователь Рудольф Зарипов еще в 1960 году опубликовал первую в мире статью об алгоритмическом сочинении музыки с использованием компьютера «Урал-1». В 1965 году Рэймонд Курцвейл (США) разработал программное обеспечение, способное распознавать музыкальные закономерности и синтезировать на их основе новые композиции. Уже в 1997 году программа ИИ под названием «Эксперименты в музыкальном интеллекте» (EMI) превзошла человека-композитора в задаче сочинения музыкального произведения, имитирующего стиль Иоганна Себастьяна Баха. В 2002 году группа музыкальных исследований в Лаборатории компьютерных наук *Sony* в Париже под руководством французского композитора и учёного Франсуа Паше разработала алгоритм *Continuator*, представляющий собой уникальный способ возобновлять композицию после остановки живого музыканта.

По оценкам специалистов, для многих музыкантов использование ИИ может показаться излишне механистичным или даже угрозой для аутентичности классической музыки. Важно понимать, что ИИ не заменяет живого композитора или исполнителя, а служит инструментом, расширяющим их возможности. Так, например, ИИ может предложить новые гармонические решения, варианты оркестровки и др., и это не означает, что машина создает музыку вместо человека; напротив, она помогает раскрыть новые грани творчества, которые ранее могли быть недоступны [11]. Важным преимуществом использования ИИ-систем в музыке является возможность быстрого прототипирования идей и экспериментов с различными музыкальными стилями, что особенно полезно для композиторов, работающих в условиях ограниченного времени, например, при создании музыки для кино или театра. ИИ может предложить несколько вариантов аранжировки или композиции, из которых композитор выберет наиболее подходящий, и это позволяет ускорить процесс создания произведений. Кроме того, ИИ-системы, способные анализировать и воспроизводить различные музыкальные жанры, могут служить обучающим средством для музыкантов и композиторов, желающих освоить различные стили и техники.

Искусственный интеллект совершает прорывы в области музыкального сочинительства. Одними из самых известных музыкальных ИИ-платформ являются *OpenAI MusNet* (разработчик американская научно-исследовательская организация OpenAI) и *AIVA* (Artificial Intelligence Virtual Artist). Использование этих программ открывает невероятные возможности для воссоздания или продолжения творческого наследия композиторов, чьи произведения остались по разным причинам незавершенными.

Разработка компании OpenAI – нейронная сеть *MuseNet* (https://openai.com/index/musenet), использует ту же универсальную технологию обучения без учителя, что и GPT-2 и способна генерировать четырехминутные музыкальные композиции с использованием десяти различных инструментов и сочетать разнообразные музыкальные стили. OpenAI MuseNet может предсказывать последовательность нот и аккордов, что позволяет имитировать стиль уже написанной части произведения и упрощает работу композиторов, помогая завершать незаконченные работы.

Стартап AIVA Technologies из Люксембурга разработал виртуального композитора *AIVA* (https://www.aiva.ai). AIVA специализируется на создании оркестровой музыки, черпая вдохновение из произведений великих композиторов прошлого. В 2016 году AIVA стал первым в мире виртуальным композитором, получившим признание музыкальной авторской организацией (SACEM). AIVA сочиняет оригинальную классическую музыку, которая исполь-

зуется в фильмах, рекламной индустрии, играх. Альбом "Genesis" демонстрирует симфонические произведения, полностью созданные ИИ, показывая, как ИИ может существенно обогатить музыкальную индустрию (рисунок 2). Бесплатный план AIVA называется Free Forever и создан для тех, кто хочет попробовать возможности платформы без затрат. Платформа поддерживает более двухсот пятидесяти направлений музыки и позволяет скачать результат в форматах MP3, WAV или MIDI. В этом режиме можно создавать музыку исключительно для личного или некоммерческого использования. Авторские права на такие композиции принадлежат компании, поэтому необходимо указывать подпись *«Composed by AIVA (Artificial Intelligence Virtual Artist)»*.

Многочисленные нейросети (*Suno AI, Image to Music, Soundraw, Loudly, Boomy AI, AIVA, Soundful, GigaChat, Beatoven* и другие), разработанные для генерации музыки и доступные на различных сетевых платформах, работают так же, как и любые другие модели машинного обучения. Для получения разнообразных результатов важно, чтобы нейросеть «послушала» как можно больше треков. С их помощью можно создавать фоновую музыку для видео или даже самостоятельные музыкальные композиции. Особенность нейросетей состоит в том, что они не могут создавать принципиально новую музыку, т.е. все сгенерированные композиции будут так или иначе похожи на треки из обучающего массива.



Рис. 2. Нейросеть для генерации музыки *AIVA (Artificial Intelligence Virtual Artist)*

Обзоры популярных нейросетей для генерации музыки представлены в публикациях сети Интернет [23; 24]. Как отмечают авторы, у музыкальных нейросетей (бесплатных и коммерческих) есть существенные различия в способах генерации. В частности, к настоящему времени известны два способа создания треков: генерация нот и генерация звуков. Для создания песни проще всего сгенерировать ноты, а после исполнить их на виртуальных музыкальных инструментах. Такой способ требует меньше вычислительных ресурсов и быстрее создаёт музыку. Но у него есть и недостатки, например, на его основе нельзя сгенерировать голос или изобрести новое звучание. Для генерации звуков нейросеть создаёт сразу аудиосигнал, минуя нотную запись. В таком случае у модели машинного обучения нет ограничений на звучание: можно создавать вокал, звуки окружения и эффекты. При этом нейросети требуется больше вычислительных ресурсов и запуск на домашнем компьютере практически невозможен.

Правовые аспекты использования ИИ и нейросетей в музыкальном творчестве становятся предметом разработки в области современного права. Как отмечают эксперты [24], перед выбором ИИ-сервиса для генерации музыки важно проверить, что сгенерирован-

ные композиции можно использовать на сторонних площадках. На большинстве популярных площадок права на созданные треки можно получить, если оформить платную подписку. В соответствии с законодательством РФ об авторском праве, автором музыкального произведения считается человек, творческим трудом которого это произведение создано. Считается, что если пользователь нейросети только задаёт общие параметры будущей композиции, выбирая из предложенных программой опций, то его творческий вклад в создание композиции отсутствует.

Композиции, сгенерированные нейросетями без участия человека, на данный момент не охраняются авторским правом. Но, поскольку нейросети обучаются на чужих произведениях, использовать такие композиции можно только в личных целях. В других случаях, особенно в случае коммерческого использования, авторы произведений, на которых обучалась нейросеть, могут предъявлять претензии. Авторы или их наследники могут запрещать использование композиций и требовать выплаты денежной компенсации. Эти правила не касаются произведений, перешедших в общественное достояние. Вместе с тем, иногда сами авторы позволяют широко использовать свои произведения, публикуя их под открытой лицензией (по типу Creative Commons). В таком случае, чтобы избежать претензий, пользователю достаточно соблюдать условия открытой лицензии. Если владелец нейросети выкупил авторские права на произведения, на которых обучается нейросеть, то нужно убедиться, что он не запрещает использовать сгенерированную музыку в различных, в том числе коммерческих, целях [24].

Еще одной областью применения ИИ в культуре является **киноиндустрия**. Алгоритмы машинного обучения помогают режиссерам и продюсерам решать сложные задачи, связанные с монтажом, спецэффектами, написанием сценариев и др. Программы на основе ИИ способны анализировать видеоматериалы, предлагать лучшие варианты монтажных решений, что ускоряет процесс постпродакшена, позволяет глубже сосредоточиться на творческих аспектах. ИИ способен создавать реалистичные визуальные эффекты, которые ранее требовали огромных затрат времени и ресурсов. Разрабатываются системы, которые могут генерировать оригинальные сценарии на основе существующих данных. Естественно, ИИ не заменит талантливого сценариста; он может стать мощным инструментом для вдохновения, помощи в поиске новых идей. Так, например, фильм «Zone Out» (2021 г., режиссер Логан Киши) был частично создан с использованием ИИ, который помогал в разработке сценария, диалогов и реплик персонажей, а также создании графических эффектов, оптимизации монтажа [10].

В настоящее время существует целый ряд популярных программ и сервисов для создания и редактирования **видео** с использованием искусственного интеллекта. Рассмотри некоторые из них:

- *Runway ML* (https://runwayml.com) - платформа, которая поддерживает такие функции, как генерация видео, изменение скорости, цветокоррекция и др.
- *DeepMind's VideoSpace* (https://speos-photo.com) - технология, которая позволяет генерировать видео из последовательности изображений, может быть полезна для создания сложной анимации и спецэффектов.
- *Nvidia Broadcast* (https://www.nvidia.com) - программное обеспечение, которое использует ИИ для улучшения качества видеоконференций на основе реализации ряда функций (удаление фона, улучшение освещения, добавление анимации, и др.).
- *OpenCV* - Open Source Computer Vision Library (https://github.com/opencv/opencv) - библиотека с открытым исходным кодом, которая используется для анализа и обработки видео и поддерживает широкий спектр функций, включая распознавание лиц, отслеживание объектов и др.

Как видим, ИИ в современной культуре существенно изменяет способы создания и потребления художественного контента, предлагая пользователям новые способы и инстру-

менты для творчества и взаимодействия с аудиторией, открывая возможности для поиска новых идей и экспериментов. Несмотря на все сомнения и риски, ИИ является прогрессивным инструментом, который переопределяет деятельность представителей творческих профессий. Приводимые в пример работы художников, музыкантов демонстрируют нам, что несмотря на дискуссии, которые проводятся вокруг ИИ и его инструментария, этическая и юридическая база, способствующая их переходу в повседневное использование, находится в настоящий момент в стадии становления. Возможность обучать ИИ на разных массивах данных дает беспрецедентные результаты, а значит, и новые сферы применения. Поскольку разрабатываемые алгоритмы все больше влияют на то, как мы воспринимаем современный мир, ключом к построению этики искусственного интеллекта будущего будет отказ от контроля со стороны программистов корпораций и поощрение междисциплинарного диалога с участием представителей творческой сферы. Важно, чтобы ИИ-технологии и сервисы попали в руки художников, у которых есть способность представлять идеи своего времени в направлении формирования и развития всей сферы культуры в позитивном ключе.

Обзор популярных инструментов ИИ для сферы образования

Мировое и Российское образование также вступило в фазу активного освоения искусственного интеллекта. В целях исполнения Законодательства РФ и нормативных документов об искусственном интеллекте Минобрнауки 2 июля 2021 г. направило во все вузы РФ модуль «Системы искусственного интеллекта» для включения его с 1 сентября 2021 г. в образовательные программы по всем специальностям и направлениям подготовки. Цифровая трансформация системы образования, в первую очередь, предполагает оснащение школ и высших учебных заведений современными цифровыми технологиями, которые призваны повысить доступность обучения и обучающих материалов для всех. Цифровая трансформация делает современное образование более доступным, экономичным и содержательным, меняя привычные формы и методы преподавания, расширяя возможности педагогов и обучающихся [22].

В контексте цифровой трансформации общества сфера образования становится одной из масштабных и социально значимых областей для применения ИИ. Искусственный интеллект в образовании - это совокупность технологий и систем, которые имитируют человеческое мышление для решения учебных задач (понимают текст и речь, делают выводы, учатся на опыте, предлагают осознанные решения). В отличие от традиционных образовательных программ с фиксированными сценариями, современные ИИ-инструменты работают гибко, реагируют на запросы в реальном времени, выдают уникальные ответы для разных пользователей. С развитием ИИ-технологий такие решения становятся всё более доступными для учебных заведений и студентов, а значит, персонализированное обучение превращается из единичных кейсов в массовое явление [12].

Использование ИИ и нейросетей в современном образовании охватывает множество направлений: от виртуальных репетиторов, автоматической проверки заданий до создания индивидуальной образовательной траектории для каждого обучающегося. Цифровая трансформация образования под влиянием ИИ носит фундаментальный характер; если ранее технологии использовались для частичной автоматизации рутинных процессов, то в настоящее время они позволяют полностью пересмотреть образовательный процесс.

В теории внедрение нейросетей ведёт к смене парадигмы образования: от единой системы к гибкому и индивидуальному подходу. Преподаватель освобождается от рутинных задач (проверки заданий, составления тестов), получает больше времени на творческую работу, на прямое взаимодействие с обучающимися. Студенты перестают быть пассивными слушателями, становятся центром образовательной системы, получая контент и задания, соответствующие их индивидуальным потребностям, ритму обучения и скорости восприятия [7; 9; 12].

Одним из преимуществ использования ИИ в образовании специалисты считают возможность формирования моделей адаптивного обучения, на основе динамического выстраивания индивидуальной образовательной траектории. Анализ данных о степени подготовленности, способностях, цели, мотивации, других характеристиках обучающегося позволяет ИИ-системе составить персонализированный учебный план, включающий контент, ориентированный на его интересы и потребности. Оперативная доступность в режиме 24/7 в формате виртуальных ассистентов и чат-ботов/*chatbot* (рисунок 3), предоставляющих помощь в момент, когда возникают вопросы, что особенно важно для систем электронного обучения, – ещё одно из преимуществ ИИ [16]. Разрабатываемые интеллектуальные обучающие системы (*intelligent learning system*), симулирующие поведение учителя, решают задачи по проверке уровня знаний обучающихся, анализируют их ответы, составляют отзывы. Современные системы способны проверять не только тесты с выбором ответа, но и более сложные тестовые задания, включая эссе. Здесь используются алгоритмы на основе технологии NLP (позволяющей компьютерам интерпретировать и понимать человеческий язык, а также использовать его в различных целях), которые анализируют текст, определяют его структуру, логику, стиль и содержание [12].

Адаптивные ИИ-системы объединяет общий принцип работы: после стартового тестирования они подбирают для пользователя подходящие по сложности задания. В ходе обучения система осуществляет анализ результатов и ошибок, адаптируя дальнейшую стратегию обучения так, чтобы восполнить пробелы в знаниях обучающегося и повысить их уровень.

В целом, прогнозная аналитика – мощный инструмент, который даёт использование ИИ в образовании. Алгоритмы машинного обучения обрабатывают большие массивы данных об академической успеваемости, посещаемости, социальных условиях учащихся и проч., выявляя закономерности и тенденции. Такой анализ позволяет не только оценивать текущие результаты, но и предотвращать негативные сценарии в будущем. Системы на базе ИИ могут определять риски отчисления студентов, их неуспеваемости по тем или иным учебным дисциплинам. На глобальном уровне подобная аналитика помогает совершенствовать реализуемые в вузе образовательные программы [12; 16] .

Генеративный ИИ открывает для преподавателя новые возможности в создании обучающих материалов (генерация текстов лекций, сценариев для видео, иллюстраций, инфографики, тестовых вопросов, презентаций), что особенно важно, когда обучающий курс нужно подготовить в сжатые сроки. С появлением генеративных моделей упростился процесс создания виртуальных симуляций и тренажёров. Нейросети могут генерировать видео с виртуальными персонажами, придумывать реалистичные диалоги и сценарии, близкие к реальным рабочим ситуациям.

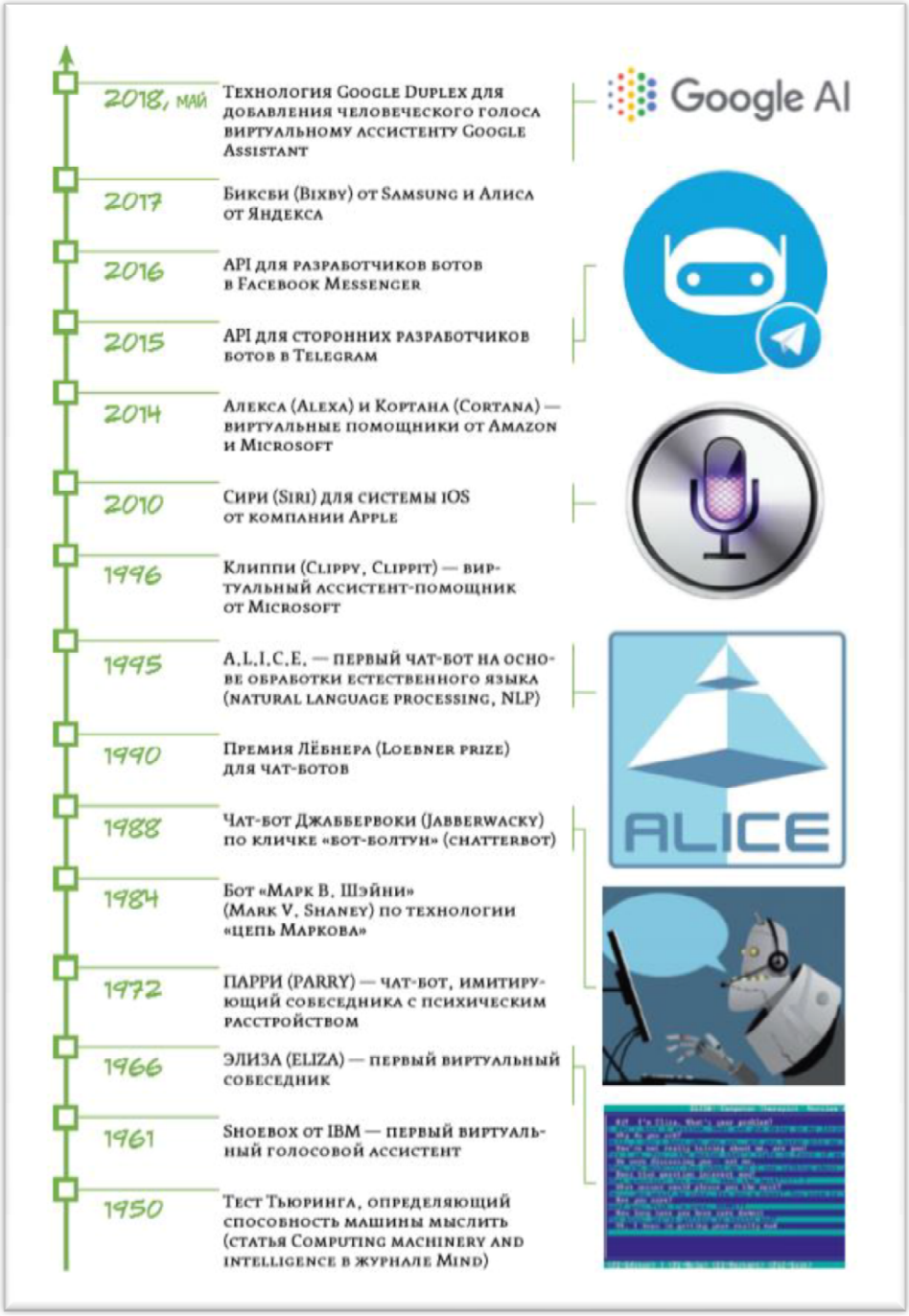


Рис. 3. Эволюция chatbot-технологий

Ниже рассмотрим примеры популярных ИИ-сервисов, ориентированных на практическое применение в сфере образования.

Адаптивные ИИ-системы

Duolingo (https://www.duolingo.com/) – платформа, оптимизирующая подбор заданий на основе огромного числа анонимных данных от пользователей. Например, если обучающийся совершает постоянно повторяющиеся ошибки при выполнении определённого типа заданий, система может не только предложить дополнительные задания, но и временно по-

низить их сложность, а также применить технику интервального повторения, чтобы помочь закрепить базовые знания.

Thinkster Math (https://www.hellothinkster.com/) - сервис сочетает в себе возможности ИИ и живого репетитора; здесь отслеживается не только правильность ответа, но и вся логика решения: какие действия предпринял обучаемый, сколько времени потратил на каждый этап, где именно допустил ошибки. На основе этих данных ИИ строит «карту мышления», выявляя слабые стороны, после чего репетитор, работая с учеником вживую, помогает устранить выявленные пробелы.

«*Учи.ру*» (https://uchi.ru/) – российская платформа «Учи.ру», которая применяет элементы адаптивного обучения, предлагая школьникам индивидуальные сценарии обучения. Система в реальном времени отслеживает прогресс каждого ученика: количество правильных и неправильных ответов, затраченное время, повторяющиеся ошибки; успешное прохождение открывает доступ к более сложным заданиям. Учебный процесс постоянно находится под контролем нейросети, которая гибко подстраивает его под потребности конкретного пользователя.

Системы проверки эссе и сочинений с обратной связью

Gradescope (https://www.gradescope.com/). Принцип работы: преподаватель загружает в систему задания и правильные ответы, затем сканирует работы студентов. ИИ распознаёт рукописный текст, группирует типичные ошибки, предоставляет аналитику результатов, что позволяет преподавателю дать целенаправленную обратную связь.

DeepSeek (https://chat.deepseek.com/) и *ChatGPT* (https://chatgpt.ru) - универсальные нейросети, которые достаточно активно используются в сфере образования. Студент может отправить написанный текст на проверку с запросом: «Найди ошибки и объясни их», на основании чего нейросеть укажет на недочёты, пояснит, как сделать правильно.

Виртуальные ассистенты и чат-боты

Gemini (https://gemini.google.com) – универсальная нейросеть работает по принципу ChatGPT, способная одновременно обрабатывать и понимать информацию разных типов: текст, изображения и аудио. Gemini может объяснять сложные темы простыми словами, создавать конспекты объёмных источников, писать тексты в разных стилях, генерировать идеи для проектов.

Kampus AI (https://kampus.ai/) - специализированная образовательная платформа, созданная для помощи студентам в решении широкого спектра учебных задач. Ключевое отличие ее от универсальных нейросетей - глубокое понимание академических требований и процессов. Kampus AI помогает писать рефераты, курсовые и дипломные проекты и др. Система не только генерирует текст, но и проверяет факты по источникам, обеспечивает высокую уникальность, автоматически оформляет работу в соответствии с требованиями ГОСТ. Для максимального удобства сервис доступен в виде чат-бота в Telegram, что позволяет пользоваться им с телефона в любой момент.

По мере практического внедрения ИИ и нейросетей в образовательный процесс обнаруживаются не только их **преимущества**, но и определённые риски. Среди явных преимуществ отметим такие, как: 1) экономия времени преподавателя**,** увеличение возможностей для творческой работы и продуктивного общения со студентами, в силу того, что ИИ автоматизирует рутинные операции (проверку домашних заданий, составление тестов, отчётность и проч.); 2) оперативный доступ к знаниям и постоянная поддержка - универсальные нейросети, такие как GigaChat, ChatGPT, выступают в роли единого ключа к огромному массиву информации, предоставляя помощь в режиме 24/7; 3) объективность, непредвзятость оценки, снижение субъективных факторов в оценивании.

Ключевые риски практического внедрения ИИ в образовательный процесс: 1) проблемы конфиденциальности данных (ИИ-системы обрабатывают огромные массивы персональной информации, как следствие возникает вопрос её надёжного хранения, защиты от утечек); 2) «обезличивание» обучения и дефицит живого общения, сокращение прямого взаимодействия студентов с преподавателями и одногруппниками, что ведёт к социальной изоляции; 3) риск списывания и возникающей зависимости от технологий (студенты часто используют нейросети не в качестве помощника, а для получения готовых ответов, что тормозит развитие их самостоятельности и критического мышления); 4) возможные ошибки нейросети (ИИ не всегда даёт точные ответы, может «придумывать» факты, особенно если не находит нужной информации в своей базе знаний, в силу чего контент все еще требует проверки фактической точности).

Выводы

Технологии ИИ, становясь в современной культуре неотъемлемой частью творческого процесса, открывают новые возможности для креативности, делая произведения искусства более доступными для массовой аудитории. Анализ примеров практического применения популярных нейросетей, подтверждает, что ИИ способен создавать оригинальные работы, но их ценность остается предметом многочисленных обсуждений и дискуссий. Обнаруживается, что пользователи довольно активно интересуется ИИ-генераторами, что свидетельствует об их растущем влиянии на культуру современного общества. Однако выявляются и значительные риски, такие как потеря уникальности художественных произведений, перенасыщение арт-рынка, проблемы с соблюдением и защитой авторских прав.

Использование ИИ и нейросетей требует осознанного подхода, направленного на сохранение уникальности человеческого видения и мастерства. В связи с этим, будущее искусства, вероятно, будет определяться дальнейшим сотрудничеством человека и машины, где искусственный интеллект будет выступать в роли партнера, расширяющего границы возможного. Наряду с совершенствованием технологии предстоит разработка этических и правовых норм, которые позволят максимально использовать потенциал ИИ, избегая при этом негативных последствий для творчества личности и культуры в целом.

Одновременно развитие ИИ нейросетей в контексте образования видится также в создании гармоничного симбиоза человека и машины. В этой сфере можно ожидать развития следующих тенденций.

Глубокая адаптация под интересы и потребности студентов. Персонализация и адаптивное обучение затронут не только содержание, но и форматы подачи учебной информации, которые будут учитывать когнитивные особенности и стиль восприятия каждого обучаемого.

ИИ как неотъемлемая часть учебного процесса. Имеющие место запреты на использование нейросетей студентами будут сменяться политикой их грамотного применения в ходе их интеграции в учебный процесс. Важной составляющей информационной культуры студентов видится умение критически оценивать получаемые ответы ИИ, использовать нейросети для выполнения рутинной работы и мозгового штурма, а не для банального списывания.

Распространение иммерсивного обучения. Согласно исследованиям, эффективность обучения в виртуальной реальности естественно-научным дисциплинам уже сегодня на 76% выше, чем при использовании традиционных методов. VR/AR-технологии (VR погружает пользователя в виртуальный мир, AR добавляет цифровые элементы в существующую реальность) в привязке с ИИ будут стандартом для безопасного проведения сложных экспериментов по химии, физике, биологии, отработки практических навыков в медицине и других отраслях.

Развитие «мягких» навыков (soft skills) у преподавателей. Роль преподавателя все больше смещается от источника передачи знаний к роли наставника, который развивает у обучаемых коммуникацию, креативность, критическое мышление, т.е. те навыки, где ИИ пока не может соперничать с человеком.

Как видим, искусственный интеллект - не будущее, а уже настоящее для сферы культуры и образования - открывает новые возможности для творчества, развития и познания. Главная задача на ближайшие годы - научиться использовать этот мощный инструмент разумно, внедрять его в практическую деятельность так, чтобы данная технология служила человеку, но не заменила его.

Библиографический список

1. Абашкин В. Л., Ковалёва Г. Г. Распространение искусственного интеллекта в отраслях экономики и социальной сферы. - М.: ИСИЭЗ НИУ ВШЭ, 2025: [Электронный ресурс]. – Режим доступа: https://issek.hse.ru/news/1091369132.html.

2. Авачева Т.Г., Кадырова Э.А. Искусственный интеллект в медицине как объект разработки и обучения в медицинском университете // Современные технологии в науке и образовании - СТНО-2020 / Сб. трудов III Международн. научно-технического форума. В 10-ти томах. Том 9. /Под общей редакцией О.В. Миловзорова, 2020. - С. 47-53

3. Баррат Дж. Последнее изобретение человечества: Искусственный интеллект и конец эры Homo sapiens / Джеймс Барра ; Пер. с англ. - М.: Альпина нон-фикшн, 2015. - 304 с.

4. Бекиров С.Н. Социально-философские проблемы внедрения в высшее образование искусственного интеллекта и искусственной жизни // Проблемы современного педагогического образования. – 2022. - № 77 (2). – С.49-52 : [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sotsialno-filosofskie- problemy-vnedreniya-v-vysshee-obrazovanie-iskusstvennogo-intellekta-i-iskusstvennoy-zhizni (дата обращения 03.04.2026)

5. Бруссард М. Искусственный интеллект: Пределы возможного / Мередит Бруссард; Пер. с англ. - М. : Альпина нон-фикшн, 2020. - 362 с.

6. Буякова К.И., Дмитриев Я.А., Иванова А.С., Фещенко А.В., Яковлева К.И. Отношение студентов и преподавателей к использованию инструментов с искусственным интеллектом в вузе. // Образование и наука. -2024. - №26(7). – С. 160–193

7. Вовк Е. В., Супрун А. А. Искусственный интеллект и цифровая педагогика как тренд современной образовательной среды высших учебных заведений // Проблемы современного педагогического образования. - 2022. - № 77-2. – С.84-86

8. Григорьева П.А., Гаев Л.В. Культурное влияние искусственного интеллекта // Международный журнал гуманитарных и естественных наук. – 2024. - №6-4 (93).- С. 41-43: [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kulturnoe-vliyanie-iskusstvennogo-intellekta (дата обращения 03.04.2026)

9. Даггэн С. Искусственный интеллект в образовании: изменение темпов обучения. Аналитическая записка ИИТО ЮНЕСКО / ред. С. Ю. Князева; пер. с англ.: А. В. Паршакова. - М.: Институт ЮНЕСКО по информационным технологиям в образовании, - 2020 : [Электронный ресурс]. – Режим доступа: https://iite.unesco.org/wp-content/uploads/2020/12/Steven_Duggan_AI-in-Education_2020_RUS.pdf (дата обращения 03.04.2026)

10. Ефимова М. Искусственный интеллект в культуре: как нейросети меняют кино, музыку и дизайн : [Электронный ресурс]. – Режим доступа: https://doersdoings.ru/technologies/iskusstvennyj-intellekt-v-kulture/ (дата обращения 03.04.2026)

11. Искусственный интеллект в современном музыкальном творчестве) : [Электронный ресурс]. – Режим доступа: https://www.classicalmusicnews.ru/articles/artificial-ntelligence-in-modern-musical-creativity/ (дата обращения 07.04.2026)

12. Искусственный интеллект в образовании: как использовать нейросети для учебы и преподавания /А. Дербина // Chad AI: Блог о нейросетях : [Электронный ресурс]. – Режим доступа: https://blog.chadgpt.ru/ii-v-obrazovanii/ (дата обращения 09.04.2026)

13. Искусственный интеллект - надежды и опасения: [сборник: перевод с английского В. Желнинова] /под ред. Джона Брокмана. - М.: Издательство АСТ, 2020. - 384 с.

14. Кондратов А. Электронный разум. Очерк исследований по проблеме искусственного интеллекта. – М.: Знание, 1987. - 186 с.

15. Константинова Л.В., Ворожихин В.В., Петров А.М., Титова Е.С., Штыхно Д.А. Генеративный искусственный интеллект в образовании: дискуссии и прогнозы // Открытое образование. - 2023. - № 27 (2). – С. 36-48

16. Краснова Г.А., Можаева Г.В. Электронное образование в эпоху цифровой трансформации: научное издание. – Томск: Издательский Дом Томского государственного университета, 2019. – 200 с.

17. Курбанова З. С., Исмаилова Н. П. Нейросети в контексте цифровизации образования и науки // Мир науки, культуры, образования. - 2023. - № 3 (100). – С.307-309

18. Лекун, Я. Как учится машина: революция в области нейронных сетей и глубокого обучения: перевод с фр. / Я. Лекун. - Москва: Альпина ПРО, 2021. - 335 с.

19. Лисовская А. Как искусственный интеллект трансформирует современное искусство : [Электронный ресурс]. – Режим доступа: https://msca.ru/blog/articles/kak-iskusstvennyy-intellekt-transformiruet-sovremennoe-iskusstvo (дата обращения 07.04.2026)

20. Лукинов В.А., Соколов Д.А. Роль искусственного интеллекта в цифровой трансформации современной России // Научное обозрение. Технические науки. - 2023.- № 2. - С. 38-43 : [Электронный ресурс]. – Режим доступа: https://science-engineering.ru/ru/article/view?id=1432 (дата обращения: 06.04.2026).

21. Морковкин Е.А., Новичихина А.А., Замулин И.С. Искусственный интеллект как инструмент современного искусства // Вестник ХГУ им. Н.Ф. Катанова. 2021. - №1(35). – С.55-59

22. Стратегия цифровой трансформации отрасли науки и высшего образования (утв. Минобрнауки России) : [Электронный ресурс]. – Режим доступа: http://www.consultant.ru//spa.msu.ru/wp-content/uploads (дата обращения 03.04.2026)

23. Топ-10 нейросетей для написания песен и генерации музыки : [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/bothub/articles/960084 (дата обращения 08.04.2026)

24. Топ-11 нейросетей для создания музыки : [Электронный ресурс]. – Режим доступа: https://skillbox.ru/media/code/top8-neyrosetey-dlya-sozdaniya-muzyki (дата обращения 08.04.2026)

25. Широколобова А. Г. Искусственный интеллект как инструмент оптимизации работы преподавателя высшей школы // Педагогика. Вопросы теории и практики. – 2024.Том 9. Вып. 2. : https://pedagogy-journal.ru/en/article/ped20240018/fulltext (дата обращения 03.04.2026)

СЕКЦИЯ «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ЗАЩИТА ИНФОРМАЦИИ»

УДК 004.056.3; ГРНТИ 50.41.23

ИССЛЕДОВАНИЕ МЕТОДОВ ВОССТАНОВЛЕНИЯ УДАЛЕННЫХ И ПОВРЕЖДЕННЫХ ДАННЫХ В РАЗЛИЧНЫХ ФАЙЛОВЫХ СИСТЕМАХ

А.С. Стенин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, antonstenin53330@gmail.com

Аннотация. Восстановление удаленных данных – ключевая тема этого исследования. Рассмотрены методы восстановления данных для файловых систем FAT32 и NTFS. Проанализирована их архитектура. Сильными сторонами FAT32 являются кроссплатформенность и простота структуры, что упрощает восстановление при сохранности таблицы размещения файлов. NTFS выделяется высокой надёжностью благодаря журналированию, избыточности метаданных и поддержке сложных атрибутов безопасности. Слабыми сторонами FAT32 признаны уязвимость к фрагментации, отсутствие журнала транзакций, что может привести к потери данных при повреждении ключевых структур. Для NTFS характерны сложность структуры, ограниченная совместимость с другими операционными системами, в ней обеспечивается целостность метаданных, а не пользовательских данных. Основными принципами восстановления для FAT32 являются реконструкция цепочек кластеров через таблицу размещения и сканирование по сигнатурам. Для NTFS: анализ и восстановление записей главной файловой таблицы, а также использование журнальных структур для реконструкции событий файловой системы. Также было проведено сравнение предложенных решений. Критериями послужили: эффективность работы при незначительных и серьёзных повреждениях, возможность восстановить структуру каталогов и метаданные, а также требования, которые решения предъявляют к системным ресурсам.

Ключевые слова: файловая система, NTFS, FAT32, файловые таблицы, журналирование изменений.

STUDYING METHODS TO RECOVER DELETED AND CORRUPTED DATA IN VARIOUS FILES

A.S. Stenin

Ryazan State Radio Engineering University, Russia, Ryazan, antonstenin53330@gmail.com

Abstract. Recovery of deleted data is the key topic of this study. Methods of data recovery for FAT32 and NTFS file systems are considered. Analyzed their architecture. The strong points of FAT32 are cross-platform and simple structure, which makes it easier to recover while preserving the file placement table. NTFS stands out for its high reliability due to logging, metadata redundancy and support of complex security attributes. The weaknesses of FAT32 are vulnerability to fragmentation, lack of transaction log, which can lead to data loss when damaging key structures. NTFS has a complex structure, limited compatibility with other operating systems and ensures the integrity of metadata rather than user data. The main principles of recovery for FAT32 are the reconstruction of cluster chains via placement table and signature scanning. For NTFS: analysis and recovery of master file table records, as well as the use of log structures to reconstruct file system events. The proposed solutions were also compared. The criteria were: efficiency of work with minor and serious damage, ability to restore the structure of directories and metadata, as well as requirements that solutions impose on system resources.

Keywords: file system, NTFS, FAT32, file tables, change logging.

Введение

Восстановление удаленных и поврежденных данных, хранящихся в различных файловых системах, является актуальной проблемой, которая в современном мире возникает почти во всех сферах деятельности человека. Внедрение цифровых технологий в различные систе-

мы способствовало переносу данных с бумажных носителей на жесткие диски, которые представляют собой физический накопитель с системой структурного хранения файлов.

Ключевыми концепциями для понимания темы является выбор файловой системы для физического хранилища. При выборе следует обратить внимание на ее надежность, производительность и совместимость. Рассматриваемые файловые системы FAT32 и NTFS имеют архитектурные различия. В первой используется линейная структура таблицы [1], а во второй – сложные базы данных на основе B+-деревьев в NTFS [2]. Недостатки и уязвимости файловых систем напрямую определяют выбор методов и алгоритмов восстановления данных.

В настоящее время для решения задачи восстановления удаленных и поврежденных данных в файловых системах FAT32 и NTFS широко применяется ряд методов.

Анализ существующих методов/решений для файловой системы FAT32

Для системы FAT32 существуют следующие методы: восстановление таблицы размещения файлов (FAT) и сканирование по сигнатурам (file carving). Рассмотрим каждый из методов.

Основной метод восстановления в FAT32 – «Восстановление таблицы размещения файлов» основан на работе с этой таблицей. В этой файловой системе реализован принцип хранения двух копий таблицы размещения файлов. Данный подход позволяет восстановить данные из копии при повреждении основной таблицы [1]. В процессе восстановлении данных выполняются следующие этапы:

1) производится сравнение основной и резервной копий FAT для выявления поврежденных секторов хранилища;

2) переставляются цепочки кластеров на основе анализа данных директорий;

3) восстанавливается структура каталогов через анализ записей директорий.

Эффективность восстановления данным методом зависит от степени фрагментации файлов: чем выше фрагментация, тем сложнее восстановить исходную структуру данных [3], так как обновление вспомогательной таблицы также происходит с каждым изменением исходной таблицы. При журналировании перезаписывается минимум служебной информации. Если изменения слишком велики, то перезапись вспомогательной таблицы будет происходить множество раз, а значит вспомогательная таблица будет хранить промежуточное значение, а не изначальное состояние файла.

Но при серьезных повреждениях FAT следует применять другой метод – «Сканирование по сигнатурам» [4]. Также сама структура FAT позволяет использовать file carving благодаря [1] простой линейной организации данных, минимальному журналированию, прямому доступу к данным. Несмотря на все это, метод сканирования по сигнатуре имеет следующие ограничения: высокая фрагментация на заполненных местах, отсутствие резервирования метаданных, а также ограничение на размер кластера.

В практическом руководстве [4] идеальный сценарий работы алгоритма данного метода: алгоритм восстановления начинается с поиска сигнатуры заголовка файла, затем определяется размер путем анализа структуры соответствующего формата, после чего происходит извлечение непрерывного блока данных до одного из завершающих флагов (искомый футер, конец файла или следующая сигнатура).

Анализ существующих методов/решений для файловой системы NTFS

Рассмотрим следующие методы восстановления данных для файловой системы NTFS: анализ главной файловой таблицы (MFT) и работа с журнальными структурами.

Анализ главной файловой таблицы (MFT). Стоит отметить, что файловая система NTFS использует остаточно сложную структуру на основе MFT. В [2] подробно описана

структура MFT и методы ее анализа. Реализовать восстановление данных можно через поиск в неиспользуемых областях диска, анализ файловых атрибутов (например, $DATA или $FILE_NAME) для реконструкции метаданных, а также использование резервной копии MFT для восстановления поврежденных записей.

MFT содержит достаточно информации для полного восстановления структуры файлов даже при серьезных повреждениях файловой системы [5].

Но если мы хотим использовать ключевую особенность файловой системы NTFS, то можно взаимодействовать с журнальными структурами. Журналирование является ключевой особенностью данной файловой системы. Журнал транзакций ($LogFile) обеспечивает целостность метаданных файловой системы [6]. NTFS предоставляет следующие методы работы с журналом:

1) анализ записей транзакций для восстановления последовательности операций;

2) использование журнала изменений USN ($UsnJrnl) для отслеживания истории изменений файлов;

3) восстановление данных через точки повторной обработки.

Журнальные структуры могут содержать информацию об удаленных файлах, даже если они были удалены из MFT [7].

Сравнительный анализ

Проведя анализ представленных методов, выявлены их сильные и слабые стороны (таблица 1).

Таблица 1. Основные критерии рассматриваемых методов восстановления файлов

Критерий	Восстановление FAT	File Carving для FAT32	Анализ MFT для NTFS	Работа с журнальными структурами NTFS
Эффективность при незначительных повреждениях	Высокая (85-95%) при сохранности резервной копии FAT [1]	Низкая (20-30%) - метод не оптимален для таких случаев [4]	Очень высокая (90-98%) благодаря избыточности MFT [2]	Высокая (80-90%) для метаданных, средняя для данных [6]
Эффективность при серьезных повреждениях	Низкая (10-20%) при повреждении обеих копий FAT [9]	Высокая (70-85%) для форматов с четкими сигнатурами [10]	Средняя (40-60%) - зависит от степени повреждения MFT [5]	Низкая (15-25%) - журналы могут быть повреждены [7]
Восстановление структуры каталогов	Полное восстановление имен и иерархии [1]	Невозможно восстановить имена и структуру [4]	Полное или частичное восстановление структуры [2]	Восстановление через журнал изменений USN [7]
Восстановление метаданных	Полное восстановление атрибутов и времени [3]	Невозможно восстановить метаданные [4]	Полное восстановление метаданных из MFT [3]	Частичное восстановление через журнал транзакций [6]
Требования к ресурсам	Низкие - быстрая обработка [9]	Высокие - полное сканирование носителя [4]	Средние - анализ структуры MFT [5]	Средние - парсинг журналов [6]

Заключение

Многие существующие файловые системы используют различные подходы к работе с данными, а также предусматривают механизмы восстановления удалённых или повреждённых фрагментов. Несмотря на высокие показатели эффективности представленных способов

в рассмотренных файловых системах, ни один из подходов не может гарантировать полное восстановление данных.

Библиографический список

1. Wasim A.B., Quadri S.M.K. Review of FAT Data Structure of FAT32 File System // Oriental Journal of Computer Science & Technology. 2010. № 3. С. 161-164.
2. Касперски К. Файловая системы NTFS извне и изнутри // Системный администратор. 2004. № 11 (24). С. 72-77.
3. Кулаков В. Программирование дисковых подсистем. СПб: Питер, 2002. 762 с.
4. Касперски К., Холмогоров В., Кирилова К. Восстановление данных. СПб: БХВ, 2021. 277 с.
5. Болотов А.С., Болотова Т.П. Файловая система NTFS: обзор версий, производительность // Вестник университета. 2012. № 7. С. 192-197.
6. NTFS Overview // Microsoft Learn. 2025. URL: https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn466522(v=ws.11) (дата обращения: 08.09.2025).
7. Huebner E. et al. Data Hiding in the NTFS File System // Digital Investigation. 2006. № 4. С. 211-226.
8. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. М.: МГТУ им. Н.Э.Баумана, 2009. 652 с.
9. Кудинова А.А., Огар Т.П. Сравнение типов файловых систем для флэш-накопителей: NTFS, FAT32, EXFAT и другие // России - творческую молодёжь. Волгоград: ВГТУ, 2024. С. 98-100.
10. Rusbarsky K.L. A Forensic Comparison of NTFS and FAT32 File Systems // Marshall University Forensic Science Center & Fbi, Heart of America Regional Computer Forensics Laboratory. 2012. № 1. С. 1-29.

УДК 621.317.39.084.2; ГРНТИ 29.35

АРХИТЕКТУРА ИЗОЛИРОВАННОГО СТЕНДА ДЛЯ ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

В.В. Ни, В.А. Мещеряков
Национальный исследовательский Томский государственный университет,
Российская Федерация, Томск, nivladislav350@mail.ru, mva@mail.tsu.ru

Аннотация. В работе рассматриваются принципы построения, логическая и физическая структура испытательных стендов, предназначенных для проведения сертификационных испытаний средств защиты информации (СЗИ) и анализа программного обеспечения (ПО) на соответствие требованиям ФСТЭК России. Особое внимание уделяется вопросам обеспечения изоляции среды, воспроизводимости результатов и автоматизации процессов выявления недекларированных возможностей (НДВ).
Ключевые слова: программное обеспечение, защита информации, фаззинг-тестирование.

ARCHITECTURE OF AN ISOLATED STAND FOR CERTIFICATION TESTING

V.V. Ni, V.A. Meshcheryakov
The National Research Tomsk State University,
Russia, Tomsk, nivladislav350@mail.ru, mva@mail.tsu.ru

The summary. This paper examines the design principles, logical, and physical structure of test rigs designed for certification testing of information security tools (ISS) and software analysis for compliance with FSTEC requirements. Particular attention is paid to ensuring environment isolation, reproducibility of results, and automation of undeclared capability (UDC) identification processes.
Keywords: software, information security, fuzz-testing.

Актуальность создания специализированных стендов обусловлена ужесточением требований регуляторов к безопасности программного обеспечения, используемого на объектах критической информационной инфраструктуры (КИИ). Сертификация СЗИ – это процесс подтверждения того, что продукт действительно выполняет заявленные функции безопасности и не содержит скрытых дефектов или программных закладок.

Стенд для испытаний – это не просто набор компьютеров, а строго регламентированная экосистема, обеспечивающая чистоту эксперимента.

Нормативно-правовая база и требования ФСТЭК

Проектирование архитектуры стенда должно опираться на ледующие документы:

1.Приказ ФСТЭК №55: Положение о системе сертификации средств защиты информации.

2.Приказ ФСТЭК №76: Требования по уровням доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

3.ГОСТ Р 56939-2016: Защита информации. Разработка безопасного программного обеспечения [1].

4.Методические документы ФСТЭК по выявлению НДВ и анализу уязвимостей.

Согласно этим нормам, для высших уровней доверия (1, 2, 3) требуется проведение испытаний в среде, максимально исключающей внешнее влияние и утечку исследуемого кода [2].

Концепция изоляции: Физический и логический уровни

Концепция изоляции является фундаментом при проектировании стенда для сертификационных испытаний средств защиты информации (СЗИ). В отличие от стандартных сред разработки, испытательный стенд должен функционировать как «цифровая крепость», обеспечивая двустороннюю безопасность. Изоляция здесь реализуется на двух взаимосвязанных уровнях – физическом и логическом, и преследует две критические цели.

Первая цель – защита исследуемого объекта. Исходные коды СЗИ и проектная документация представляют собой интеллектуальную собственность высшей ценности, а в ряде случаев – государственную тайну. Архитектура стенда должна исключать любую возможность утечки этих данных. На физическом уровне это достигается принципом «воздушного зазора» – полным отсутствием физических соединений стенда с внешними сетями и интернетом. На логическом уровне внедряются строгие мандатные механизмы контроля доступа, шифрование накопителей и запрет на использование отчуждаемых носителей информации, не прошедших процедуру очистки.

Вторая цель – защита внешней среды. В процессе сертификации ПО подвергается агрессивным воздействиям: динамическому анализу и фаззинг-тестированию. Исследуемый объект может содержать программные закладки или критические уязвимости, которые при активации способны проявить деструктивные свойства – от попыток самораспространения по сети до проведения DoS-атак на инфраструктуру лаборатории. Здесь изоляция выступает в роли «саркофага». Логический уровень защиты обеспечивается использованием гипервизоров и контейнеризации. Каждая итерация теста запускается в изолированной виртуальной среде (песочнице) с жестко ограниченными лимитами ресурсов (CPU, RAM) и имитацией сетевого окружения внутри виртуального коммутатора.

Физический уровень защиты в этом контексте подразумевает размещение серверного оборудования в экранированных шкафах, предотвращающих утечку информации по каналам ПЭМИН (побочных электромагнитных излучений и наводок).

Таким образом, сочетание физической автономности и логической сегментации создает стерильную среду. Это гарантирует, что результаты испытаний будут достоверными, исследуемый код – в сохранности, а информационная инфраструктура организации – в полной безопасности от «агрессивного» поведения тестируемого ПО [3].

Логическая архитектура и сегментация изолированного стенда для испытаний СЗИ

Проектирование стенда для проведения сертификационных испытаний средств защиты информации (СЗИ) и анализа программного обеспечения на отсутствие недекларированных возможностей (НДВ) требует перехода от классической модели «одной сети» к строго сегментированной иерархической структуре. Логическая сегментация – это не просто разделение IP-адресов, а реализация комплексной политики безопасности, которая минимизирует риски компрометации процесса испытаний и обеспечивает достоверность получаемых результатов.

Эффективный стенд должен быть разделен на функциональные зоны, каждая из которых обладает собственным набором правил доступа, набором программных средств и уровнем доверия. Такая архитектура позволяет реализовать принцип «нулевого доверия» внутри самой лаборатории. Предлагаются следующие зоны:

1. Зона управления – «мозг» всей инфраструктуры. Это изолированная зона, предназначенная для взаимодействия экспертов-испытателей с компонентами стенда. Главная задача этого сегмента – обеспечить централизованное администрирование и строгий аудит всех действий, проводимых в процессе исследования.

Зона управления реализует следующие функции.

Управление ресурсами стенда. Эксперты используют данный сегмент для запуска виртуальных машин в Исполняемом сегменте, настройки параметров сканирования в Сегменте анализа и управления хранилищами данных.

Ведение журналов и аудит. Согласно требованиям ФСТЭК, все действия эксперта должны быть протоколированы. В зоне управления разворачиваются системы сбора логов (SIEM или ELK-стеки), которые агрегируют данные о сетевой активности, запускаемых процессах и доступе к файлам.

Подготовка отчетности. Здесь формируются протоколы испытаний, акты анализа уязвимостей и итоговые заключения. Эта зона считается наиболее «чистой» и защищенной от воздействия потенциально опасного ПО.

В качестве инструментария используются:

- компьютеры с усиленной защитой от НСД, оснащенные специализированным ПО для доступа к другим сегментам через защищенные шлюзы;
- терминальные клиенты, с использованием протоколов RDP (с TLS-шифрованием) или SSH для удаленного управления серверами анализа и исполнения;
- системы регистрации инцидентов и трекинга задач для фиксации хода испытаний;
- средства мониторинга для контроля работоспособности аппаратных ресурсов стенда.

2. Зона анализа – это место, где происходит основная работа по выявлению уязвимостей и проверке программного кода. Здесь сосредоточены самые ресурсоемкие и интеллектуальные инструменты. В данной зоне необходимо использовать динамический анализ, фаззинг и анализ трафика.

Динамический анализ проводится на работающем ПО. В этой зоне подготавливаются скрипты для автоматизированного тестирования.

Фаззинг – это генерация огромного количества некорректных входных данных для проверки устойчивости ПО. Инструментарий включает специализированные российские разработки для поиска НДВ.

Анализ трафика используется посредством программ «Wireshark» и «Burp Suite» для перехвата и модификации запросов, передаваемых исследуемым СЗИ.

3. Зона исполнения – это «полигон», где объект испытаний (ОИ) развертывается в своей целевой среде. Главное требование к этому сегменту – максимальная близость к реальным условиям эксплуатации при сохранении полной изоляции.

Современные СЗИ должны работать на различных платформах, поэтому стенд должен содержать библиотеку «чистых» образов. Как пример – Windows 10 и выше, включая специфические конфигурации Active Directory или отечественные ОС: «Astra Linux», «РЕД ОС», «Альт Линукс». Испытания на этих системах обязательны для сертификации по требованиям доверия ФСТЭК. Контейнеризацию можно осуществить в среде «Docker» и кластерах Kubernetes для тестирования облачных решений безопасности.

4. Хранилище эталонов – это пассивная, но критически важная зона. Она служит единым источником правды для всех процессов испытаний. Доступ к этой зоне строго ограничен: данные могут только считываться в процессе тестов, а запись разрешена только администратору стенда.

В состав хранилища должны входить следующие компоненты.

Библиотека дистрибутивов. Образы ОС в формате ISO или шаблоны виртуальных машин (OVA/OVF) с контрольными суммами, подтвержденными производителем.

Базы данных сигнатур уязвимостей. Локальные зеркала баз ФСТЭК, CVE, NVD. Это позволяет проводить сканирование без обращения к интернету.

Архив объектов испытаний. Исходные коды, проектная документация и бинарные сборки СЗИ, проходящего сертификацию по выявлению уязвимостей и проверке программного кода.. Хранение организовано с использованием систем контроля версий (например, GitLab), работающих в режиме «только чтение» для большинства участников.

Репозиторий инструментов. Локальные копии Python-библиотек, компиляторов (GCC, MSVC) и зависимостей, необходимых для сборки исследуемого ПО в «стерильных» условиях.

Ключом к успеху сегментации является контроль потоков данных между зоной. управления и зонами анализа и исполнения:

- разрешены только протоколы управления (RDP, SSH, VNC);
- запрещен прямой проброс файлов без предварительной проверки;
- разрешена доставка агентов тестирования и сбор дампов памяти;
- категорически запрещен любой трафик, кроме ответов на запросы инструментов анализа. Это предотвращает атаку «изнутри» объекта испытаний на инфраструктуру стенда.
- доступ по протоколам HTTP/HTTPS (локальные зеркала репозиториев) или NFS/SMB возможен с правами «только чтение».

Программный инструментарий стенда для сертификационных испытаний

Динамический анализ предполагает проверку программного обеспечения в процессе его выполнения в доверенной операционной среде. Фаззинг (Fuzzing) является наиболее эффективным методом динамического поиска уязвимостей, заключающимся в подаче на вход программы огромного массива полуструктурированных случайных данных с целью вызвать отказ в обслуживании или аномальное поведение.

Проблема фаззинга заключается в экспоненциальном росте пространства состояний программы. Для достижения приемлемого покрытия кода (Code Coverage) за ограниченное время сертификационных испытаний стенд должен использовать распределенную архитектуру, которая строится по принципу «Мастер – исполнитель». Главный узел генерирует тестовые наборы данных и распределяет их между узлами-исполнителями. Это позволяет увеличить скорость перебора входных векторов в десятки и сотни раз. Использование контейнеризации под управлением локального оркестратора позволяет мгновенно наращивать мощность анализа при тестировании сложных системных сервисов.

Для фаззинга на стенде применяются следующие подходы.

1. Инструменты, которые используют обратную связь от целевой программы.

2. Специализированные средства для анализа сетевых протоколов СЗИ (TLS, IPsec), требующие понимания структуры пакетов.

Программная среда стенда должна включать компоненты мониторинга, которые классифицируют падения (crashes): Является ли ошибка воспроизводимой? Приводит ли она к возможности удаленного выполнения кода (RCE)? Влияет ли она на доступность СЗИ?

Стенд должен включать в себя изолированные серверы сборки, среда которых полностью контролируется специалистами испытательной лаборатории. Сборка проводится на «чистых» дистрибутивах операционных систем, исключающих наличие сторонних компиляторов или библиотек, а программный инструментарий настраивается так, чтобы при повторной сборке из тех же исходных кодов получался бит-в-бит идентичный бинарный файл. Это достигается путем фиксации временных меток, путей к файлам и версий компиляторов.

Аппаратная реализация испытательного стенда

Аппаратный уровень является фундаментом всей системы сертификационных испытаний. Надежность и доверенность программных средств анализа не имеют смысла, если подлежащая аппаратная платформа содержит аппаратные закладки или недокументированные функции на уровне микрокода процессора или чипсета. В связи с этим, проектирование аппаратной части стенда требует особого подхода, сочетающего производительность и технологический суверенитет.

Согласно актуальной политике обеспечения информационной безопасности критической информационной инфраструктуры (КИИ), сертификационные испытания СЗИ рекомендуется проводить на оборудовании, обладающем подтвержденным уровнем доверия.

Использование серверов на базе процессоров «Эльбрус» (например, Эльбрус-8С/16С) является приоритетным для стендов, предназначенных для испытаний СЗИ высших уровней доверия. Архитектурным преимуществом является оригинальная архитектура с широким командным словом. Она обеспечивает высокую степень защищенности от классических атак типа переполнения буфера или возврата в библиотеку, так как многие механизмы защиты здесь реализованы на уровне «кремния».

Для сертификации важно, чтобы эксперты могли понимать логику работы системы на самом низком уровне. Наличие отечественной документации на архитектуру команд процессора позволяет исключить наличие скрытых команд.

Проверка функционирования СЗИ в специфических средах, отличных от x86, что позволяет выявить ошибки переносимости и скрытые зависимости от архитектуры.

Процессоры семейства «Байкал» (Baikal-M, Baikal-S) актуальны для тестирования СЗИ, ориентированных на конечные пользовательские устройства и встраиваемые системы. Такие процессоры позволяют создавать компактные кластеры для проведения распределенного фаззинг-тестирования при ограниченном энергопотреблении стенда. Наличие готовых платформ под управлением отечественных ОС («Astra Linux», «Альт») делает их идеальными узлами для «исполняемого сегмента» стенда.

Несмотря на курс на импортозамещение, архитектура x86 остается доминирующей для большинства современных СЗИ. Для стенда используются серверы отечественной сборки, прошедшие проверки на отсутствие НДВ.

Обязательным требованием является наличие аппаратных модулей доверенной загрузки (АМДЗ), таких как «Аккорд» или «Соболь», блокирующих несанкционированный доступ к системе до загрузки ОС.

Процесс сертификации генерирует колоссальные объемы информации. Один сеанс интенсивного фаззинга или динамического анализа может порождать терабайты данных в сутки: обнаружение ошибок, детальные логи работы анализаторов, сетевого трафика и системных событий ОС, а также требования виртуализации хранения множества состояний ВМ для мгновенного отката к «стерильной» среде.

В связи с этим, должны выполняться следующие требования к архитектуре к системе хранения данных (СХД):

- отказоустойчивость – применение RAID-массивов (уровни 6 или 10) для предотвращения потери результатов многодневных испытаний при выходе из строя накопителей;

- производительность (IOPS) – для фаззинга критически важна скорость записи. Рекомендуется использование многоуровневого хранения – SSD/NVMe для активных задач анализа и емкие HDD для архивного хранения логов;

- локализация – СХД должна быть физически расположена внутри периметра стенда; использование облачных или внешних хранилищ категорически запрещено.

Сетевая инфраструктура стенда должна обеспечивать строгую изоляцию сегментов и контроль каждого пакета данных.

Для построения сети используются управляемые коммутаторы. Основные требования к ним:

- поддержка VLAN (IEEE 802.1Q). Она позволяет логически разделить сеть на зону управления, зону фаззинга и зону хранения. Это предотвращает возможность влияния нестабильного ПО из зоны испытаний на работу управляющих серверов стенда;

- списки доступа (ACL). Настройка правил фильтрации трафика на уровне портов. Должен соблюдаться принцип «запрещено всё, что не разрешено явно».

Аппаратная реализация должна предусматривать физический разрыв связи с глобальной сетью Интернет. Обмен данными с внешним миром (например, получение обновлений анализаторов или передача отчетов заказчику) осуществляется через специализированную «станцию очистки» или доверенные носители информации с обязательным антивирусным контролем.

Аппаратный комплекс должен быть защищен от внешних факторов:

- использование ИБП двойного преобразования для предотвращения повреждения файловых систем при скачках напряжения.

- поддержание температурного режима в серверных стойках, так как фаззинг-кластеры работают в режиме 100% нагрузки CPU длительное время.

- стойки с оборудованием должны быть опечатаны и оснащены датчиками вскрытия.

Обеспечение информационной безопасности самого стенда

Испытательный стенд является объектом повышенного риска, так как в его контуре циркулируют наиболее чувствительные активы: исходные тексты программ, проектная документация и сведения о еще не устраненных уязвимостях. Компрометация такой системы может привести не только к утечке интеллектуальной собственности заказчика, но и к фальсификации результатов сертификации. Поэтому защита самого стенда строится по принципу эшелонированной обороны.

Для предотвращения образования условий утечки информации за счет возникающих в любой цифровой радиоэлектронной аппаратуре электромагнитного излучения, необходимо обеспечить:

- экранирование стенда сертификационных испытаний или применения радиопоглощающих покрытий для его защиты;

- построения развязывающих радиочастотных фильтров в общих цепях питания аппаратных средств или применения локальных источников питания;

- выбор пространственной ориентации стенда с учетом диаграмм направленности элементов излучения или расширение зоны локализации с учетом затухания электромагнитного излучения.

Эти меры позволят защитить утечку и влияние электромагнитного излучения на интеллектуальную собственность, заложенную в архитектуру стенда для проведения сертификационных испытаний. Это являются еще одним элементом эшелонированной обороны.

Доступ экспертов к ресурсам стенда жестко ограничен. Необходимо внедрение двухфакторная аутентификация (2FA), исключающая доступ по одному лишь паролю. Помимо знания секретного кода, исследователь должен обладать аппаратным фактором – USB-токеном или смарт-картой (например, Рутокен или JaCarta). Это гарантирует, что даже в случае перехвата пароля злоумышленник не сможет проникнуть в среду испытаний.

Стенд функционирует в режиме тотального логирования. Регистрации подлежат не только факты входа в систему, но и каждое значимое действие: запуск автоматизированных сканеров, обращение к файлам исходного кода, изменение сетевых правил или создание снимков виртуальных машин. Журналы аудита передаются на выделенный сервер в защищенном сегменте, что исключает возможность их модификации или удаления со стороны испытателя. Это обеспечивает прозрачность процесса и возможность ретроспективного анализа в случае инцидентов.

Для предотвращения несанкционированного доступа (НСД) применяются сертифицированные российские СЗИ, такие как Dallas Lock или TrustLock. Эти системы реализуют мандатный принцип управления доступом и обеспечивают целостность программной среды. СЗИ блокируют неиспользуемые порты ввода-вывода, контролируют подключение внешних носителей и создают изолированную программную среду, в которой разрешен запуск только того ПО, которое необходимо для проведения испытаний. Таким образом, стенд превращается в «черный ящик», защищенный от внешних атак и внутренних злоупотреблений.

Библиографический список

1. Проект обеспечения информационной безопасности бизнес-процессов: Тестирование программного обеспечения// Дзен [Электронный ресурс]. – 2023. – Режим доступа: https://dzen.ru/a/ZH5m0mGeMlzZ4F9O. – Дата доступа 01.02.2026.

2. Методика тестирования обновлений безопасности программных, программно-аппаратных средств// ФСТЭК России [Электронный ресурс]. – 2022. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g– Дата доступа 03.02.2026.

3. Марков А.С. Актуальные вопросы сертификации средств защиты информации по требованиям безопасности информации//Информационное противодействие угрозам терроризма. – 2020. – №28.

УДК 004.056:378.147; ГРНТИ 50.41.19,14.35.09

РАЗРАБОТКА ОБРАЗОВАТЕЛЬНОЙ ПЛАТФОРМЫ НА БАЗЕ МИКРОСЕРВИСНОЙ DLP-СИСТЕМЫ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

С.А. Филимонов

Казанский государственный энергетический университет,
Российская Федерация, Казань, stanislav.filimonov04@mail.ru

Аннотация. Представлена разработка микросервисной DLP-платформы (Data Loss Prevention) с использованием Apache Kafka как образовательного инструмента для подготовки специалистов в области информационной безопасности. Основное внимание уделено интеграции практических учебных сценариев в систему защиты данных. Платформа обеспечивает обработку более 10 000 событий в секунду и может использоваться для формирования компетенций в области кибербезопасности.

Ключевые слова: DLP-система, Apache Kafka, микросервисная архитектура, информационная безопасность, образовательные технологии, кибербезопасность.

DEVELOPMENT OF AN EDUCATIONAL PLATFORM BASED ON A MICROSERVICE DLP SYSTEM FOR TRAINING CYBERSECURITY SPECIALISTS

S.A. Filimonov
Kazan State Power Engineering University,
Russian Federation, Kazan, stanislav.filimonov04@mail.ru

Abstract. This paper presents the development of a microservice DLP (Data Loss Prevention) platform using Apache Kafka as an educational tool for training specialists in the field of information security. The focus is on integrating practical educational scenarios into the data protection system. The platform supports the processing of over 10,000 events per second and can be used to build competencies in cybersecurity.
Keywords: DLP system, Apache Kafka, microservice architecture, information security, educational technologies, cybersecurity.

Растущие объёмы неструктурированных данных и требования к реальному времени обрабатываемых событий ставят перед DLP-системами задачу масштабирования и гибкости. Традиционные монолитные решения теряют производительность при больших нагрузках и плохо подходят для лабораторного обучения современным методам проектирования распределённых систем. В работе предложена микросервисная архитектура DLP с использованием Apache Kafka как центральной шины событий. Помимо проектных и эксплуатационных преимуществ, архитектура может быть нацелена на образовательное применение: развернутая платформа может служить основой для лабораторных работ, практических кейсов и тренажёров по анализу инцидентов и реагированию. Внедрение микросервисного подхода в DLP-систему устраняет разрыв между академическими курсами и требованиями индустрии, позволяя студентам работать с технологиями, аналогичными тем, что используют современные компании.

Архитектура системы

В рамках нашего исследования [1] была создана и протестирована система предотвращения утечек данных (DLP - Data Loss Prevention), отличающаяся высокой устойчивостью к нагрузкам и построенная на микросервисах и событийном подходе. Эти свойства были достигнуты благодаря эффективному построению структуры системы. В отличие от классических монолитных систем, здесь в качестве центрального компонента для асинхронного обмена сообщениями применяется распределённая шина данных Apache Kafka (рис. 1) [6].

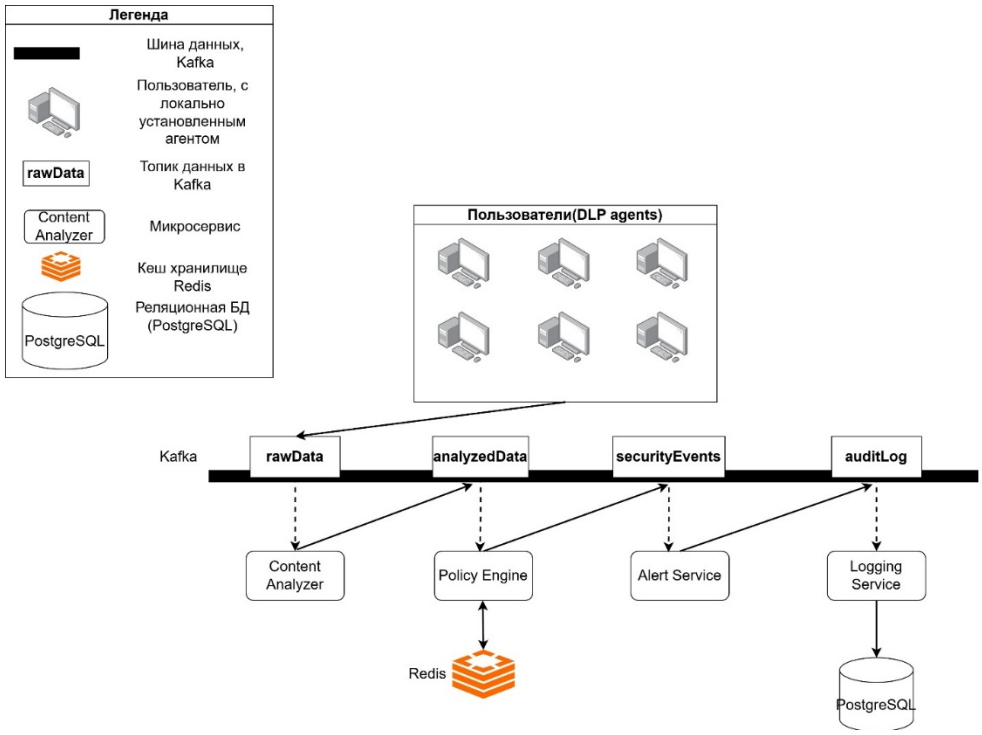


Рис. 1. Схема микросервисной DLP-платформы на базе Apache Kafka

Общая схема и принципы. Система состоит из набора независимых микросервисов (производители событий, сервисы анализа контента, применяющие политики, сервисы постановки задач SOAR/SIEM, генераторы уведомлений) и распределённой шины Apache Kafka для обмена событиями. Kafka обеспечивает асинхронную передачу сообщений, буферизацию, параллелизм через партиции и отказоустойчивость через репликацию. Микросервисы развёрнуты в контейнерах и взаимодействуют по стандартизованным протоколам (REST, gRPC, Kafka-топики). Предложенный подход обеспечивает высокую степень модульности и расширяемости системы: добавление новой функциональности (топиков) осуществляется путем инкрементальной разработки и развертывания специализированных микросервисов без необходимости модификации существующих компонентов [2].

Архитектурные преимущества:

– изоляция отказов и независимое обновление сервисов;
– горизонтальное масштабирование «горячих» компонентов (партиции/консьюмеры);
– гарантированная доставка и буферизация для сглаживания пиковых нагрузок;
– гибкая интеграция с SIEM/SOAR/LDAP/AD, системами журналирования и мониторинга;
– высокая модульность системы.

Таким образом, данная архитектура устраняет традиционные ограничения по производительности и отказоустойчивости, присущие классическим DLP-системам. Она обеспечивает изоляцию сбоев, модульность, гибкое горизонтальное масштабирование отдельных компонентов (микросервисов, отвечающих за анализ контента, применение политик и генерацию уведомлений), а также гарантированную доставку событий за счет буферизации в Kafka [5].

Для реализации системы были выделены следующие ключевые компоненты.

Продюсеры событий: генерация/эмуляция пользовательских действий (email, web-upload, файловые операции).

Сервисы предобработки: нормализация, извлечение метаданных, анонимизация тестовых данных.

Сервис применения политик: загрузка правил из БД (PostgreSQL), кэширование в Redis, сопоставление содержимого события с политиками.

Сервис генерации уведомлений и интеграция с SIEM/SOAR.

Мониторинг и метрики: сбор RPS (количество запросов к сервису в секунду от произвольного пользователя), задержек, потребления ресурсов (Prometheus/Grafana).

Прототип системы был протестирован на серверном оборудовании начального уровня. Результаты тестирования подтвердили высокую эффективность подхода для задач информационной безопасности.

В 60-секундном нагрузочном тесте система показала следующие характеристики:

- 658 200 сообщений за 60 с (≈10 829 RPS);
- 99% сообщений обрабатывались с задержкой <89 мс;
- в ходе моделирования набора тестовых угроз около 30% трафика было классифицировано как потенциально подозрительное, что соответствует параметрам тестовой выборки и подтверждает корректность функционирования системы;
- ресурсы сервера в тесте – загрузка CPU ≈52% (от максимальной загрузки), память ≈23% (≈892 МБ), сетевой ввод ≈124.7 МБ/с.

Тестирование подтвердило горизонтальную масштабируемость системы и ее способность выдерживать нагрузки, превышающие типовые показатели монолитных DLP-решений. Кроме того, анализ метрик потребления ресурсов позволяет уверенно заключить, что предложенная архитектура не требует дорогостоящего серверного оборудования и способна эффективно функционировать на базовых аппаратных средствах.

Созданная архитектура, объединяющая гибкость микросервисов и потоковую обработку данных с помощью Kafka, может эффективно связывать теорию с практическими навыками. На её основе можно разрабатывать учебные кейсы – от настройки отдельных сервисов до моделирования атак с нагрузкой более 10 000 RPS, что соответствует современным требованиям в области кибербезопасности.

Варианты лабораторного стенда по работе с микросервисами, Kafka и DLP: цели и задачи

Ниже перечислены ключевые цели и задачи, которые ставятся при использовании лабораторного стенда:

- научить студентов проектировать и отлаживать микросервисные приложения и потоковые конвейеры;
- показать администрирование Kafka (топики, партиции, реплики, балансировка);
- отрабатывать разработку и настройку DLP-политик и анализ инцидентов.

В качестве типовых заданий можно предложить следующие темы.

«Настройка продюсера/консьюмера: создать продюсер, генерирующий события, и консьюмер для фильтрации по топику».

«Анализ влияния партиций/реплик: измерить RPS и задержки при увеличении числа партиций/реплик».

«Создание учебной политики «обнаружение конфиденциального документа»: настроить правило, инициировать «утечку» и отработать цепочку реакции».

«Инцидент-реакция: имитировать попытку выгрузки исходного кода и отработать процесс создания тикета в SOAR и последующего разбора инцидента».

Классические труды по проектированию распределенных систем [3] могут стать теоретической и практической основой для создания стенда.

На текущий момент ведется разработка методических указаний для некоторых из перечисленных выше тем. Для примера кратко опишем содержание работы по созданию учебной политики – среды для моделирования инцидентов утечки данных. Для разработки учеб-

ных политик DLP доступны подробные обзорные материалы от компаний Forcepoint и Symantec [4].

Суть политики – это формализованное правило, которое состоит из трех основных частей:

- что искать? (критерий или условие);
- где искать? (контекст: почта, мессенджер, файловый обмен и т.д.);
- что делать при обнаружении? (реакция или действие).

Политика A – конфиденциальные документы:

Что искать: ключевые слова («Секретно», «Коммерческая тайна», «Договор №»).

Где: исходящая почта и вложения.

Реакция: в боевом режиме – блокировка отправки и запись в SIEM; в учебном – пометка «ИНЦИДЕНТ» и логирование для разбора.

Политика B – платежные данные (PAN - Primary Account Number):

Что искать: шаблон номера карты (регулярное выражение).

Где: сетевой трафик (HTTP, FTP), файлы.

Реакция: симуляция остановки сессии и генерация подробного предупреждения в учебном журнале.

Политика C – защита исходного кода:

Что искать: расширения (.java, .py, .cpp) или признаки кода (большое количество фигурных скобок, ключевые слова).

Где: web-upload, облачные хранилища, USB.

Реакция: в учебном режиме – запись инцидента и разбор критериев отличия кода от документа.

Методика проведения занятий и оценивание могут быть следующими.

Формат занятий – комбинированный: практические лаборатории (60–90 мин), домашние задания (контейнерные развертывания), мини-проекты (командная разработка микросервисов и сценариев атак).

Оценивание основывается на корректности развертывания, полноте тестовых сценариев, глубине анализа инцидентов и умении интерпретировать метрики (RPS, p99 задержки, уровень ложных срабатываний).

Работа в таких форматах способствует формированию у студентов ключевых профессиональных и личностных компетенций, таких, как проектирование событийно-ориентированных систем, разработка микросервисов и политик безопасности, анализ инцидентов и взаимодействие с SOAR/SIEM, командная работа и документирование исследований. В итоге выпускники обретут не только знания, но и практический опыт, который будет востребован работодателями.

Подводя итог, можно констатировать, что в ходе исследования разработана и апробирована прототипная микросервисная DLP-платформа на базе Apache Kafka. Экспериментальные результаты подтверждают высокую пропускную способность (>10 000 RPS) и низкие задержки (<89 мс), а модульная архитектура делает платформу пригодной для использования как учебного стенда. Предложенные лабораторные сценарии и политики дают возможность формировать у студентов компетенции, актуальные для индустрии информационной безопасности. Перспективы дальнейшей разработки – внедрение платформы в образовательные программы в виде практикума и развитие набора сценариев для обучения реагированию на реальные угрозы.

Автор выражает искреннюю благодарность своему научному руководителю, доценту кафедры «Информационные технологии и интеллектуальные системы» КГЭУ, к.ф.-м.н. Петровой Наталье Константиновне за профессиональное наставничество и помощь в исследовании, благодаря которой была выполнена эта работа.

Библиографический список

1. Филимонов С.А., Петрова Н.К. Архитектура высоконагруженной DLP-системы на базе микросервисов и Apache Kafka // Материалы IV междунар. науч.-практ. конф. «Цифровая трансформация: тенденции и перспективы», Москва, 18.12.2025 (в печати)
2. Пашичев В.С., Ивашковская Т.К. Оптимизация механизма доставки сообщений в Apache Kafka // Материалы 76-й Всерос. науч.-техн. конф. студентов, магистрантов и аспирантов. Ярославль: ЯГТУ, 2023. С. 110-112. URL: https://7universum.com/ru/tech/archive/item/16138 (дата обращения: 30.01.2026)
3. Клеппман М. Высоконагруженные приложения: программирование, масштабирование, поддержка / пер. с англ. СПб.: Питер, 2025. 640 с. URL: https://www.piter.com/collection/bestsellery-oreilly/product/vysokonagruzhennye-prilozheniya-programmirovanie-masshtabirovanie-podderzhka-2 (дата обращения: 22.12.2025)
4. Gordon A., Grimes J. Data Loss Prevention for Dummies // John Wiley & Sons, Inc., 2021. 64 p. URL: https://info.cyberhaven.com/hubfs/Webflow_Resources/Dummies_DLP_2025.pdf (дата обращения: 01.02.2026)
5. Филисов Д.А. Архитектура высоконагруженных приложений / Universum: технические науки: электрон. научн. журн. 2023. № 10(115). URL: https://7universum.com/ru/tech/archive/item/16138 (дата обращения: 23.12.2025).
6. Apache Kafka Documentation [Электронный ресурс] // Apache Software Foundation. URL: https://kafka.apache.org/documentation/ (дата обращения: 23.12.2025)

УДК 004.056; ГРНТИ 81.93.29

УТОЧНЕНИЕ ПОНЯТИЯ «БЕЗОПАСНОЕ ПО» ДЛЯ РАЗРАБОТКИ И ВЫБОРА МЕР ЗАЩИТЫ ПО

Ю.М. Кузьмин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, kuzmin_yurii@mail.ru

Аннотация. В работе выполнен анализ и уточнение понятия безопасного программного обеспечения. Уточнены требования к разработке и обеспечению безопасности ПО.
Ключевые слова: жизненный цикл ПО, безопасность ПО, ошибка, уязвимость.

CLARIFICATION OF THE CONCEPT OF OF SAFE SOFTWARE FOR THE DEVELOPMENT AND SELECTION OF PROTECTION MEASURES

Y.M. Kuzmin

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, kuzmin_yurii@mail.ru

The summary. The paper analyzes and clarifies the concept of secure software. Requirements for software development and security have been clarified.
Keywords: software development life cycle, application security, software error, vulnerability.

Введение

Необходимость уточнения понятия «Безопасное программное обеспечение (ПО» продиктована следующими обстоятельствами:

- в различных руководящих документах даются сильно не совпадающие формулировки этого понятия;
- отсутствие единства формулировок провоцирует разные взгляды разработчиков ПО на решение проблемы обеспечения безопасности ПО.

В литературе и руководящих документах по защите программ и данных часто используются следующие родственные формулировки:

- защищенное ПО;
- безопасное ПО;
- доверенное ПО.

Даже в проектах ФГОС 4 поколения образовательной программы базового высшего образования по специальности 34.01 «Кибербезопасность» в разное время давались разные названия соответствующей специализации:

- в первых итерациях проекта формулировка была «специализация № 3 «Разработка защищенного программного обеспечения»;
- начиная с 7-ой итерации проекта (июнь 2024 г.) название изменилось на «специализация № 3 «Разработка защищенного (доверенного) программного обеспечения».

Защищенное ПО

Защищенное ПО предполагает встраивание специальных средств (технических средств защиты авторских прав - ТСЗАП) в ПО для защиты авторских прав разработчика ПО (защита от несанкционированного доступа (НСД), от несанкционированного копирования, от анализа ПО). Законодательной основой для защиты авторских прав являются:

- 4 часть ГК РФ (см. например статьи 1125, 1226, 1228, 1229, 1233, 1234, 1235, 1240, 1250, 1252, 1255, 1259, 1261, 1280, 1299, 1465);
- УК РФ (см. например, статьи 146 ч.2, 159.6, 272, 273, 274, 274.1, 281). Здесь надо напомнить, что в 2008-2010 г. году прокуратурой г. Магадана расследовалось уголовное дело № 73956 (так называемое «Магаданское дело»), когда разработчик ПО - Жуков В.В., защищая с помощью ТСЗАП свои авторские права на бухгалтерское ПО, нарушил другое право – право бухгалтерии на информацию и получил два года лишения свободы условно и штраф 100 тысяч рублей по статье № 273 ч.1 УК РФ за разработку вредоносного ПО. Обвинение основывалось на том, что разработчик с помощью ТСЗАП заставил ПО по истечении срока действия договора работать с функциональными ограничениями, что было расценено как блокирование доступа к информации.
- КоАП РФ об административных правонарушениях (статья 7.12).

Безопасное ПО

Безопасное ПО в разных редакциях ГОСТ Р 56539 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» определялось по-разному:

- в редакции от 2016 г. [1] это «ПО, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы, т.е. безопасное ПО должно быть написано с использованием методов и средств безопасной разработки ПО и не содержать уязвимостей;
- в редакции от 2024 г. [2] дается немного расширенное толкование этого понятия: «Безопасное ПО: ПО, разработанное в ходе реализации совокупности процессов (мер), направленных на предотвращение появления и устранение недостатков ПО», т.е. безопасное ПО не должно содержать неустраненных недостатков.

Под недостатком ПО в этом ГОСТ понимается:

- несоответствие ПО заданным требованиям;
- ошибки в ПО, допущенные в ходе разработки, которые (если их не исправить) могут являться *а*) причиной невыполнения ПО своих функций и *б*) причиной появления уязвимостей в ПО.

Практические примеры таких недостатков (в основном для программ на языках C/C++) рассматриваются в [3] и [4].

При этом от разработчиков ПО сертифицированных средств защиты информации (они требуются для защиты информации в особо важных ИСПДн, ГИС, значимых объектах КИИ) требуется не просто использование процессов безопасной разработки, но и подтверждение (сертификация) процессов безопасной разработки ПО. Для этого ФСТЭК России издала

Приказ №240 [5], в соответствии с которым сертифицирующая организация должна осуществлять:

- проверку, соответствует ли руководство по безопасной разработке ПО требованиям, установленным в Приказе;
- проверку, соответствуют ли особенности реализованных в организации процессов безопасной разработки ПО требованиям по безопасной разработке в [2];
- проверку, имеются ли у разработчика необходимые средства разработки ПО, тестирования ПО, средства для композиционного, статического, динамического анализа ПО, соответствующие требованиям по безопасной разработке в [2];
- проверку, соответствуют ли фактические процессы безопасной разработки ПО у разработчика тем процессам, которые описаны в руководстве по безопасной разработке ПО;
- инструментальную проверку сертифицирующими органами, как реализованы у разработчика процессы безопасной разработки ПО, и какая используется среда в процессе разработки и сборки ПО;
- проверку, обеспечена ли организация разработчика сотрудниками, у которых имеются знания, умения и навыки, необходимые и достаточные для безопасной разработки ПО.

Остается открытым вопрос – как оценить степень безопасности ПО количественно? Для ответа на этот вопрос есть три пути:

1. Свое толкование понятие «Безопасное ПО» приводится в [6]. В соответствие с этим документом безопасное ПО – это ПО, для которого фактический уровень доверия соответствует целевому *уровню доверия* (задается организацией, использующей приложение). Фактический уровень доверия определяется как результат анализа рисков небезопасности ПО, поэтому для его оценки надо использовать [7], в котором описаны все необходимые шаги по анализу и обработке и снижению рисков небезопасности ПО (до приемлемого уровня). Целевой уровень доверия соответствует заданному владельцем приложения допустимого (или приемлемого) уровня риска (в соответствии с принятой в организации политикой управления рисками). Таким образом, для оценки степени безопасности ПО необходимо провести анализ (оценку) рисков небезопасности ПО и оценить, насколько остаточный риск соответствует приемлемому.
2. Согласно [8] и Методике поиска уязвимостей в ПО [9] безопасным можно считать ПО, для которого потенциал нападения ниже уровня стойкости ПО (задается в [9] для каждого уровня доверия (уровни доверия для разного рода систем описаны в [10]). Потенциал нападения вычисляется по [9] и Приложению В к [8]. Вычисления проводятся с учетом знаний об уровне нарушителя – Н1 (базовый уровень – отдельные личности без спец. средств взлома ПО), Н2 (базовый повышенный), Н3 (средний уровень возможностей) или Н4 (высокие возможности – шпионские ведомства с полным набором средств взлома ПО). Уровни нарушителя рассматриваются в Приложении 8 к [11]).
3. Безопасным в полной мере (полностью удовлетворяющим требованиям по безопасной разработке ПО, установленным в [2]) можно считать ПО, выпущенное в рамках сертифицированного конвейера разработки безопасного ПО, который обеспечивает защиту на всех стадиях жизненного цикла разработки ПО. Такие корпоративные конвейеры были созданы и используются в Cloud.ru, СберТех, Т1 (Сфера), Инфотекс. Проблемой являлось использование в них открытого ПО и необходимость импортзамещения. В сентябре 2025 г. 8 отечественных разработчиков вместе с ИСП РАН и НТЦ «ФОБОС-НТ» представили полностью импортонезависимый конвейер разработки безопасного ПО [12]. В этом конвейере используется только российское ПО, и все инструменты защиты ПО разработаны компа-

ниями из России. Данный конвейер соответствует требованиям регулятора – ФСТЭК России.

Доверенное ПО

Доверенное ПО – это ПО, которое выполняет все те функции (функциональные требования), которые описаны в ТЗ на него и не выполняет других (возможно вредоносных) функций. То есть кроме требований по отсутствию в ПО ошибок и требований по защищенности ПО от анализа и НСД необходимо учитывать еще требования функциональной безопасности (надежности) ПО, такие как

- выявление в ПО закладок, реализующих неописанное в документации поведение ПО;
- контроль правильности получаемых результатов;
- защита от отказов в обслуживании;
- контроль работоспособности и производительности;
- защита от ошибок во внешней среде (от действий пользователя, от ошибок аппаратуры, от ошибок при работе с базой данных и т.п.);
- резервное копирование и восстановление;
- самовосстановление при ошибках и сбоях.

Конкретные требования по функциональной безопасности ПО, разрабатываемого для разных видов промышленных изделий, зафиксированы, например, в [13, 14, 15, 16].

Выводы

Таким образом, **в данной работе показано, что понимать под безопасным ПО** надо не только ПО без ошибок и уязвимостей (согласно [1] и [2]), но и ПО, защищенное от НСД, копирования, анализа и взлома, а также функционально безопасное (надежное) ПО. Такой подход к определению необходим для планирования комплекса мер по обеспечению и повышению безопасности разрабатываемого ПО, включающего:

- меры по безопасной разработке ПО (без уязвимостей);
- меры по защите ПО от НСД и анализа;
- меры по обеспечению функциональной безопасности ПО.

Библиографический список

1. ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». [Электронный ресурс]. - Режим доступа: https://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=195653. - Дата доступа: 8.02.2026.

2. ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». [Электронный ресурс]. - Режим доступа: https://protect.gost.ru/document1.aspx?control=31&id=263523. - Дата доступа: 8.02.2026.

3. ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ ПО. Общие требования». [Электронный ресурс]. - Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=257755. - Дата доступа: 8.02.2026.

4. ГОСТ Р 71206 «Защита информации. Разработка безопасного программного обеспечения.Безопасный компилятор языков С/С++. Общие требования». ». [Электронный ресурс]. - Режим доступа: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=3&month=2&year=2024&search=&id=257752. - Дата доступа: 8.02.2026.

5. Приказ ФСТЭК России от 01.12.2023 г. №240 «Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации». [Электронный ресурс]. - Режим доступа: https://docs.cntd.ru/document/1305682626. - Дата доступа: 8.02.2026.

6. ГОСТ Р 27034-1 - 2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопсность приложений. Часть 1. Обзор и общие понятия». [Электронный ресурс]. - Режим доступа: https://docs.cntd.ru/document/1200112883. - Дата доступа: 8.02.2026.

7. ГОСТ Р 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.». [Электронный ресурс]. - Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=177398. - Дата доступа: 8.02.2026.

8. ГОСТ Р ИСО-МЭК 18045–2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий». [Электронный ресурс]. - Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=184854. - Дата доступа: 8.02.2026.

9. Информационное сообщение ФСТЭК России от 10 февраля 2021 г. № 240/24/647 «Об утверждении Методики выявления уязвимостей и недекларированных возможностей в программном обеспечении». [Электронный ресурс]. - Режим доступа: https://fstec.ru/component/attachments/download/2923. - Дата доступа: 08.02.2026.

10. Приказ ФСТЭК России от 02.06.2020 г. №76 Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам ТЗИ и средствам обеспечения безопасности информационных технологий».

11. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]. - Режим доступа: https://fstec.ru/component/attachments/download/2919.. - Дата доступа: 08.02.2026.

12. В России представлен суверенный конвейер разработки безопасного ПО -. [Электронный ресурс]. - Режим доступа: https://www.cnews.ru/news/line/2025-09-18_v_rossii_predstavlen_suverennyj. - Дата доступа: 08.02.2026.

13. ГОСТ Р МЭК 61508-2-2012 «Национальный стандарт Российской Федерации. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам».

14. ГОСТ Р МЭК 60880-2010 «Национальный стандарт Российской Федерации. Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А».

15. ГОСТ Р МЭК 62304-2013 «Национальный стандарт Российской Федерации. Изделия медицинские. Программное обеспечение. Процессы жизненного цикла»

16 ГОСТ Р ИСО 26262-6-2021 «Дорожные транспортные средства. Функциональная безопасность. Часть 6. Разработка программного обеспечения изделия».

УДК 004.056.53; ГРНТИ 81.93.29

АНАЛИЗ ВОЗМОЖНОСТЕЙ ЯЗЫКА UML ДЛЯ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Ю.В. Конкин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, konkinjv@yandex.ru

Аннотация. В данной работе рассматривается Unified Modeling Language (UML) с точки зрения его использования для моделирования сценариев реализации угроз безопасности информации при разработке модели угроз. Предлагается рассматривать модель угроз безопасности информации с точки зрения объектно-ориентированного анализа и проектирования, возможностей языка UML для представления сценариев защиты информации и документирования проекта системы защиты информации. В заключении работы делается вывод о возможности использования универсального языка моделирования UML в задачах разработки систем защиты информации.

Ключевые слова: система защиты информации, угроза безопасности информации, модель угроз, сценарий реализации угрозы, сценарий защиты, язык UML.

ANALYSIS OF UML LANGUAGE CAPABILITIES FOR MODELING INFORMATION SECURITY THREATS

Yu.V. Konkin
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, konkinjv@yandex.ru

The summary. This paper examines the Unified Modeling Language (UML) from the perspective of its use for modeling scenarios of information security threats during the development of a threat model. It proposes to consider the information security threat model from the perspective of object-oriented analysis and design, as well as the capabilities of the UML language for representing information protection scenarios and documenting the information protection system project. In conclusion, the paper concludes that the universal modeling language UML can be used in the development of information protection systems.
Keywords: information protection system, information security threat, threat model, threat implementation scenario, protection scenario, UML language.

Введение

Разработка системы защиты информации является сложной структурированной задачей, которую необходимо рассматривать с различных точек зрения: программно-аппаратной, организационной и правовой.

Система защиты информации должна исключать несанкционированный доступ. В ходе разработки такой системы нужно сделать:

1) оценить ее текущее состояние безопасности информации;

2) разработать для нее модель угроз безопасности информации;

3) разработать последовательность действий для совершенствования системы защиты информации на основе модели угроз.

При разработке системы защиты информации первые два шага выполняются с учетом взаимных результатов. Оценка текущего состояния безопасности информации выполняется на основе актуальных угроз безопасности информации, которые определяются в результате разработки соответствующей модели. В ходе оценки текущего состояния безопасности информации используется структурно-функциональная модель информационной системы, с помощью которой можно подробно рассмотреть защищенность функций системы. Такой подход позволяет определить защищенность системы на любом шаге ее создания.

В настоящее время информационные системы разрабатываются с помощью средств автоматизированного проектирования. При разработке систем защиты информации также используются данные средства, обеспечивающие проектирование программных и аппаратных частей системы.

С этой точки зрения модель угроз безопасности информации можно рассматривать как самостоятельную систему, так и подсистему обеспечения безопасности системы обработки информации.

В соответствии с [1] в структуре модели угроз безопасности информации выделяются основные элементы:

1) описание информационной системы как объекта защиты;

2) источники угроз безопасности информации и способы их реализации;

3) выводы об актуальности угроз безопасности информации исследуемой или разрабатываемой информационной системы.

От качества разработки модели угроз безопасности информации зависит и правильность выбора организационных и технических мер и средств защиты безопасности информации.

Современные информационные системы имеют сложную объектную структуру, для разработки которых применяют объектно-ориентированные технологии. Структуру указанных выше элементов также можно рассматривать с точки зрения объектно-

ориентированного проектирования, с использованием языка UML [2]. Язык UML использует диаграммы, которые позволяют представить сущности предметной области как объекты с определенным состоянием и поведением. Модель угроз безопасности информации также рассматривается с различных сторон, поэтому применение объектно-ориентированных технологий в данной задаче является оправданным [3].

Язык UML и сценарии реализации угроз безопасности информации

Использование языка UML состоит в разработке диаграмм в определенной последовательности, чтобы выполнить нисходящий и разносторонний процесс построения моделей информационной системы. Для моделирования сценариев реализации угроз безопасности информации наиболее подходят следующие диаграммы:

1) вариантов использования;
2) классов;
3) состояний;
4) последовательности;
5) деятельности.

Унифицированный язык моделирования UML успешно применяется при проектировании различных технический систем [2]. Диаграммы UML отражают структуру и работу системы, для которой разрабатывается модель, а также способствует наглядному представлению ее иерархической архитектуры с различных сторон. Это упрощает анализ состава системы и процессов, которые она выполняет, а следовательно, делает возможным подготовить последующую реализацию системы. Модели на языке UML делают возможным рассмотрения системы защиты информации с различных точек зрения, на основе которых будет выполняться ее анализ, разработка и размещение на объекте информатизации. Язык UML также может быть использован для выполнения разработанных моделей систем защиты безопасности информации. Кроме того, этот язык может быть использован для документирования решений по структуре системы, всей ее иерархии, а также безопасности информации, является средством описания организационно-технических требований к системе и способам ее тестирования.

В языке UML прецеденты на диаграмме вариантов использования представляют особенности моделируемой системы с точки зрения внешних систем. Диаграммы взаимодействия, состояния и действия описывают систему с точки зрения ее активности. Объектно-ориентированные особенности системы представляются диаграммами классов, которые также описывают функциональные требования, предъявляемые к моделируемым системам.

На первом шаге моделирования сценариев реализации угроз определяются требования к системе защиты информации с учетом возможных угроз безопасности информации, воздействующих на процессы организации, с нанесением ущерба разной степени.

На втором шаге выполняется классификация угроз безопасности информации и их группировка по особенностям реализации. Количество угроз безопасности информации очень большое, следовательно необходимы классификация угроз и оценка порождаемых ими рисков, а также формирование рекомендаций и мер по защите от них.

На третьем шаге выполняется обоснование непосредственно методологии обеспечения безопасности информации.

На четвертом этапе выполняется оценка рисков безопасности информации. На основе результатов оценок рисков и способов управления рисками формируется система управления безопасностью информации организации. Качество таких оценок зависит от целостности и полноты анализа и оценки факторов риска, а также эффективности методов, поддерживающих принятие решений, и исполнения их впоследствии. При оценке рисков безопасности информации используются различные параметры, такие как нелинейность и сложность при-

менения [3]. Кроме того, эти параметры являются неопределенными, но существенными факторами, которые влияют на качество оценки риска безопасности информации и, следовательно, учитываются при оценке таких рисков. Для работы с такими неопределенностями возможно применение теории нечетких множеств [3].

На пятом этапе выполняется оценка эффективности обеспечения безопасности информации. В реальной работе возможно возникновение ранее неизвестных угроз, которые не были учтены при анализе безопасности информации. Такие угрозы могут уменьшить эффективность мер защиты информации. Эти особенности должны быть рассмотрены при оценке эффективности безопасности информации с системной точки зрения.

Таким образом, на основе языка UML можно реализовать задачу моделирования сценариев реализации угроз безопасности информации при разработке систем защиты информации.

Диаграмма вариантов использования содержит сервисы будущей системы. Эти сервисы доступны внешним системам. Такие системы являются актерами. Каждый вариант использования предназначен для описания сервисов, предоставляемых актёру. Таким образом, каждый вариант использования определяет набор функций, совершаемый системой при взаимодействии с актёром. При этом определяется, что система будет делать, но никак не определяется, как система будет выполнять сервисы вариантов использования и взаимодействовать с актёрами. Диаграмма вариантов использования имеет специальное представление в виде графа, на котором отображаются в виде графических элементов варианты использования, актёры и отношения между ними. Вариант использования является удобным способом описания реализации угрозы безопасности информации.

Язык UML поддерживает объектно-ориентированное проектирование, обеспечивая возможность объектной декомпозиции предметной области задачи. Полученные объекты могут находиться в отношении наследования.

Применение UML как средства разработки моделей создаваемой системы защиты информации позволяет и заказчику и разработчику выработать единый подход к представлению задачи.

Первой диаграммой, описывающей будущую систему, разрабатывается диаграмма вариантов использования или прецендентов. Данная диаграмма представляет описание того, что будет делать система, то есть ее функциональное назначение. Подробностей реализации функций системы эта диаграмма не содержит.

Из диаграммы вариантов использования следует концептуальное представление создаваемой системы для использования в дальнейшей разработке.

Среди отношений между элементами диаграммы вариантов использования устанавливаются несколько видов отношений. Для решения задачи, рассматриваемой в данной работе, используются следующие два вида отношений:

1) отношения ассоциации для указания некоторой связи между вариантом использования и актёром;

2) отношения обобщения для указания факта, что один вариант использования является более общим для второго варианта использования.

Диаграмма классов в объектно-ориентированном программировании предназначена для представления абстракций и сущностей проектируемой системы.

Эта диаграмма является графом специального вида, состоящим из узлов, представляющих классы, между которыми установлены различные структурные отношения, например, отношение наследования. Кроме того, на этой диаграмме отображаются внутренние данные класса и алгоритмы его методов. В языке UML класс является представлением набора объектов, обладающих идентичными представлением внутреннего состояния, алгоритмами, описывающими поведение и отношениями с другими объектами.

В представлении класса указывается обязательное имя, атрибуты с типами данных и операции (методы) с параметрами. Атрибуты и операции уточняются в ходе проектирования системы. Для построения иерархии классов между классами указываются различные отношения: наследования, ассоциации, зависимости.

Диаграмма классов дает наглядное представление системы, что является ее преимуществом. Это сильно проявляется при разработке сложных систем, имеющих много различных классов, а также сложную структуру взаимосвязей этих классов. Такое свойство диаграммы классов может найти применение при разработке системам защиты информации.

Для моделирования угроз, ориентированных на отдельные активы, удобно применять диаграмму последовательности. Эта диаграмма отражает сообщения между объектами системы, которые удобно применять при проектировании системы защиты безопасности информации.

Сценарии реализации угроз безопасности информации можно разработать на основе диаграмм деятельности. Кроме того, здесь можно применить расширения языка UML – нотации BPNM [4].

Данная нотация может быть применена в случаях сложных сценариев реализации угроз безопасности информации, для которых необходимо подробное описание процессов.

Любая угроза должна быть описана следующими сценариями:

1) сценарий для реализации угрозы;

2) сценарий для защиты от угрозы.

Первый из указанных сценариев целесообразно рассматривать как состояние системы защиты информации на момент разработки сценария.

При проектировании систем защиты безопасности информации большое значение имеет их моделирование. Использование объектно-ориентированного подхода с использованием языка UML является в данном случае удобным и обоснованным [5].

Кроме того, такие модели позволяют подробно документировать разработку сложных систем, делая ее понятной как заказчику так и разработчику.

Выводы

Объектно-ориентированный подход с использованием языка UML позволяет разрабатывать сценарии реализации угроз безопасности информации, а также проекты систем защиты безопасности информации. Описание сценария содержит диаграммы вариантов использования, диаграммы классов, на основе которых определяются источники угроз безопасности информации, диаграммы последовательности и деятельности. Созданные на основе UML сценарии реализации угроз могут использоваться как документация на систему защиты безопасности информации. Такая документация будет использована специалистами по защите информации при построении систем защиты от угроз безопасности информации.

Библиографический список

1. Методический документ «Методика оценки угроз безопасности информации». Утвержден ФСТЭК России 5 февраля 2021 г.

2. Рогачев А.Ф., Федорова Я.В. Использование UML-моделей для исследования и обеспечения информационной безопасности сложных технических систем //Известия Нижневолжского агроуниверситетского комплекса: Наука и высшее профессиональное образование. 2014. № 4(36). С.236-241.

3. Филяк П.Ю. Мишарин Г.Д. Создание модели информационной безопасности средствами языка UML// Информационная безопасность. 2015. Т. 18. № 2. С. 254-259.

4. Приезжая А.Н. Технологии встраивания функций безопасности в бизнес-процессы// Вестник РГГУ. Серия: документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2009. №10. С. 71-84.

5. На каком языке рисуют схемы: что такое UML и почему его понимают во всём мире [Электронный ресурс]. – Режим доступа: https://practicum.yandex.ru/blog/uml-diagrammy.

УДК 004.056; ГРНТИ 81.93.29

OSINT-РАЗВЕДКА: КАК ОСУЩЕСТВЛЯЕТСЯ И НА ЧЕМ ОСНОВЫВАЕТСЯ

М.С. Спирьянов, Ю.М. Кузьмин
Рязанский государственный радиотехнический университет имени В.Ф. Уткина,
Российская Федерация, Рязань, mish.goscha@yandex.ru, kuzmin_yurii@mail.ru

Аннотация. В статье рассматривается разведка по открытым источникам (OSINT) как методологически оформленный процесс получения выводов на основе общедоступных данных. Показано место OSINT в жизненном цикле защиты информации: от оценки внешней экспозиции и мониторинга угроз до поддержки расследований инцидентов. Описаны ключевые этапы конвейера OSINT (постановка задачи, сбор, очистка, анализ, верификация, отчет) и критерии качества результатов: достоверность, актуальность, полнота, согласованность и воспроизводимость. Отдельно рассматривается цифровой след как источник сведений, способных повысить эффективность социальной инженерии и таргетированных атак. Предложены практические меры снижения OSINT-экспозиции организации и подход defensive OSINT как регулярного аудита публичной информации.
Ключевые слова: OSINT, разведка по открытым источникам, цифровой след, социальная инженерия, защита информации, информационные системы.

OPEN-SOURCE INTELLIGENCE (OSINT): HOW IT IS CONDUCTED AND WHAT IT IS BASED ON

M. S. Spiryanov, Y.M. Kuzmin
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, mish.goscha@yandex.ru, kuzmin_yurii@mail.ru

The summary. The paper discusses open-source intelligence (OSINT) as a disciplined process of collecting, processing, validating and analyzing publicly available information for security-related decision-making. The OSINT role within information security is outlined, including external exposure assessment, threat intelligence support and incident response enrichment. A typical OSINT pipeline is described (requirements, collection, cleaning, correlation, verification and reporting), along with result quality criteria such as credibility, timeliness, completeness, consistency and reproducibility. Special attention is given to the digital footprint as a source of actionable context for targeted social engineering and other attacks. Defensive OSINT is proposed as a regular audit of publicly exposed data and a set of mitigation measures to reduce unnecessary visibility.
Keywords: OSINT, open-source intelligence, digital footprint, social engineering, information security, information systems.

Введение

Рост объема публичной информации о людях, организациях и цифровой инфраструктуре приводит к тому, что существенная часть контекста для атак и защитных решений формируется вне периметра информационных систем. Публикации на корпоративных сайтах, открытые реестры, вакансии, публичные профили, материалы конференций и архивы вебстраниц создают «цифровой след», который может быть собран и интерпретирован без непосредственного воздействия на ИС.

Разведка по открытым источникам (OSINT) представляет собой не набор случайных поисковых запросов, а процесс, ориентированный на доказательность: формулирование задачи, сбор и нормализация данных, сопоставление фактов из независимых источников, оценка достоверности и оформление выводов в виде отчета. В практиках защиты информации OSINT применяется для внешнего аудита информационной безопасности организации, обогащения разведки угроз дополнительными источниками и подержки расследований инцидентов безопасности информации [1].

Цель статьи – систематизировать основы OSINT-разведки в контексте защиты информации, описать типовой конвейер работ и показать, каким образом цифровой след повышает как защитные возможности, так и риски таргетированных атак и социальной инженерии.

На рисунке 1 ниже показано визуальное представление цифрового следа объекта разведки.

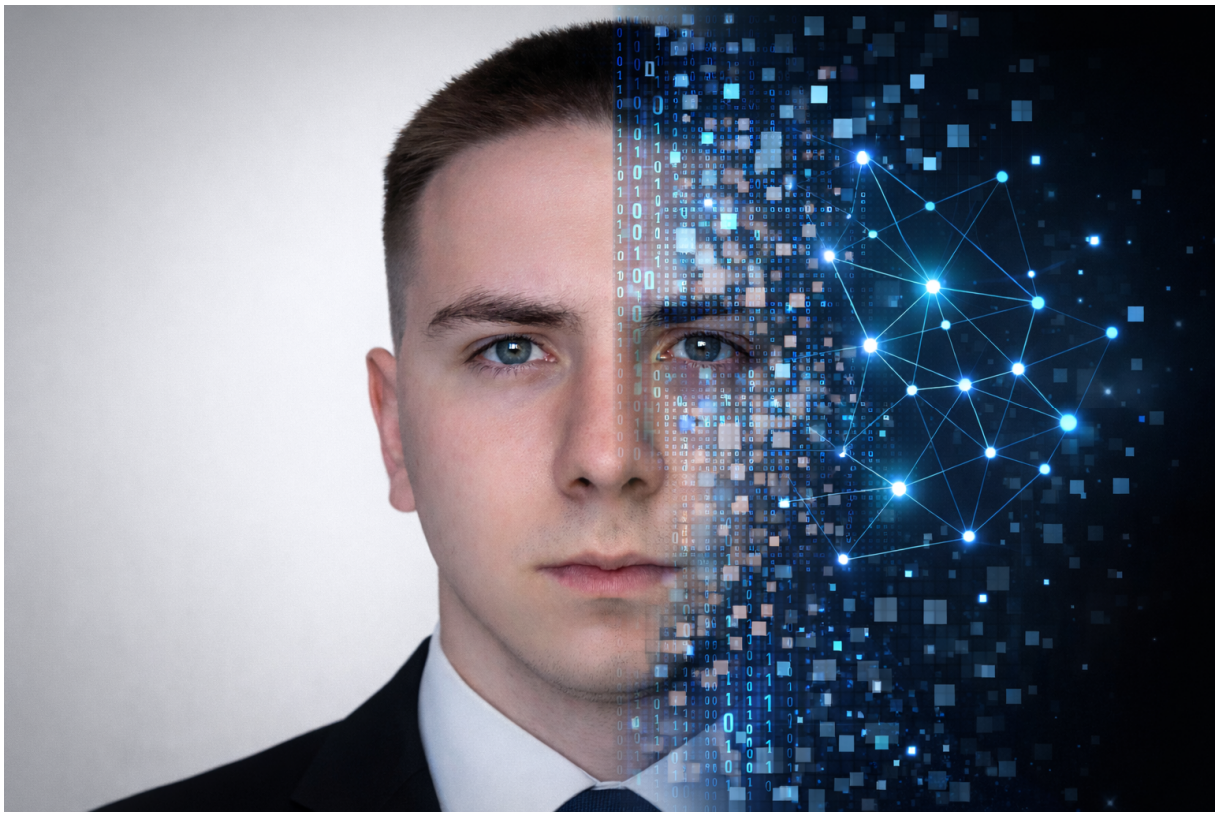


Рис. 1. Визуальная метафора цифрового следа: объект наблюдения и его цифровые представления

1. Понятийная база и место OSINT в защите информации

OSINT (Open-Source Intelligence) – сбор и анализ информации из открытых источников с целью получения проверяемых выводов, полезных для принятия решений. В рамках защиты информации OSINT рассматривается как легитимная работа с публично доступными данными при соблюдении правовых и этических ограничений.

В отличие от неформального поиска, OSINT ориентирован на воспроизводимость и верификацию: каждый факт должен иметь источник, а значимые выводы – подтверждаться несколькими независимыми наблюдениями или авторитетным первичным источником. Это особенно важно для ИБ, где ложные корреляции приводят к ошибочным управленческим решениям или неверным приоритетам реагирования.

С позиции информационных систем объектами OSINT-анализа выступают: (1) персоналии и их роли, (2) организация и связи с контрагентами, (3) технологический ландшафт и внешние сервисы, (4) документы и медиа, (5) события и изменения активности. Анализ строится вокруг сущностей и отношений между ними, что естественным образом приводит к использованию графовых моделей и методов корреляции данных [2, 3].

2. Категории источников OSINT и их значимость для ИБ

В таблице 1 ниже приведены примеры источников OSINT.

Таблица 1. Примеры источников OSINT и типовые риски цифрового следа

Категория источников	**Что можно извлечь (в интересах защиты)**	**Типовые риски при избыточной экспозиции**
Официальные документы и отчеты	политики, регламенты, контакты подразделений, упоминания подрядчиков	раскрытие внутренних процессов и цепочки согласований
Корпоративные сайты и медиа	актуальные сервисы, точки контакта, публичные инициативы	повышение убедительности фишинга за счет «правдоподобного» контекста
Вакансии и описания проектов	упоминания технологий и требований к стеку, модель эксплуатации	частичное раскрытие технологического ландшафта и зависимости от вендоров
Публичные социальные сети	роль сотрудников, профессиональные связи, публичные события	таргетирование социальной инженерии, подбор «правильной» легенды
Технические метаданные внешних сервисов	косвенные признаки используемых платформ и провайдеров, изменения инфраструктуры	рост атак на внешнюю поверхность при накоплении контекста
Архивы и кэшированные копии	устаревшие версии страниц, старые контакты и документы	восстановление «удаленной» информации и неактуальных деталей

Для стороны защиты ценность OSINT состоит в возможности своевременно обнаруживать нежелательную публикацию чувствительных сведений, оценивать внешнюю поверхность атаки и обучать персонал на реальных примерах. Для атакующей стороны ключевым фактором является корреляция: отдельные элементы цифрового следа, будучи собранными в единый профиль, существенно снижают стоимость подготовки таргетированных атак.

3. Методологические основы: качество данных и интеллект-цикл

Методологическое ядро OSINT опирается на интеллект-цикл: постановка задачи, сбор, обработка, анализ, оформление вывода и обратная связь. На каждом этапе задаются критерии приемки: какие данные считаются релевантными, как проверяется их происхождение и каким образом фиксируются допущения. Этот цикл показан на рисунке 2.

Качество OSINT-результата определяется совокупностью признаков: достоверность источника, актуальность, полнота, согласованность с независимыми данными и воспроизводимость. Практически это означает необходимость триангуляции: важные факты подтверждаются несколькими источниками и, по возможности, первичными публикациями (официальные документы, заявления владельца ресурса, публичные отчеты).

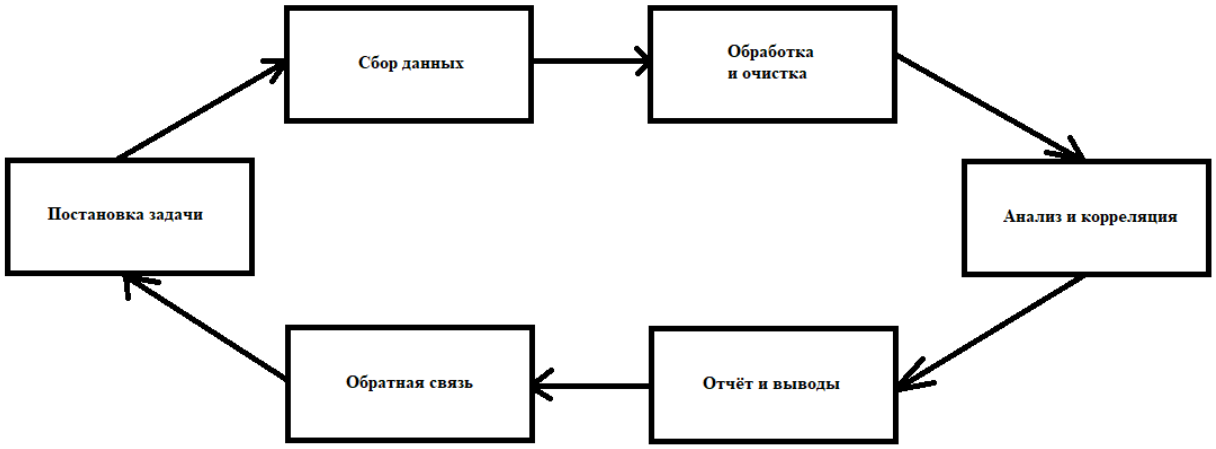


Рис. 2. Интеллект-цикл OSINT как последовательность стадий от постановки задачи до отчета

4. Конвейер OSINT-разведки в задачах ИБ

Практическая реализация OSINT начинается с формулирования требований: определяются целевые сущности, временной горизонт, допустимые источники и критерии успеха. Далее выполняется сбор данных, который в ИБ часто сочетает мониторинг публичных публикаций, анализ открытых реестров, источников и наблюдение за изменениями внешней экспозиции (например, появление новых публичных ресурсов или контактов).

Этап обработки включает очистку, нормализацию форматов и разрешение сущностей, когда одно и то же имя, домен или организация приводятся к единому представлению. Аналитический этап строится на корреляции событий и связей, оценке уверенности и оформлении аргументации: какие факты подтверждают гипотезу, какие противоречат и почему они отброшены или требуют дополнительной проверки.

Отчет в OSINT-ориентированной работе по ИБ должен содержать краткое резюме для руководства и техническое приложение для специалистов: список источников, ключевые наблюдения, уровень уверенности по каждому выводу и рекомендации по снижению выявленных рисков.

5. OSINT как риск: цифровой след и таргетированные воздействия

Цифровой след становится поверхностью атаки, когда публичная информация позволяет злоумышленнику реконструировать структуру организации, выявить роли и цепочки взаимодействия, подобрать правдоподобные поводы для коммуникации и оценить внешние зависимости. Эти знанния о организации повышают эффективность атак типа социальной инженерии и точность выбора сценариев воздействия на внешние компоненты ИС.

Типовыми «усилителями» риска выступают: избыточная детализация вакансий, публикация внутренних шаблонов документов, повторяющиеся контактные данные и отсутствие контроля за устаревшими материалами в архивах. Сам по себе отдельный элемент цифрового следа редко критичен, критичность возникает при накоплении и корреляции данных.

6. Оборонительный (defensive) OSINT и меры снижения OSINT-экспозиции

Оборонительный OSINT можно рассматривать как регулярный аудит публичной информации об организации и ее ключевых процессах. Практика оборонительного OSINT включает периодическую инвентаризацию внешних публикаций, мониторинг новых упоминаний и проверку того, что чувствительные сведения не оказываются в открытом доступе по ошибке.

Комплекс мер снижения возможностей получения разведанных с помощью OSINT-разведки включает: (1) регламентацию публичных коммуникаций и согласование публикаций, (2) обучение персонала цифровой гигиене и распознаванию социальной инженерии, (3) унификацию и минимизацию публичных сведений о внутренних процедурах, (4) контроль корпоративных ресурсов и архивов, (5) технические меры защиты внешних сервисов (актуальные настройки доступа, минимизация избыточных метаданных, мониторинг утечек).

Заключение

OSINT-разведка является инструментом двойного назначения: она одновременно повышает качество защитных решений и демонстрирует, как публичные данные могут быть использованы против организации. Внедрение оборонительной OSINT позволяет снижать избыточную экспозицию, повышать устойчивость к социальной инженерии и укреплять защищенность информационных систем. Перспективным направлением является интеграция OSINT-разведки с процессами мониторинга и реагирования (SIEM/SOAR/XDR).

Библиографический список

1. Сидорова М.Е., Кузьмин А.Р. Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности [Электронный ресурс]. - Режим доступа: vestnik-rosnou.ru/sites/default/files/61_PDFsam_N1.pdf . - Дата доступа: 08.02.2026.
2. Слащинин О.А. Разведка по открытым источникам (OSINT) информации в следственной деятельности [Электронный ресурс]. - Режим доступа: elib.bsu.by/bitstream/123456789/311424/1/Slashchynin%2C%20O.A.%20Razvedka%20po%20otktritym%20istochnikam%20%28OSINT%29.pdf. - Дата доступа: 08.02.2026.
3. Кочергин Я.А. Использование открытых источников информации (OSINT) в следственной и оперативно-розыскной деятельности [Электронный ресурс]. - Режим доступа: cyberleninka.ru/article/n/ispolzovanie-otkrytyh-istochnikov-informatsii-osint-v-sledstvennoy-i-operativno-rozysknoy-deyatelnosti. - Дата доступа: 08.02.2026.

УДК 004.056; ГРНТИ 81.93.29

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМ

О.С. Семочкина, С.А. Вилкова, Ю.М. Кузьмин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, kuzmin_yurii@mail.ru

Аннотация. Современные студенты ежедневно используют цифровые платформы: сдают задания на платформах для дистанционного обучения, общаются в мессенджерах, хранят материалы в облачных папках. Но вместе с удобством приходят риски: взломы аккаунтов, утечки персональных данных, фишинговые рассылки от «имени деканата». В докладе простым языком объясняется, как искусственный интеллект помогает защищать образовательные сервисы: учится на поведении пользователей, замечает подозрительную активность (например, когда «студент» в 3 часа ночи скачивает все экзаменационные билеты за 2 минуты) и даже предсказывает атаки до их совершения. Приведены реальные примеры из практики российских вузов и простые аналогии из повседневной жизни.

Ключевые слова: кибербезопасность, искусственный интеллект, образовательные платформы, защита данных студентов, машинное обучение.

PROSPECTS FOR USING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY OF EDUCATIONAL PLATFORMS

O.S. Semochkina, S.A. Vilkova, Y.M. Kuzmin

Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, kuzmin_yurii@mail.ru

Abstract. Today's students use digital platforms on a daily basis: they complete assignments on distance learning platforms, communicate via messaging apps, and store their materials in cloud folders. However, with convenience comes risk: account hacks, personal data leaks, and phishing emails sent on behalf of the university. This report provides a simple explanation of how artificial intelligence helps protect educational services: it learns from user behavior, detects suspicious activity (such as a "student" downloading all exam questions in 2 minutes at 3 a.m.), and even predicts attacks before they occur. The article provides real-life examples from Russian universities and simple analogies from everyday life.

Keywords: cybersecurity, artificial intelligence, educational platforms, student data protection, and machine learning.

Введение

Обычно студенты используют искусственный интеллект как «шпаргалку»: для поиска ответов на экзаменах, решения математических задач или написания рефератов. Но за пределами учебного процесса ИИ становится мощным инструментом защиты – не для обхода правил, а для соблюдения их. В условиях роста кибератак на образовательные системы (217%

рост за 3 года по данным Роскачества [1]) цифровая безопасность перестала быть технической деталью – она превратилась в ключевой элемент учебного процесса.

По данным «Лаборатории Касперского» каждая третья кибератака в России в 2025 году была направлена на образовательные учреждения. Почему? Потому что в университетских системах хранятся «золотые жилы» для злоумышленников:

- персональные данные студентов (паспорта, СНИЛС, ИНН);
- научные разработки и диссертации;
- доступ к государственным информационным системам через учётные записи преподавателей.

Традиционные антивирусы и брандмауэры здесь бессильны: они ловят известные вирусы, но не замечают, когда хакер заходит в систему под вашим логином и паролем. В статье рассматриваются вопросы, как ИИ превосходит традиционные методы защиты, какие ресурсы требуют его внедрение и где именно в университете он может спасти данные студентов и преподавателей.

Традиционные методы защиты: сильные и слабые стороны

Помимо ИИ-систем в вузах применяются следующие системы:
– сигнатурные системы – блокируют известные вирусы по базам сигнатур;
– двухфакторная аутентификация (2FA) – требует код из приложения или SMS для входа;
– системы обучения сотрудников и студентов – тренинги по распознаванию фишинга;
– шифрование данных – TLS для трафика, шифрование баз данных.

Почему их недостаточно?

Несмотря на широкое распространение классических средств защиты, они не способны в полной мере противостоять современным киберугрозам в образовательной среде.

Сигнатурные системы эффективны только против известных угроз, для которых уже существует сигнатура в базе данных. Однако хакеры постоянно модифицируют вредоносный код, создавая полиморфные версии вирусов, которые обходят детектирование. Особенно уязвимы эти системы перед атаками типа zero-day – эксплуатацией неизвестных уязвимостей, для которых сигнатуры ещё не разработаны.

Двухфакторная аутентификация (2FA) значительно повышает безопасность входа в систему, но не защищает от социальной инженерии. Мошенники используют фишинг – отправляют студентам и сотрудникам письма или сообщения в мессенджерах от имени деканата, бухгалтерии или медпункта с просьбой «подтвердить данные». Жертва сама вводит логин, пароль и даже одноразовый код на поддельном сайте, после чего злоумышленник получает полный доступ к аккаунту.

Обучение персонала и студентов – важный, но недостаточный элемент защиты. Человеческий фактор остаётся самой уязвимой точкой любой системы безопасности: усталость, стресс, недостаток внимания или простое незнание могут привести к ошибке. Кроме того, тренинги проводятся периодически, а кибератаки происходят круглосуточно.

Шифрование данных (протоколы TLS для передачи трафика, шифрование баз данных) защищает информацию от перехвата при передаче и хранении, но бессильно против инсайдерских угроз. Если злоумышленник получает легальные учётные данные сотрудника с правами доступа к базе, шифрование не помешает ему экспортировать персональные данные студентов.

Преимущества ИИ-защиты: что он делает лучше, чем другие системы?

Искусственный интеллект кардинально меняет подход к кибербезопасности, переходя от реактивной защиты к проактивной. Рассмотрим ключевые преимущества ИИ-систем перед традиционными методами.

Скорость реакции. Традиционные системы обнаруживают угрозы через часы или даже дни – особенно если анализ выполняется вручную администратором. ИИ-системы работают в режиме реального времени, обнаруживая аномалии за 2–5 минут. Это критически важно для образовательных платформ, где каждая минута задержки может привести к утечке персональных данных тысяч студентов [1].

Адаптивность. Сигнатурные системы требуют постоянного ручного обновления баз данных – специалист должен добавить новую сигнатуру после каждой обнаруженной угрозы. ИИ же самообучается: каждый новый инцидент делает систему умнее. Она анализирует паттерны атак, выявляет закономерности и автоматически адаптирует алгоритмы детектирования без участия человека [5].

Прогностическая способность. Классические системы реагируют на уже начавшуюся атаку – когда злоумышленник уже проник в систему. ИИ способен предсказывать атаки за 20–40 минут до их реализации. Как метеоролог предсказывает дождь по падению давления, так и ИИ замечает «предвестники»: сканирование портов, тестовые запросы к базе данных, серию неудачных входов. Это даёт администраторам время на блокировку угрозы на стадии разведки [4].

Снижение ложных срабатываний. Сигнатурные системы часто «кричат» на ложные угрозы – например, блокируют легитимный трафик или помечают активность студента как подозрительную из-за временного всплеска активности во время сессии. ИИ учится на поведении каждого пользователя индивидуально: если студент всегда сдаёт задания в последнюю ночь перед дедлайном, система это запомнит и не будет считать такую активность аномальной. Это снижает нагрузку на администраторов и повышает доверие пользователей к системе защиты [5].

Круглосуточная работа. Человеческий администратор устаёт, уходит на обед, спит ночью. ИИ работает 24/7 без перерывов, что особенно важно для защиты образовательных платформ, доступных студентам в любое время суток. Ночная атака, которая могла бы пройти незамеченной при ручном мониторинге, будет мгновенно обнаружена ИИ-системой [1].

Необходимые ресурсы для внедрения ИИ-защиты

Людские ресурсы:

– Специалисты по кибербезопасности (1–2 человека на 10 000 пользователей) для настройки и мониторинга системы.

– Координаторы проекта из числа преподавателей (для интеграции в учебный процесс).

– Студенты-волонтёры (для тестирования и сбора обратной связи).

Программные ресурсы:

– ИИ-платформы: TensorFlow, PyTorch для обучения моделей.

– Системы интеграции: API для подключения к Moodle, электронному дневнику, корпоративной почте.

– Сервисы анализа: для визуализации аномалий.

– Среды тестирования: MITRE Caldera для симуляции атак в изолированной среде [4].

Аппаратные ресурсы:

– Серверы с GPU: для обработки данных в реальном времени (минимум 2 сервера для резервирования).

– Компьютеры для тестирования: симуляция атак в изолированной среде.

Где именно в университете можно внедрить ИИ-защиту?

ИИ-защиту целесообразно внедрять в ключевые цифровые точки университетской инфраструктуры, где концентрируются персональные данные и критически важные учебные процессы.

Личные кабинеты студентов и преподавателей – первая линия защиты. ИИ анализирует поведенческие паттерны: время входа, геолокацию, скорость действий. При аномалии (например, вход в 3 ночи с массовой выгрузкой файлов) система мгновенно блокирует сессию и уведомляет владельца аккаунта [5].

Системы управления обучением (Moodle, Canvas, электронные дневники) содержат оценки, задания, переписку. ИИ отслеживает подозрительные запросы к базе данных – например, попытки экспорта оценок всех студентов группы за пределы учебного расписания – и предотвращает несанкционированный доступ [1].

Корпоративная почта и мессенджеры – основной канал фишинговых атак. ИИ распознаёт мошеннические сообщения по контексту: письма «от деканата» с просьбой подтвердить данные через сторонний сайт, сообщения «от медпункта» с запросом персональных показателей. Такие письма автоматически попадают в карантин до проверки администратором [2].

Облачные хранилища с научными работами (дипломы, диссертации, патенты) требуют особой защиты. ИИ контролирует массовые скачивания и копирование файлов, блокируя попытки выгрузки интеллектуальной собственности неавторизованными пользователями [5].

Серверы и сетевая инфраструктура университета также подключаются к ИИ-мониторингу. Система анализирует сетевой трафик в реальном времени, выявляя сканирование портов, DDoS-атаки или попытки горизонтального перемещения внутри сети после первичного проникновения [4].

Защита от ИИ: двусторонняя плоскость рисков

Важно осознавать, что искусственный интеллект – это не фантастическая технология, а инструмент с двойным назначением. Его использование несёт не только возможности, но и риски, требующие комплексной защиты.

Использование искусственного интеллекта в образовательной и корпоративной среде создаёт двустороннюю угрозу безопасности, требующую комплексной защиты как от утечек данных во внешние сервисы, так и от вредоносного контента, поступающего из нейросетей.

Внутренние риски связаны с неконтролируемой передачей корпоративных данных во внешние ИИ-сервисы. Сотрудники и студенты часто загружают в публичные чат-боты (ChatGPT, Gemini и др.) конфиденциальные документы, исходный код, персональные данные и служебную информацию – в среднем 46% промптов содержат корпоративные данные [6]. Это приводит к нарушению требований комплаенса [3], потере контроля над интеллектуальной собственностью и попаданию коммерческой информации в обучающие выборки публичных моделей. Особенно опасно распространение так называемого «теневого ИИ» (AI Shadow IT) – несанкционированных сервисов и плагинов, находящихся вне контроля ИТ-службы. При этом 60% организаций не имеют никаких политик управления использованием ИИ, что усугубляет проблему [6].

Внешние риски исходят непосредственно от нейросетей и злоумышленников, использующих ИИ как инструмент атак. Современные угрозы включают автоматизацию фишинга с помощью ИИ для создания персонализированных сообщений социальной инженерии, генерацию визуально неотличимых фишинговых страниц-клонов официальных сервисов, а также распространение заражённых документов (.docm, .xlsm с макросами) и скриптов (.js, .exe) через ответы ИИ-сервисов. Особую опасность представляет методика prompt-injection – ма-

нипуляция промптами для принуждения модели раскрыть конфиденциальные данные или внедрить вредоносные инструкции в ответы [6].

Таким образом, защита от ИИ требует двунаправленного подхода: контроля исходящего трафика (чтобы предотвратить утечки данных при запросах к нейросетям) и фильтрации входящего трафика (чтобы заблокировать вредоносные вложения, скрипты и поддельные страницы в ответах ИИ). Только комплексное решение обеспечивает безопасное использование преимуществ искусственного интеллекта без компрометации данных и инфраструктуры.

Что могут сделать студенты уже сегодня?

ИИ-защита – это хорошо, но 80% атак начинаются с действий самого пользователя. Простые правила:

1. Никогда не переходите по ссылкам из писем «от администрации вуза» – заходите на сайт вуза напрямую через браузер.
2. Используйте двухфакторную аутентификацию (2FA) – даже при утечке пароля злоумышленник не войдёт без кода из приложения или СМС.
3. Разные пароли для разных сервисов – если взломали соцсеть, это не должно открыть доступ к личному кабинету университета.
4. Сообщайте в ИТ-службу о подозрительных письмах и сообщениях. Так вы не только защищаете себя, но и помогаете обучать ИИ на реальных примерах угроз.

Заключение

Искусственный интеллект не заменяет традиционные методы защиты – он дополняет их. Его сила в том, что он видит то, что невидимо для классических систем: аномалии в поведении, предвестники атак, скрытые угрозы. Однако внедрение ИИ требует чёткого планирования: ресурсов, экспертизы и интеграции в существующие процессы. При этом важно соблюдать требования законодательства о персональных данных – анализироваться должны только метаданные, а не содержимое личных сообщений и файлов [3].

Главный вывод: будущее кибербезопасности образования – не в замене человека машиной, а в создании симбиоза, где ИИ обрабатывает рутину и анализирует данные, а человек принимает стратегические решения. Для студентов это означает не только защиту персональных данных, но и уверенность в том, что их учебный процесс не будет прерван кибератакой.

Библиографический список

1. Кибербезопасность в образовании: национальный отчёт 2025 / АНО «Цифровая экономика». – М., 2025. – 84 с.
2. Kaspersky Security Bulletin 2025: Education Sector Review. – Moscow: Kaspersky Lab, 2025.
3. Федеральный закон № 152-ФЗ «О персональных данных» (ред. от 01.01.2026).
4. MITRE ATT&CK Framework v15. – 2025. –[Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения: 14.02.2026).
5. Руководство по внедрению ИИ-систем в образовательные учреждения / Минобрнауки России. – М., 2025. – 47 с.
6. Материалы вебинара «Нейросети в корпоративном трафике: тихий канал больших ИБ-рисков», ГК «Солар», 2026 г

УДК 004.056; ГРНТИ 81.93.29

ТАРГЕТИРОВАННЫЕ КОМПЬЮТЕРНЫЕ АТАКИ НА РЕСУРСЫ КОРПОРАТИВНЫХ СИСТЕМ И ИХ ОСОБЕННОСТИ

Н.А. Колесенков, В.О. Дедов, А.В. Дергачева
Рязанский государственный радиотехнический университет имени В.Ф. Уткина,
Российская Федерация, Рязань, 62nk@mail.ru, vabimgold@gmail.com, savdd013@gmail.com

Аннотация. В работе рассматривается феномен таргетированных кибератак на корпоративные информационные системы. Приводится определение таргетированной атаки, отличающее её от массовых вредоносных кампаний, анализируется соотношение понятий «таргетированная атака» и «APT». Представлена классификация целей и объектов воздействия, а также основные векторы проникновения (социальная инженерия, технические уязвимости, атаки через цепочки поставок). Подробно описан жизненный цикл атаки, включающий этапы разведки, проникновения, закрепления и достижения конечной цели. Выделены ключевые особенности современных таргетированных атак: использование легитимных системных инструментов (Living-off-the-land), нацеленность на человеческий фактор, сложность обнаружения, адаптивность и снижение стоимости подготовки за счёт теневого рынка. Кратко рассмотрены методы противодействия такие, как SIEM-системы и обучение персонала. Делается вывод о необходимости смены парадигмы защиты – перехода от сигнатурного анализа к выявлению аномалий и комплексному подходу.

TARGETED COMPUTER ATTACKS ON CORPORATE SYSTEMS RESOURCES AND THEIR FEATURES

N.A. Kolesenkov, V.O. Dedov, A.V.Dergachova
Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, 62nk@mail.ru, vabimgold@gmail.com, savdd013@gmail.com

The summary. This paper examines the phenomenon of targeted (directed) cyber attacks on corporate information systems. A definition of a targeted attack is given, distinguishing it from mass malware campaigns, and the relationship between the concepts of "targeted attack" and "APT" is analyzed. A classification of goals and objects of influence, as well as the main vectors of penetration (social engineering, technical vulnerabilities, supply chain attacks) are presented. The life cycle of an attack is described in detail, including the stages of reconnaissance, penetration, consolidation, lateral movement, and achievement of the final goal. The key features of modern targeted attacks are highlighted: the use of legitimate system tools (Living-off-the-land), focus on the human factor, difficulty of detection, adaptability, and reduction in preparation costs due to the shadow market. Countermeasures such as SIEM systems, and personnel training are briefly considered. The conclusion is drawn about the need to change the protection paradigm – a transition from signature analysis to anomaly detection and an integrated approach.

Для современных корпоративных сетей информация стала ценнейшим активом, а значит, главной мишенью для киберпреступников. Однако если массовые фишинговые рассылки или атаки программ-вымогателей (шифровальщиков) можно сравнить с уличными грабителями, то таргетированные атаки на корпоративные ресурсы – это спланированные ограбления банков с участием многоходовыми комбинациями. Такие инциденты уже давно наглядно показали, что жертвой может стать даже хорошо защищенная компания.

Что такое таргетированные атаки

Таргетированная атака – непрерывный процесс несанкционированной активности, вызванный набором хакерских программ, для получений несанкционированного доступа к инфраструктуре субъекта атаки или кражи данных.

Таргетированная атака – массовая атака на объекты корпоративных сетей, это, в первую очередь, не массовая рассылка «на удачу», а спланированная операция против конкретной корпоративной сети. Злоумышленник уделяет много времени и внимания изучению инфраструктуры организации, готовит план, а затем наносит точный удар. В отличие от обычного вируса, который пытается пробить стены лбом, здесь хакеры ищут незапертую дверь.

Они изучают, каким ПО пользуется компания, кто из сотрудников работает с финансами, и даже в каких соцсетях сидят инженеры. После проникновения их главная задача – не наследить, а тихо закрепиться в системе, чтобы украсть данные или получить контроль над ключевыми серверами. Весь этот процесс может длиться месяцами, оставаясь незамеченным для штатных средств защиты.

Это определение требует расшифровки по трем ключевым пунктам:

Это процесс, а не одно действие. Анализ инцидентов показывает, что её длительность часто составляет от 100 дней и более. Злоумышленники не спешат, их главная цель – оставаться незамеченными как можно дольше.

Атака строится под конкретную жертву. Хакеры изучают конкретные механизмы защиты компании, состав ПО, слабые места в поведении конкретных сотрудников. Цель – поразить побольше жертв.

За атакой стоят люди. «В ситуации целевой атаки не компьютерные системы бьются друг с другом, а люди: одни нападают, другие – отражают хорошо подготовленное нападение».

Здесь важно прояснить и соотношение с термином APT (Advanced Persistent Threat). Как поясняется в источнике, APT – это не сама атака, а комбинация утилит, вредоносного ПО, механизмов использования уязвимостей “нулевого дня”, других компонентов, специально разработанных для реализации данной атаки. Из всего вышесказанного таргетированная атака – это процесс, операция, а APT – это высокотехнологичное оружие (инструментарий), которое в этой операции может использоваться.

«Умное оружие»: классификация и векторы атак

Классификация по целям

Таргетированные атаки могут преследовать широкий спектр задач. Среди основных целей выделяются:

– Финансовые хищения: кража средств с банковских счетов, манипуляции с платежными системами.

– Промышленный шпионаж и нечестная конкуренция: хищение интеллектуальной собственности, баз данных клиентов, маркетинговых планов, а также саботаж производственных процессов конкурентов.

– Нарушение работы инфраструктуры: воздействие на объекты критической инфраструктуры (энергетика, транспорт, связь) и системы жизнеобеспечения.

– Политический шпионаж и кибервойна: получение доступа к закрытой информации государственных структур.

Объекты воздействия в корпоративной среде

Злоумышленники охотятся не за «вообще всеми данными», а за конкретными активами. Наибольшему риску, согласно статистике, подвергаются:

– Научно-исследовательские отделы: хранилища интеллектуальной собственности.

– Управленческое звено и бухгалтерия: доступ к финансовым инструментам и конфиденциальным договорам.

– Серверные базы данных: массивы персональных данных и коммерческой информации.

– АСУ ТП и производственные сегменты: устаревшее, но критически важное оборудование, безопасность которого сложно контролировать.

– Мобильные устройства сотрудников: слабое звено, через которое можно получить доступ в корпоративную сеть.

Основные векторы проникновения

Каким же образом атакующие добираются до этих целей?

1. Социальная инженерия.

Хакеры тщательно изучают конкретных сотрудников через соцсети, форумы и даже корпоративные сайты, чтобы составить письмо, которое жертва откроет без колебаний. Это может быть письмо от имени генерального директора, партнера или техподдержки. Используются также телефонные звонки с просьбой выполнить нужные действия, а, включая, современные технологии искусственного интеллект, не составит труда подменить голос вашего знакомого.

2. Технические векторы

Это направление включает эксплуатацию уязвимостей:

В веб-приложениях: взлом публичных сервисов компании для проникновения внутрь.

В программном обеспечении: использование как известных, так и неизвестных уязвимостей.

Через цепочки поставок: самый опасный вектор, когда атакуется не сама цель, а её доверенный партнер или разработчик ПО. Внедрение вредоносного кода в легитимное обновление позволяет поразить сотни компаний сразу.

Комбинированные атаки

Часто технический взлом сопровождается физическими действиями: подкуп инсайдеров, сбор информации из мусора или использование зараженных USB-носителей в физически изолированных сетях.

Анатомия таргетированной атаки (Жизненный цикл)

Таргетированная атака – это не спонтанный взлом, а хорошо отрепетированный многоактный спектакль. Чтобы понять логику действий злоумышленников, эксперты раскладывают атаку на фазы.

Фаза 1. Подготовка и разведка.

Злоумышленники собирают информацию о жертве из открытых источников (OSINT): соцсети сотрудников, сайты госзакупок, вакансии. Цель – найти слабые места в людях и софте. Иногда создаётся тестовый стенд для отработки атаки.

Фаза 2. Проникновение.

Активная фаза. Чаще всего используется целевой фишинг (spear-phishing) – письмо от имени коллеги или партнёра с вредоносным вложением. Реже – эксплуатация уязвимостей (zero-day) в публичных сервисах компании. Задача – получить первый контроль над точкой в сети.

Фаза 3. Закрепление и распространение.

Получив доступ, хакеры загружают основной инструментарий через C&C-центр. Они повышают привилегии, крадут пароли администраторов и перемещаются по сети (lateral movement), используя легитимные системные утилиты (PowerShell), чтобы не светиться в защите.

Фаза 4. Достижение цели.

Финальный этап в зависимости от задачи: кража данных (эксфильтрация), запуск шифровальщика, поломка производственных процессов (АСУ ТП) или манипуляция документами. После этого злоумышленники заметают следы и часто оставляют бэкдор для возврата.

Особенности современных таргетированных атак

Чем же таргетированные атаки отличаются от "фонового шума" киберпреступности настолько, что даже компании с серьезными бюджетами на безопасность становятся их жертвами? Эксперты выделяют несколько ключевых особенностей.

1. Использование легитимных инструментов (Living-off-the-land)

Злоумышленники маскируются под системных администраторов, используя штатные средства ОС (PowerShell) вместо вредоносного ПО. Это позволяет обходить сигнатурный анализ, так как защита не реагирует на "родные" утилиты.

2. Нацеленность на человека, а не на софт

Самый дорогой межсетевой экран бесполезен, если сотрудник сам открыл доступ атакующему. Социальная инженерия – это не примитивный обман, а тонкая психологическая атака, основанная на реальных данных о жертве.

3. Сложность обнаружения

Сигнатурные методы (антивирусы) здесь не работают, так как вредоносное ПО пишется под конкретную жертву. Атаку можно выявить только по аномалиям в поведении, но она может длиться годами оставаясь незамеченной.

4. Модульность и адаптивность

Атака управляется вручную в реальном времени: хакеры видят реакцию защиты и корректируют тактику. Если один инструмент обнаружен, они откатываются и используют другой.

5. Снижение стоимости "входного билета"

На теневом рынке можно купить готовые сборки эксплойтов и доступы. Сегодня сложные атаки становятся доступнее – не нужно писать код с нуля, достаточно умело скомбинировать готовые инструменты.

Пробежимся косвенно, по методам обнаружения и противодействия таким атакам, к ним относятся:

SIEM и поведенческий анализ (UEBA). Системы собирают логи со всей инфраструктуры и ищут аномалии: например, запуск PowerShell с нехарактерными параметрами или доступ бухгалтера к серверам баз данных в 3 часа ночи.

Охота на угрозы (Threat Hunting). Проактивный поиск следов компрометации, когда специалисты сами проверяют гипотезы о возможном присутствии злоумышленника.

Обучение сотрудников. Самый дешёвый и эффективный метод. Если персонал не открывает подозрительные вложения и сообщает о странных звонках, атакующие теряют основной вектор проникновения.

Заключение

Таргетированные атаки представляют собой принципиально иной класс угроз по сравнению с массовым вредоносным ПО. Их главная опасность – в нацеленности на конкретную компанию, тщательной подготовке и использовании человеческого фактора как основного вектора проникновения.

Противодействие таким атакам требует смены парадигмы защиты: от поиска вредоносных файлов – к выявлению аномалий в поведении пользователей и систем. Идеальной защиты не существует, но комплексный подход, включающий технические средства (SIEM) и обучение персонала, способен сделать атаку настолько дорогой и сложной, что злоумышленники предпочтут более легкую цель.

Библиографический список

1. Анатомия таргетированных атак [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/?ysclid=mlttrdn3ba150327810

2. Тагретированные (целевые) атаки [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/threats/targeted-attacks?ysclid=mlttrfn8j9837255608

3. Опасный тип киберпреступности: таргетированные атаки [Электронный ресурс]. – Режим доступа: https://softline.ru/about/blog/opasnyi-tip-kiberprestupnosti-targetirovannye-ataki?ysclid=mlttri9w9f987023250

УДК 004.056; ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В СООТВЕТСТВИИ С ИЗМЕНЕНИЯМИ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОМАЦИИ

Н.А. Колесенков, А.Р. Любакова, А.Р. Макушева
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, 62nk@mail.ru

Аннотация. В работе рассматриваются ключевые изменения в нормативно-правовом регулировании защиты информации, обусловленные вступлением в силу Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом ФСТЭК России № 117. Приведены основные отличия новых требований к защите информации от ранее действующих. Описан алгоритм действий, необходимых для выполнения операторами информационных систем с целью соответствия новым требованиям на всех стадиях и этапах обработки и хранения информации и функционирования системы.
Ключевые слова: государственные информационные системы, нормативно-правовое регулирование, защита информации, требования к защите информации.

ENSURING INFORMATION SECURITY OF STATE INFORMATION SYSTEMS IN ACCORDANCE WITH CHANGES IN INFORMATION SECURITY REQUIREMENTS

N.A. Kolesenkov, A.R. Lyubakova, A.R. Makusheva
Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, 62nk@mail.ru

Abstract. The paper considers key changes in the legal regulation of information protection caused by the entry into force of the Requirements for the protection of information contained in state information systems, other information systems of government agencies, state unitary enterprises, state institutions, approved by the order of the FSTEC of Russia № 117. The main differences between the new information protection requirements and the previously existing ones are given. The algorithm of actions necessary for information system operators to comply with new requirements at all stages and stages of information processing and storage and system operation is described.
Keywords: government information systems, legal regulation, information protection, information protection requirements.

Совершенствование нормативно-правового регулирования в сфере информационной безопасности является необходимым условием для устойчивого функционирования государственных информационных систем (далее - ГИС). Активная цифровизация, развитие технологий и искусственного интеллекта, а также рост числа и эволюция угроз безопасности информации приводят к формированию новых требований к защищенности ГИС. Утверждение приказом ФСТЭК России от 11 апреля 2025 г. №117 Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (далее – Требования, утвержденные приказом ФСТЭК России № 117) [1] стало решением, позволяющим обеспечить надежную защиту и устойчивое функционирование ГИС в современных условиях.

Требования, утвержденные приказом ФСТЭК России № 117, пришли на смену Требованиям о защите информации, не составляющих государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17 (далее – Требования, утвержденные приказом ФСТЭК России № 17) [2], внеся важные изменения в области защиты информации. В отличие от Приказа ФСТЭК России № 17, ориентированного исключительно на ГИС, Приказ ФСТЭК России № 117 распространяется на все информационные системы государственных органов и учреждений,

муниципальные информационные системы, если иное не установлено Законодательством Российской Федерации, а также на информационно-телекоммуникационную инфраструктуру, на базе которой функционируют информационные системы.

Требования, утвержденные приказом ФСТЭК России № 117, устанавливают для ГИС обязательный комплект организационно-распорядительной документации, которая должна обеспечивать полноценное выполнение всех организационных и технических мер, а также служить основой для контроля и аудита системы защиты. К таким относятся:

- политика защиты информации;
- внутренние стандарты по защите информации;
- внутренние регламенты по защите информации.

Политика защиты информации является основополагающим документом, который определяет стратегию обеспечения безопасности организации. В ней фиксируются область действия системы защиты, цели и задачи, а также принципы, на которых строится защита информации. Политика защиты информации устанавливает перечень информации, информационных систем, компонентов, подлежащих защите, перечни объектов защиты и распределяет ответственность между категориями лиц, участвующих в обеспечении безопасности. Данный документ утверждается руководителем организации и является обязательным для исполнения всеми подразделениями и работниками.

Внутренние стандарты по защите информации развивают положения политики защиты информации и устанавливают конкретные требования к реализации мер защиты.

Внутренние регламенты по защите информации, в свою очередь, описывают порядок действий и процедуры выполнения тех или иных процессов.

Все перечисленные документы должны разрабатываться с учетом особенностей деятельности оператора и функционирования его информационных систем. Стандарты и регламенты являются обязательными для исполнения всеми пользователями, а также должны доводиться до сведения подрядных организаций. Такой подход к документационному обеспечению позволяет реализовать процессное управление защитой информации.

Согласно Требованиям, утвержденным приказом ФСТЭК России № 117, ответственность за организацию защиты информации несет руководитель оператора, который вправе делегировать свои функции ответственному лицу, закрепив соответствующие полномочия и обязанности в его должностной инструкции.

Для непосредственного выполнения задач по защите информации создается структурное подразделение или назначаются отдельные специалисты, чьи функции прописываются в положении о подразделении или должностных инструкциях, при этом важно, что не менее 30 процентов работников такого подразделения должны иметь профильное образование или пройти переподготовку в области информационной безопасности для того, чтобы обладать компетенциями, необходимыми для выполнения возложенных на них функций.

Специалисты по защите информации обязаны обеспечивать безопасность во взаимодействии с ИТ-подразделениями и пользователями информационных систем, которые также участвуют в защите в рамках внутренних регламентов. Подразделение по информационной безопасности должно применять специализированные программные и программно-аппаратные средства автоматизации, включая системы выявления угроз, обнаружения вторжений, мониторинга и контроля защищенности, состав которых определяется внутренними документами организации.

Оператору системы необходимо проводить мероприятия по повышению уровня знаний пользователей информационных систем по вопросам защиты информации.

Также стоит отметить, что Требования, утвержденные приказом ФСТЭК России № 117, закрепляют процессный подход к защите информации, которая больше не сводится к разовому выполнению статичного набора требований, а превращается в непрерывно функционирующий механизм. Он представляет собой замкнутый цикл, который действует на

протяжении всего жизненного цикла информационной системы. На основании Требований, утвержденных приказом ФСТЭК России № 117, можно выделить четыре ключевых этапа, которые последовательно сменяют друг друга:

1. Разработка и планирование мероприятий и мер по защите информации;
2. Проведение мероприятий и принятие мер по защите информации;
3. Проведение оценки состояния защиты информации;
4. Совершенствование мероприятий и мер по защите информации.

На первоначальном этапе осуществляется фундаментальный анализ и подготовка к созданию системы защиты. В первую очередь идентифицируются потенциально опасные события и конкретные информационные системы, несанкционированное вмешательство в которые способно нарушить цели защиты, закрепленные в политике защиты информации. Ключевым действием является выявление и оценка актуальных угроз безопасности информации, реализация которых может нанести ущерб информационной системе. Завершается этап определением точного перечня необходимых защитных мер, сроков их проведения и оценкой ресурсов, которые потребуются для их выполнения.

Второй этап представляет собой практическую реализацию ранее разработанного плана, нацеленную на предотвращение выявленных угроз. Все действия направлены на достижение конкретных целей, например, предотвращение утечки конфиденциальных данных, блокирование несанкционированного доступа, модификации, подмены или удаления информации. Кроме того, меры призваны обеспечить отказоустойчивость систем, исключить их использование в незаконных целях и гарантировать возможность восстановления работоспособности и целостности данных после инцидентов.

Третий этап заключается в оценке состояния защиты и проводится на основе двух ключевых показателей, рассчитываемых по методическим документам ФСТЭК России. Показатель защищенности ($К_{зи}$) характеризует текущее состояние защиты информации от базового уровня угроз и должен рассчитываться не реже одного раза в шесть месяцев. Показатель уровня зрелости ($П_{зи}$) определяет достаточность и эффективность проводимых мероприятий и подлежит оценке не реже одного раза в два года. При несоответствии полученных значений нормированным руководитель информируется об этом в течение трех календарных дней, а результаты направляются в ФСТЭК России не позднее пяти рабочих дней.

Заключительный этап инициируется руководством на основе данных, полученных в ходе оценки, для устранения выявленных недостатков. Для этого формируется детальный план мероприятий по улучшению системы защиты. Утвержденный руководителем план обязателен к исполнению, а его главной целью является доведение показателей защищенности и зрелости до установленных нормативных значений. Таким образом, осуществляется переход к первому этапу управления деятельностью по защите информации.

Если в Требованиях, утвержденных приказом ФСТЭК России № 17, было 14 групп мер защиты, то Требования, утвержденные приказом ФСТЭК России № 117, расширяют этот перечень до 17 групп. В документе появились принципиально новые меры защиты, которые ранее не рассматривались или не были раскрыты. К таким мерам можно отнести:

1. Защита облачных вычислений. Теперь официально требуется защищать не только физические серверы, но и виртуальную инфраструктуру, к которой относятся гипервизоры, системы хранения данных и облачные среды;
2. Защита технологий контейнерных сред и их оркестрации. Появление данной меры стало ответом на развитие DevOps-культуры. Docker, Kubernetes и подобные технологии стали объектом регулирования;
3. Защита веб-технологий и программных интерфейсов (API). В данном случае ставится акцент на безопасность веб-приложений и взаимодействия между ними, что критично для современных распределенных систем;

4. Защита технологий интернета вещей (IoT); Это абсолютно новый раздел, обязывающий защищать "умные" устройства, если они используются в ГИС. К ним можно отнести различные "умные" датчики, позволяющие отслеживать состояние системы.

5. Защита мобильных устройств; Теперь это выделено в отдельную группу с жесткими требованиями к контролю и безопасности удаленного доступа.

Требования, утвержденные приказом ФСТЭК России № 117, стали более детализированными. Например, защита конечных устройств теперь подразумевает не просто установку средств защиты, а исключение несанкционированного доступа через интернет-интерфейсы, что фактически требует внедрения EDR-решений. В сфере привилегированного доступа теперь необходима строгая аутентификация или же применение усиленной многофакторной аутентификации (MFA), а также недопустимость смешения ролей – это прямое указание на необходимость использования PAM-систем. Требования к беспроводному доступу стали более технологичными: изоляция служебных и гостевых сетей, контроль уровней сигнала. В случае использования мобильных устройств оператор несет ответственность за безопасность даже в случае применения личных гаджетов сотрудников, включая защиту каналов связи, строгую аутентификацию и обязательный контроль.

Среди особенно заметных изменений можно отметить также введение Требованиями, утвержденными приказом ФСТЭК России № 117, жестких временных промежутков на устранение выявленных уязвимостей системы:

- уязвимости критического уровня опасности должны устраняться не более чем за 24 часа;

- уязвимости высокого уровня опасности устраняются в течение не более чем семи календарных дней;

- сроки устранения уязвимостей среднего и низкого уровней опасности устанавливаются во внутренних регламентах организации.

Таким образом, для обеспечения соответствия ГИС Требованиям, утвержденным приказом ФСТЭК России № 117, операторам предстоит реализовать ряд обязательных организационных и технических мер. Прежде всего, необходимо сформировать нормативную базу, разработав политику защиты информации и внутренние регламенты, которые установят единые правила работы для всех сотрудников. Особое внимание необходимо уделить взаимодействию с подрядными организациями, закрепив в договорах их обязанности по выполнению требований безопасности и контролируя их деятельность. Кадровый состав также должен быть приведён в соответствие с новыми нормативами, касающимися профессиональной подготовки специалистов по защите информации. Параллельно следует провести комплексный аудит существующей инфраструктуры безопасности, чтобы оценить её готовность к новым требованиям, и на основе полученных данных модернизировать технические средства защиты. Важнейшим направлением становится внедрение систем непрерывного мониторинга и контроля уязвимостей, позволяющих отслеживать состояние защищенности в реальном времени и оперативно реагировать на угрозы с учётом новых, более жестких сроков устранения уязвимостей. Кроме того, оператор обязан наладить систему регулярной отчётности, проводя плановые оценки защищенности с расчетом установленных показателей $К_{зи}$ и $П_{зи}$ и своевременно направляя результаты в ФСТЭК России для подтверждения эффективности принятых мер.

Подводя итог всему вышесказанному, можно прийти к выводу, что Требования, утвержденные приказом ФСТЭК России № 117, меняют подход к защите информации в ГИС, обеспечивая их эффективную защиту и устойчивое функционирование.

Библиографический список

1. Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государ-

ственных органов, государственных унитарных предприятий, государственных учреждений». – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117?ysclid=mlzebijcsr788064750

2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17?ysclid=m7 chbeq265918238503

УДК 004.056; ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ПРОЗРАЧНОГО ШИФРОВАНИЯ И АНАЛИЗА DLP-СИСТЕМ ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ В АСУ ТП

Г.А. Милованов, Т.И. Калинкина

Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, eyesclothesshop@gmail.com, tkalinkina2014@mail.ru

Аннотация. Объектом рассмотрения является система защиты информации в автоматизированных системах управления технологическими процессами промышленного предприятия, основанная на технологиях прозрачного шифрования и предотвращения утечек данных. Методом проведения работы является анализ современных угроз информационной безопасности в АСУ ТП, сравнительный анализ существующих решений прозрачного шифрования и DLP-систем, моделирование архитектуры защищенной АСУ ТП, разработка методики интеграции средств защиты информации, тестирование производительности и эффективности предложенных решений, оценка соответствия требованиям стандартов информационной безопасности. В результате разработан проект системы защиты информации для АСУ ТП, включающий: архитектуру интеграции средств прозрачного шифрования с минимальным влиянием на производительность технологических процессов, конфигурацию DLP-системы с настроенными политиками контроля каналов передачи данных, методические рекомендации по внедрению и эксплуатации системы защиты. Областью применения данного проекта является промышленные предприятия с критичной инфраструктурой АСУ ТП в нефтегазовой, энергетической, химической отраслях, на производственных объектах.

Ключевые слова: АСУ ТП, шифрование, DLP-система, политики контроля каналов передачи данных, система защиты информации.

THE USE OF TRANSPARENT ENCRYPTION AND ANALYSIS OF DLP SYSTEMS TO PREVENT DATA LEAKS IN APCS (AUTOMATED PROCESS CONTROL SYSTEMS)

G.A. Milovanov, T.I. Kalinkina

Ryazan State Radio Engineering University named after V.F. Utkin, Russian Federation, Ryazan, eyesclothesshop@gmail.com, , tkalinkina2014@mail.ru

The summary. The object of consideration is the information protection security system for automated process control systems (APCS) at industrial enterprises, based on transparent encryption technologies and data leak prevention (DLP). The method of the work is the analysis of modern threats to information security in APCS, a comparative analysis of existing solutions for transparent encryption and DLP systems, modeling the architecture of a secure automated process control system, developing a methodology for integrating information security tools, testing the performance and effectiveness of proposed solutions, and assessing compliance with information security standards. As a result, a project of an information security system for automated process control systems has been developed, including: an architecture for integrating transparent encryption tools with minimal impact on the performance of technological processes, a configuration of a DLP system with configured data channel control policies, and guidelines for the implementation and operation of a security system. The scope of application of this project is industrial enterprises with critical infrastructure of automated process control systems in the oil and gas, energy, chemical industries, and production facilities.

Keywords: automated process control systems (APCS), encryption, DLP systems, policies for data transmission channel control, security system.

Современные автоматизированные системы управления технологическими процессами представляют собой сложные программно-аппаратные комплексы, обеспечивающие мониторинг, управление и оптимизацию производственных процессов в режиме реального времени. В состав типовой АСУ ТП входят программируемые логические контроллеры (далее - ПЛК), человеко-машинные интерфейсы (Human-machine interface, далее - HMI), «диспетчерское управление и сбор данных» (Supervisory Control And Data Acquisition, далее - SCADA) системы, инженерные станции, серверы баз данных и сетевое оборудование.

В процессе функционирования АСУ ТП генерируются и обрабатываются различные категории данных, имеющих критическое значение для предприятия, утечка такой информации может привести к серьезным последствиям для предприятия: потере конкурентоспособности, финансовым убыткам, нарушению производственного процесса, техногенным авариям.

Интеграция АСУ ТП с корпоративными сетями существенно расширили возможности атак и повысили риски утечек конфиденциальной информации.

За последние годы количество кибератак на промышленные объекты выросло более чем на 200%, а ущерб от утечек данных исчисляется миллионами долларов для отдельных предприятий.

Согласно исследованию IBM Cost of a Data Breach Report 2023, средняя стоимость утечки данных в промышленном секторе составляет 4,45 млн долларов США. Для российских предприятий эта цифра варьируется от 30 до 150 млн рублей в зависимости от масштаба компании и критичности утраченной информации.

По данным Роскомнадзора и аналитиков ряда организаций 2024-2025 года характеризовались ростом числа инцидентов информационной безопасности в промышленном секторе, усилением требований регуляторов к защите критической информационной инфраструктуры, необходимостью обеспечения непрерывности технологических процессов при внедрении средств защиты, недостаточной изученностью вопросов интеграции систем прозрачного шифрования и систем предотвращения утечек данных (Data Loss Prevention, далее - DLP) в инфраструктуру АСУ ТП.

Анализ инцидентов информационной безопасности в промышленных системах показывает, что основными каналами утечки данных являются: несанкционированное копирование данных на внешние носители, передача данных через корпоративную почту, облачные хранилища, мессенджеры, а также по сетевым протоколам при подключении АСУ ТП к корпоративной сети.

В связи с этим основной задачей является исследование и разработка методов защиты информации для АСУ ТП, с использованием сквозного шифрования и средств предотвращения утечек данных, которая обеспечит защиту конфиденциальности данных АСУ ТП в состоянии хранения и передачи, контроль каналов передачи данных, минимальное влияние на производительность и функционирование технологических процессов, возможность интеграции с существующими системами безопасности предприятия.

Для решения поставленной задачи необходимо провести комплексное исследование технологий прозрачного шифрования и DLP-систем, выполнить их сравнительный анализ, разработать архитектуру интегрированной системы защиты и подготовить методические рекомендации по внедрению.

Традиционные средства защиты информации, разработанные для корпоративных IT-систем, зачастую не учитывают специфику АСУ ТП: требования к непрерывности процессов, ограниченные вычислительные ресурсы контроллеров, использование специализированных промышленных протоколов. Это создает необходимость разработки специализированных подходов к защите данных в промышленных системах управления.

На рынке представлены различные подходы к защите конфиденциальной информации в промышленных системах, которые можно классифицировать следующим образом:

Подход 1: Использование только периметровой защиты (межсетевые экраны, системы обнаружения вторжений). Данный подход основан на изоляции АСУ ТП от внешних сетей и контроле сетевого трафика на границах сегментов. Преимуществами являются минимальное влияние на производительность систем внутри защищаемого периметра, отсутствие необходимости установки агентов на конечные устройства, относительная простота развертывания. Основной недостаток – неэффективность против внутренних нарушителей, имеющих легитимный доступ к системам. Периметровая защита не может предотвратить утечку данных через USB-носители, печать документов, использование личных мобильных устройств для фотографирования экранов. Согласно отчету Ponemon Institute, стоимость инцидента утечки данных через инсайдеров в среднем на 30-40% выше, чем при внешних атаках, из-за сложности обнаружения и длительного времени компрометации;

Подход 2: Использование только DLP-систем без шифрования. DLP-системы обеспечивают контроль каналов передачи данных и могут блокировать попытки несанкционированной передачи конфиденциальной информации. Преимущества: обнаружение и предотвращение утечек в реальном времени, возможность анализа поведения пользователей, формирование детальных отчетов об инцидентах. Недостатки: данные остаются незащищенными в состоянии покоя, при физической компрометации носителей информация доступна в открытом виде, DLP не защищает от утечек при выводе из эксплуатации или передаче оборудования на ремонт;

Подход 3: Использование только прозрачного шифрования без DLP. Шифрование защищает данные в состоянии покоя, делает невозможным извлечение информации при физической компрометации носителей. Преимущества: высокий уровень защиты данных на дисках, автоматическое шифрование всех записываемых данных, соответствие требованиям регуляторов по защите конфиденциальной информации. Недостатки: не предотвращает утечки данных авторизованными пользователями через легитимные каналы, так как для пользователя, прошедшего аутентификацию, данные доступны в расшифрованном виде;

Подход 4 (предлагаемый): Комплексное использование прозрачного шифрования и DLP-систем. Интеграция двух технологий обеспечивает защиту на двух уровнях: шифрование защищает данные в состоянии покоя от несанкционированного доступа при физической компрометации, DLP контролирует действия авторизованных пользователей и предотвращает утечки через различные каналы передачи данных. Синергетический эффект заключается в том, что недостатки одной технологии компенсируются преимуществами другой.

Комплексный подход, несмотря на более высокую стоимость и сложность развертывания, обеспечивает наивысший уровень защиты, закрывая наибольшее количество векторов атак и сценариев утечек данных.

Предлагаемое решение превосходит альтернативные подходы по следующим критическим аспектам:

1) полнота защиты. Комплексный подход обеспечивает защиту на всех этапах жизненного цикла данных;

2) глубокая эшелонированная защита. При компрометации одного уровня защиты второй уровень продолжает функционировать;

3) соответствие регуляторным требованиям. Стандарты информационной безопасности промышленных систем ([1], [2]) требуют применения множественных уровней защиты. Российские регуляторы (ФСТЭК России, ФСБ России) предъявляют обязательные требования к шифрованию конфиденциальной информации на объектах критической информационной инфраструктуры. Комплексный подход обеспечивает выполнение всего спектра требований;

4) возможность детального аудита. Интеграция DLP и шифрования позволяет не только блокировать инциденты, но и фиксировать попытки утечек для последующего расследования, выявления скомпрометированных учетных записей, анализа паттернов поведения на-

рушителей. Это критически важно для соответствия требованиям по расследованию инцидентов информационной безопасности.

Методом проведения работы является анализ современных угроз информационной безопасности в АСУ ТП, сравнительный анализ существующих решений прозрачного шифрования и DLP-систем, моделирование архитектуры защищенной АСУ ТП, разработка методики интеграции средств защиты информации, тестирование производительности и эффективности предложенных решений, оценка соответствия требованиям стандартов информационной безопасности.

Потенциальный прямой экономический эффект от реализации решений комплексного подхода к защите информации существенно будет превышать как затраты на разработку комплекса нормативно-правовой документации, методического, программного и программно-технического обеспечения разработанной системы, так и дальнейшие прямые затраты на обеспечение ее функционирования.

Помимо прямых финансовых выгод, внедрение комплексной системы защиты информации обеспечивает ряд стратегических преимуществ:

- соответствие требованиям законодательства в области защиты критической информационной инфраструктуры;
- повышение инвестиционной привлекательности предприятия за счет демонстрации зрелости процессов ИБ;
- укрепление доверия партнеров и клиентов;
- возможность получения более выгодных условий страхования киберрисков;
- формирование культуры информационной безопасности в организации.

Проведенный анализ показывает экономическую целесообразность внедрения комплексной системы защиты информации на основе прозрачного шифрования и DLP-технологий в АСУ ТП промышленных предприятий. Несмотря на значительные первоначальные инвестиции проект обеспечивает снижение рисков утечки конфиденциальной информации на 75-85%, предотвращение потенциального ущерба в размере 7,5 млн рублей ежегодно, окупаемость инвестиций в течение 1,5-2 лет, положительный экономический эффект на протяжении всего жизненного цикла системы.

Библиографический список

1. IEC 62443 серия международных стандартов «Промышленные коммуникационные сети – Сетевая и системная безопасность»;
2. NIST SP 800-82 «Руководство по безопасности операционных технологий (ОТ)»;
3. Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
4. ГОСТ Р 34.12-2015: «Информационная технология. Криптографическая защита информации. Блочные шифры»;
5. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;
6. Банк данных угроз безопасности информации (информационное сообщение ФСТЭК России «О банке данных угроз безопасности информации» от 6 марта 2015 г. № 240/22/879);
7. Методический документ ФСТЭК от 05.02.2021 «Методика оценки угроз безопасности».

УДК 004.056; ГРНТИ 81.93.29

CTF: НАВЫКИ И НАПРАВЛЕНИЯ РАБОТ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ЗАЩИТЕ ИНФОРМАЦИИ

Р.О. Аколупин, М.С. Спирьянов, Ю.М. Кузьмин

Рязанский государственный радиотехнический университет имени В.Ф. Уткина,
Российская Федерация, Рязань, rastan13666@gmail.com, mish.goscha@yandex.ru, kuzmin_yurii@mail.ru

Аннотация. CTF (Capture The Flag) рассматривается как практико-ориентированная модель обучения защите информации: участник проходит путь от разведки и анализа входных данных до доказуемого получения результата и оформления write-up. Дана классификация направлений задач (web, pwn, reverse, crypto, forensics, OSINT, cloud/mobile, automation) и показано, какие навыки в каждом направлении обладают наибольшей переносимостью в прикладные роли (AppSec, pentest, SOC/DFIR, threat research). Предложена компактная шкала оценки ценности навыков по критериям переносимости, частоты применения, барьера входа и цены ошибки.

Ключевые слова: CTF, информационная безопасность, уязвимости, AppSec, DFIR, реверс-инжиниринг, криптография, OSINT, DevSecOps.

CTF: SKILLS AND WORK DIRECTIONS IN INFORMATION SYSTEMS AND INFORMATION SECURITY

R.O. Akolupin, M. S. Spiryanov, Y.M. Kuzmin

Ryazan State Radio Engineering University named after V.F. Utkin,
Russia, Ryazan, rastan13666@gmail.com, mish.goscha@yandex.ru, kuzmin_yurii@mail.ru

The summary. Capture The Flag (CTF) competitions are treated as a hands-on training model for information security. A participant moves from reconnaissance and input analysis to a reproducible result and a write-up. We classify common task tracks (web, pwn, reverse engineering, cryptography, forensics, OSINT, cloud/mobile, automation) and map them to applied roles (AppSec, pentesting, SOC/DFIR, threat research). A compact skill-value rubric is proposed using transferability, usage frequency, entry barrier, and error cost.

Keywords: CTF, information security, vulnerabilities, AppSec, DFIR, reverse engineering, cryptography, OSINT, DevSecOps.

Введение

Информационные системы объединяют программные компоненты, сети, пользователей и данные; нарушения защиты проявляются как утечки, подмена, простои и потеря управляемости. Практическая подготовка специалиста требует навыка переходить от симптома к механизму возникновения проблемы и к контролируемому исправлению.

CTF (Capture The Flag) дает формально проверяемую цель (флаг) и тренирует воспроизводимую цепочку действий. Ключевой результат для курса "Информационные системы и защита информации" - дисциплина разведки, проверка гипотез и инженерная автоматизация, которые переносимы в аудит, пентест и реагирование.

Таксономия направлений CTF и связь с прикладными ролями

На рисунке 1 показана карта соответствия направлений задач CTF и прикладных ролей в ИБ. Она позволяет планировать обучение по принципу "навык -> тип задач -> роль": например, web-задачи в первую очередь развивают AppSec и pentest, а forensics напрямую конвертируется в SOC/DFIR.

Форматы CTF и типовые артефакты задач

Основные форматы: Jeopardy (набор независимых задач), Attack-Defense (защита своего сервиса и атака чужих) и смешанные соревнования. Attack-Defense особенно полезен для понимания жизненного цикла уязвимости: одна и та же ошибка влияет на доступность, целостность и конфиденциальность, а исправление должно выдерживать агрессивный трафик и

попытки обхода. Артефакты имитируют реальные источники данных: исходный код, бинарные файлы, сетевые дампы (pcap), журналы событий, конфигурации, контейнеры и образы дисков. Обязательное условие учебной ценности - работа только в санкционированной лабораторной среде.

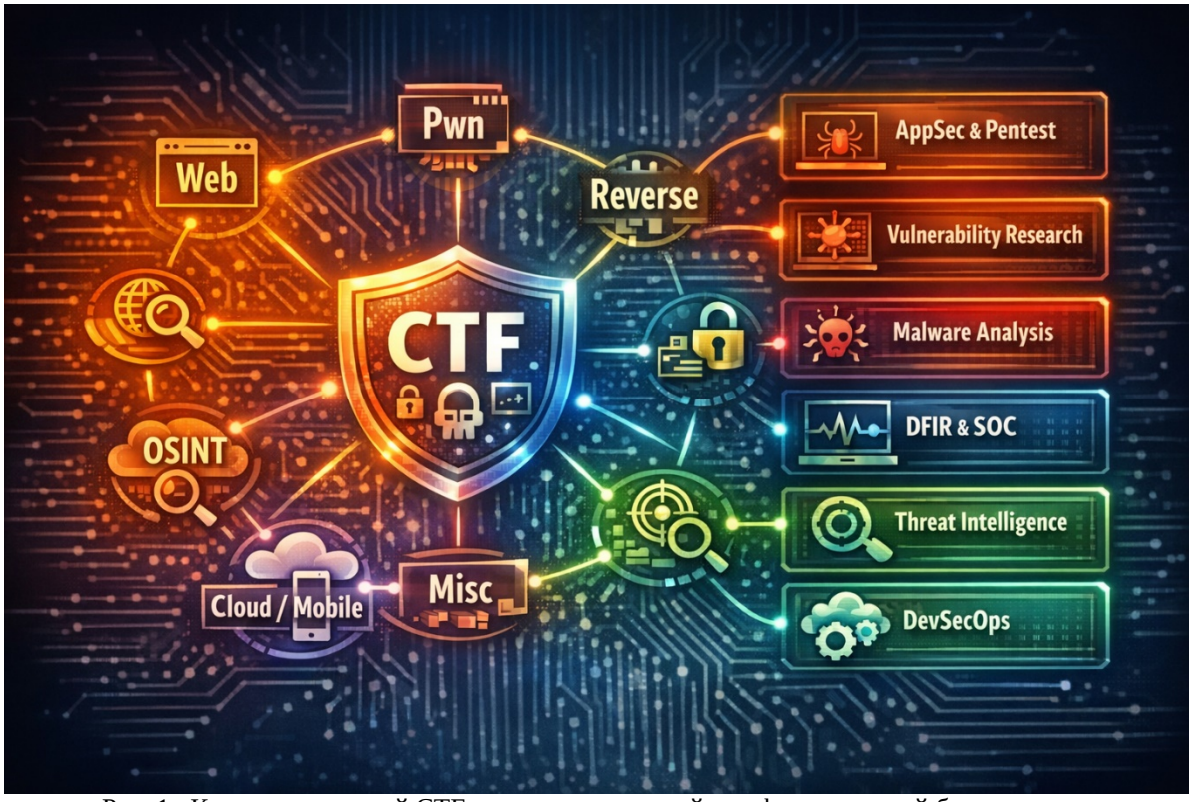


Рис. 1. Карта направлений CTF и прикладных ролей в информационной безопасности

Направления задач и практическая ценность навыков

Таблица 1 суммирует связь направления, ключевых навыков, типовых артефактов и прикладных ролей. Сводка удобна при распределении ролей в команде и выборе персональной специализации.

Таблица 1. Соответствие направлений CTF, артефактов и прикладных ролей

Направление	Фокус навыков	Типовые артефакты	Роли/задачи
Web	HTTP, сессии, авторизация, инъекции, бизнес-логика	код, запросы/ответы, конфиги	AppSec, pentest, code review
Forensics	таймлайны, логи, pcap, восстановление артефактов	pcap, образы, журналы	SOC/DFIR, расследования
Reverse	анализ бинарей, протоколов, обфускации, патчинг	exe/elf, дампы, плагины	malware analysis, threat research
Pwn	память, mitigations, ROP, эксплуатация ошибок	сервис/бинарь, libc, docker	vuln research, exploit dev
Crypto	протоколы, ошибки реализации, случайность, подписи	скрипты, параметры, дампы	security engineering, аудит
OSINT	поиск/верификация, корреляция, граф связей	публичные данные, метаданные	threat intel, аналитика
Cloud/Mobile	IAM, секреты, контейнеры, клиентская безопасность	policy, images, APK/IPA	cloud security, DevSecOps
Automation/Misc	скрипты, парсинг, пайплайны, стего	разнородные файлы	ускорение анализа во всех ролях

Конвейер решения CTF-задачи и минимальная методика оценивания навыков

CTF проверяет воспроизводимый конвейер: разведка -> гипотезы -> проверка -> автоматизация -> валидация -> write-up. Write-up фиксирует входные условия, причину уязвимости, шаги получения результата и идею исправления; в прикладной работе это эквивалентно отчету и регрессионным тестам.

На рисунке 2 ниже показан конвейер решения CTF-задач.

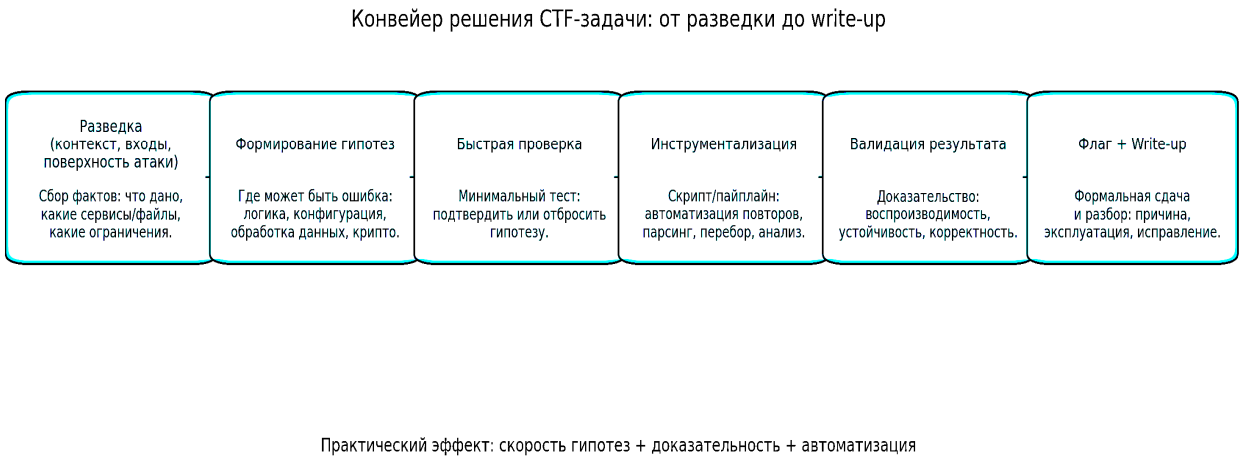


Рис. 2. Конвейер решения CTF-задачи: от разведки до write-up

Ключевые направления: что именно стоит изучать

Web

Ценный минимум: модель авторизации (проверка прав на каждом действии), безопасная обработка ввода и понимание бизнес-процессов. Наиболее значимые классы ошибок: IDOR/обход ролей, инъекции, SSRF и нарушения доверия при отображении данных (XSS). Практический критерий: воспроизводимость, оценка влияния и предложение исправления (проверка прав, валидация, журналирование).

Forensics

Ценный минимум: построение таймлайна и доказательность вывода через несколько независимых артефактов. Типовые кейсы: восстановление цепочки действий по pcap и логам, поиск точки входа и пути вывода данных, анализ метаданных файлов. Переносимость максимальна для SOC/DFIR.

Reverse Engineering

Ценный минимум: восстановление логики из бинаря/байткода и понимание форматов/протоколов. Прикладная конвертация: анализ вредоносного ПО и сторонних компонент, выявление скрытых проверок и извлечение индикаторов. Индикатор компетенции: быстрый поиск ключевых функций и написание декодера/патча.

Pwn

Ценный минимум: модель памяти и защит (ASLR, NX, PIE, canary), triage уязвимостей и оценка контролируемости. Полный exploit-dev требует времени, но даже базовый уровень дает пользу: локализация класса ошибки, воспроизведение и понимание условий эксплуатации.

Crypto

В задачах чаще ломают реализацию: повтор nonce, слабая случайность, неверная проверка подписи, ошибки кодирования, протокольные упрощения. Ценный минимум: модель

угроз и требования к схеме (конфиденциальность, целостность, доступность). Цена ошибки высокая: утечка ключа обычно необратима.

OSINT

Ценный минимум: системный поиск, верификация источников и корреляция сущностей (аккаунты, домены, метаданные, временные связки). Правило качества: вывод формируется только при наличии независимых подтверждений, иначе возрастает риск ложной атрибуции.

Cloud/Mobile/Hardware

Критичные темы: права и конфигурации (IAM), утечки секретов, контейнерные образы и цепочки доставки, безопасность API для мобильных клиентов. Переносимость высокая для DevSecOps: least privilege, секрет-менеджмент, логирование и проверка политик.

Automation/Misc

Сквозной навык: построение инструментов и пайплайнов (парсинг, перебор, нормализация логов, извлечение артефактов). Он повышает скорость решения задач и снижает человеческие ошибки; поэтому ценен для всех специализаций.

Интересные моменты CTF, которые дают образовательный эффект

- Дисциплина разведки: сначала карта поверхности, затем гипотезы и минимальные тесты.
- Командная специализация: разделение ролей ускоряет решение и имитирует работу SOC/red team.
- Инструментальное мышление: повторяемость достигается скриптом, а не ручными действиями.
- Write-up как аудит: причина -> эксплуатация -> рекомендации -> проверка исправления.
- Этика: атакующее мышление тренируется только в разрешенной среде.

Заключение

CTF обеспечивает измеримую практику для курса по защите информации: формируется конвейер анализа, доказательности и документирования. Для старта наиболее полезны Web, Forensics, Reverse и Pwn повышают уникальность профиля при большем барьере входа; Crypto и Hardware критичны из-за высокой цены ошибок реализации и конфигурации.

Библиографический список

1. CTFtime.org. What is Capture The Flag? URL: https://ctftime.org/ctf-wtf (дата обращения: 23.02.2026).
2. OWASP. OWASP Top Ten Web Application Security Risks (версия 2025). URL: https://owasp.org/www-project-top-ten/ (дата обращения: 23.02.2026).
3. NIST. SP 800-61 Rev. 3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. 2025. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (дата обращения: 23.02.2026).
4. MITRE. MITRE ATT&CK(R) Knowledge Base. URL: https://attack.mitre.org/ (дата обращения: 23.02.2026).
5. Carnegie Mellon University. picoCTF. URL: https://picoctf.org/ (дата обращения: 23.02.2026).
6. OverTheWire. Wargames. URL: https://overthewire.org/ (дата обращения: 23.02.2026).
7. Sutton M., Greene A., Amini P. Fuzzing: Brute Force Vulnerability Discovery. Addison-Wesley, 2007.
8. Anderson R. Security Engineering. 3rd ed. Wiley, 2020.
9. Microsoft. STRIDE Threat Model (концепция моделирования угроз).
10. Nelson A. et al. NIST SP 800-61 Rev. 3 (официальная публикация NIST, 2025).

УДК 004.056.; ГРНТИ 50.03.05

АНАЛИЗ УГРОЗ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Н.В. Ларин, А.Ю. Мельник, В.О. Прохоров, А.А. Бубнов
Рязанский государственный радиотехнический университет имени В.Ф. Уткина, Российская Федерация, Рязань, nikita.larin_2019_20@mail.ru

Аннотация. В работе рассматриваются актуальные проблемы обеспечения кибербезопасности критической информационной инфраструктуры (КИИ) Российской Федерации. Приводятся основные понятия, нормативная база и принципы построения системы защиты. На основе документов ФСТЭК России предпринята попытка систематизации угроз безопасности информации, актуальных для объектов КИИ. Рассмотрены основные классы угроз: внешние кибератаки, внутренние нарушения и технические сбои. Более подробно проанализированы угрозы, связанные с несанкционированным доступом и вредоносным программным обеспечением. Остальные виды угроз рассмотрены в контексте их влияния на доступность и целостность данных. Дана оценка важности защиты КИИ для национальной безопасности страны.
Ключевые слова: критическая информационная инфраструктура (КИИ), ФСТЭК России, модель угроз, информационная безопасность, систематизация угроз, 187-ФЗ, защита информации.

ANALYSIS OF CYBERSECURITY THREATS TO CRITICAL INFORMATION INFRASTRUCTURE

N.V. Larin, A.Yu. Melnik, V.O. Prokhorov, A.A. Bubnov
Ryazan State Radio Engineering University named after V.F. Utkin, Russia, Ryazan, nikita.larin_2019_20@mail.ru

The summary. The paper discusses current issues related to ensuring the cybersecurity of the critical information infrastructure (CII) of the Russian Federation. It provides the basic concepts, regulatory framework, and principles for building a protection system. Based on the documents of the Federal Service for Technical and Export Control of the Russian Federation, an attempt is made to systematize the information security threats relevant to CII facilities. The main classes of threats are considered, including external cyberattacks, internal violations, and technical failures. The paper provides a detailed analysis of threats related to unauthorized access and malicious software. Other types of threats are considered in the context of their impact on data availability and integrity. The importance of protecting CII for the country's national security is assessed.
Keywords: critical information infrastructure (CII), FSTEC of Russia, threat model, information security, threat systematization, 187-FZ, information protection.

Одной из главных проблем современного цифрового общества является обеспечение устойчивости и безопасности систем, от которых зависит жизнедеятельность государства. К таким системам относится критическая информационная инфраструктура (КИИ). Под КИИ понимаются информационные системы, сети связи и автоматизированные системы управления, которые принадлежат субъектам критической инфраструктуры (например, энергетика, транспорт, здравоохранение, финансы, связь) и нарушение или прекращение функционирования которых может привести к тяжелым последствиям. Выбор методов и средств защиты зависит от категории значимости объекта, которая определяется в соответствии с законодательством. Качество защиты информации, поступающей, обрабатываемой и хранящейся в таких системах, определяется и зависит от ряда факторов, которые будут влиять на выявление, предотвращение и ликвидацию инцидентов. Среда функционирования КИИ является сложной и неоднородной. При этом в инфраструктуре будут наблюдаться различные мешающие безопасному функционированию факторы: действия злоумышленников, ошибки персонала, технические отказы. Наиболее перспективным методом обеспечения безопасности является построение комплексной системы защиты информации (СЗИ) на основе актуальной модели угроз. Использование документов ФСТЭК России для построения СЗИ позволяет стандартизировать подход и значительно повысить уровень защищенности. В данной

статье будут рассмотрены различные классы угроз и предпринята попытка их систематизации для упрощения понимания проблематики.

Нормативная база и важность защиты КИИ

Основой для регулирования вопросов безопасности КИИ в России является Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон устанавливает правовые основы обеспечения безопасности КИИ при ее функционировании. Однако сам закон задает лишь общие рамки. Конкретные методики, требования и подходы разрабатываются уполномоченным органом – ФСТЭК России (Федеральная служба по техническому и экспортному контролю).

Важность защиты КИИ невозможно переоценить. В современном мире информационные технологии пронизывают все сферы жизни. Отключение системы управления электросетью в крупном регионе может парализовать транспорт, остановить заводы и оставить людей без света и тепла. Атака на банковскую инфраструктуру может привести к потере сбережений граждан и дестабилизации экономики. Кибератаки на медицинские учреждения могут поставить под угрозу жизнь пациентов, если откажет оборудование или станут недоступны базы данных.

Таким образом, защита КИИ – это не просто техническая задача для системных администраторов, а вопрос национальной безопасности. Государство заинтересовано в том, чтобы даже в условиях внешнего давления или внутренних сбоев ключевые системы продолжали работать. Именно поэтому ФСТЭК России выпускает ряд приказов, которые обязательны для исполнения субъектами КИИ. Среди них ключевыми являются: – Приказ ФСТЭК России от 25.12.2017 № 239 (утверждает требования по обеспечению безопасности значимых объектов КИИ); – Приказ ФСТЭК России от 14.03.2014 № 31 (утверждает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных, часто используемый как база для моделирования угроз); – Методические документы ФСТЭК по построению моделей угроз безопасности информации.

Попытка систематизации угроз безопасности КИИ

В данной работе предпринята попытка систематизации угроз, опираясь на требования ФСТЭК, но излагая их простым языком для лучшего понимания сути проблем. В нормативных документах угрозы часто описываются сложным техническим языком. Для практического применения удобно разделить их на несколько крупных групп по источнику возникновения и способу воздействия.

В общей модели угроз безопасности информации можно выделить три основных класса:

1. Угрозы, связанные с внешним воздействием (кибератаки).
2. Угрозы, связанные с внутренним фактором (персонал и процессы).
3. Угрозы, связанные с техническими сбоями и средой функционирования.

Внешние кибератаки

Это наиболее обсуждаемая группа угроз. Под внешним воздействием понимается деятельность злоумышленников, не имеющих легального доступа к системе, но пытающихся его получить или нарушить работу системы извне.

Несанкционированный доступ (НСД). Это классическая угроза, когда злоумышленник пытается войти в систему под чужим именем. Это может быть сделано путем подбора паролей, использования украденных учетных данных или эксплуатации уязвимостей в программном обеспечении. Для КИИ опасность НСД заключается в том, что получив доступ, зло-

умышленник может изменить настройки оборудования, похитить данные или заложить «мину замедленного действия».

Вредоносное программное обеспечение (ВПО). Сюда относятся вирусы, черви, трояны и, что наиболее опасно для КИИ, программы-шифровальщики (вымогатели). Особенность угроз для КИИ в том, что здесь часто используется целевое вредоносное ПО, созданное специально для промышленного оборудования (например, черви типа Stuxnet или Industroyer). Такое ПО умеет работать со специфическими протоколами управления технологическими процессами. Если в обычном офисе вирус просто зашифрует файлы, то в системе КИИ он может физически вывести из строя турбину или изменить давление в трубопроводе.

Сетевые атаки (DoS/DDoS). Атаки типа «Отказ в обслуживании» направлены не на кражу данных, а на то, чтобы сделать сервис недоступным. Для КИИ доступность является одним из главных параметров безопасности. Если система управления движением поездов не ответит на запрос в нужный момент, это может привести к аварии. DDoS-атаки часто используются как отвлекающий маневр, пока хакеры проникают в сеть через другой канал.

Межсетевое взаимодействие. Угрозы могут проникать из смежных сетей. Например, сеть предприятия КИИ может быть связана с сетью интернета для обновления ПО или с сетью подрядчиков. Если защита на границе этих сетей слабая, угроза легко мигрирует внутрь защищаемого периметра. ФСТЭК требует обязательного использования средств межсетевого экранирования для разделения сетей разного уровня доверия.

Внутренние угрозы и человеческий фактор

Статистика показывает, что значительная часть инцидентов происходит не из-за хакерских атак, а из-за ошибок или действий сотрудников.

Ошибки персонала. Системные администраторы или операторы технологических процессов могут случайно ввести неверную команду, удалить важный файл или неправильно настроить оборудование. В сложных системах КИИ цена такой ошибки крайне высока. Часто это происходит из-за недостаточной квалификации или усталости.

Действия инсайдеров. Это умышленные действия сотрудников, имеющих легальный доступ. Мотивом может быть месть работодателю, финансовая выгода (продажа данных) или вербовка внешними спецслужбами. Инсайдер опасен тем, что он знает структуру защиты и имеет законные права доступа. Обнаружить такие действия сложнее, чем внешнюю атаку, так они не всегда выглядят как нарушение правил.

Нарушение регламентов. Даже если технические средства защиты установлены, они могут не работать, если персонал не соблюдает правила. Например, подключение личного ноутбука к служебной сети, использование слабых паролей, запись паролей на стикерах. ФСТЭК в своих требованиях делает большой акцент на организационные меры: инструктажи, журналы учета, разграничение прав доступа.

Технические сбои и среда функционирования

Эта группа угроз часто недооценивается, но для КИИ она критична.

Отказы оборудования. Любое «железо» имеет срок службы. Серверы, маршрутизаторы, датчики могут выйти из строя. Для КИИ требуется обеспечение отказоустойчивости (резервирование каналов связи, дублирование серверов). Угрозой здесь является отсутствие резерва или его неготовность к включению.

Программные ошибки (баги). В программном обеспечении, особенно в зарубежном, могут быть скрытые ошибки или недекларированные возможности. В условиях импортозамещения актуальной угрозой становится использование ПО, которое может быть отключено производителем удаленно или содержать закладки.

Физические воздействия. Пожары, наводнения, перебои с электропитанием. Информационная инфраструктура не существует в вакууме. Если в дата-центре отключится кондиционирование, серверы перегреются и отключатся. Если пропадет электричество, системы встанут. Поэтому защита КИИ включает в себя и физическую охрану объектов, и системы бесперебойного питания.

Сравнительная характеристика и приоритеты

При анализе угроз для КИИ важно понимать, что не все угрозы равнозначны. В обычных коммерческих системах на первое место часто выходит конфиденциальность (чтобы не украли секреты). В КИИ на первое место выходят целостность (чтобы данные не были изменены) и доступность (чтобы система работала всегда).

Например, спам атака на информационные ресурсы неприятна, но не катастрофична. А вот изменение сигнала светофора или стрелки на путях – это катастрофа. Поэтому при систематизации угроз для КИИ приоритет отдается тем сценариям, которые ведут к нарушению технологического процесса.

ФСТЭК России в Приказе № 239 требует, чтобы меры защиты соответствовали классу защищенности объекта. Это означает, что нельзя защищать все объекты одинаково. Для объекта первой категории (наиболее значимого) требования максимальны: обязательное использование отечественных средств защиты, сертифицированных ФСТЭК, постоянный мониторинг инцидентов (подключение в ГосСОПКА). Для менее значимых объектов требования мягче. Это позволяет распределить ресурсы эффективно.

Важным аспектом является актуализация модели угроз. Мир меняется, появляются новые виды атак. То, что было безопасно пять лет назад, сегодня может быть уязвимо. Поэтому систематизация угроз – это не разовая работа, а непрерывный процесс. Субъект КИИ должен регулярно пересматривать свои риски.

Выводы

В ходе работы был проведен анализ угроз кибербезопасности критической информационной инфраструктуры. На основе изучения документов ФСТЭК России и Федерального закона № 187-ФЗ можно сделать следующие выводы.

Во-первых, защита КИИ является стратегически важной задачей для обеспечения суверенитета и стабильности Российской Федерации. Последствия успешных кибератак на объекты КИИ могут носить не только экономический, но и гуманитарный характер.

Во-вторых, предложенная систематизация угроз на три класса (внешние, внутренние, технические) позволяет упростить процесс построения модели угроз. Такое разделение помогает специалистам по безопасности не упустить важные аспекты, сосредотачиваясь не только на хакерах, но и на ошибках персонала и надежности оборудования.

В-третьих, соблюдение требований ФСТЭК России является необходимым минимумом. Однако формальное выполнение требований без понимания реальных рисков не гарантирует безопасности. Необходим комплексный подход, включающий технические средства защиты, организационные меры и постоянный контроль.

Перспективным направлением развития является внедрение систем мониторинга и реагирования на компьютерные инциденты (SOC), а также переход на отечественное программное и аппаратное обеспечение, что снижает риски наличия закладок и зависимости от иностранных производителей. Дальнейшие исследования могут быть направлены на разработку автоматизированных методов оценки актуальности угроз в реальном времени.

Библиографический список

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

3. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Методические рекомендации ФСТЭК России по построению модели угроз безопасности информации. – М., 2020.

5. Григорьев В. А., Мельников В. В. Безопасность информационных технологий. Системный подход. – Москва: Горячая линия – Телеком, 2019.

6. Девянин П. Н. Модели безопасности компьютерных систем. – Москва: Академия, 2018.

7. Информационная безопасность: учебник для вузов / под ред. В. А. Галатенко. – 3-е изд. – Москва: ИНФРА-М, 2021.

СОДЕРЖАНИЕ

ИНФОРМАЦИЯ О IX МЕЖДУНАРОДНОМ ФОРУМЕ «СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ» СТНО-2026»……. 3

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ. РАДИОТЕХНИКА И ЭЛЕКТРОНИКА»..... 6

Секция «ЦИФРОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РЕАЛЬНОГО ВРЕМЕНИ»..... 6

Кудимов Н.О. Практическая реализация БПФ на ПЛИС: добавление алгоритма ЦОС в проект сбора данных..... 6

Алексашин А.А., Волченков В.А. Моделирование многоскоростных структур узкополосных КИХ-фильтров в среде SIMINTECH..... 10

Виноградов Н.С. Сравнение использования алгоритмов OSD и ORBGRAND для декодирования кодов BCH..... 15

Литвинова В.С., Волченков В.А. Исследование возможностей среды SIMINTECH по моделированию электрических цепей постоянного тока..... 19

Елисеев М.В., Линович А.Ю. Разработка модели приёмника ЛЧМ-сигналов с адаптивной компенсацией помех в среде MATLAB для изучения алгоритмов цифровой обработки сигналов..... 23

Плющиков В.С., Бакке А.В. Применение нейросетевых архитектур для адаптации радиоканала к помеховой обстановке..... 26

Сивов Н.Д., Волченков В.А. Разработка модели синхронизации средств связи в отечественной среде математического моделирования SIMINTECH..... 31

Фетисова Л.А., Волченков В.А. Разработка модели формирования аналогового и дискретного сигналов в среде математического моделирования SIMINTECH для изучения их характеристик обучающимися..... 37

Заря А.С., Волченков В.А. Исследование возможностей проектирования компонентов телекоммуникационных устройств в различных средах математического моделирования..... 44

Королев Д.С., Волченков В.А. Обзор и анализ способов распознавания речевых сигналов с использованием нейросетей..... 51

Филимонова М.О., Витязев С.В. Оценка вычислительной эффективности графического процессора в реализации обученной нейросети при анализе GPR-изображений..... 58

Секция «АКТУАЛЬНЫЕ ЗАДАЧИ ХИМИЧЕСКИХ ТЕХНОЛОГИЙ»..... 64

Юдаев С.А., Алтабаев Е.В. Исследование влияния содержания оксида активных металлов в катализаторе на эффективность процесса окисления биодизельного топлива…. 64

Храпова Е.Ю., Мельник Г.И. Функциональные наполнители и модификаторы в рецептурах полимерных мембран на основе ПВХ..... 67

Шашкина Г.А., Кулавина Н.Ю., Медведева В.В. Синтез схемы разделения смеси пентан - гексан - гептан..... 71

Лызлова М.В., Шанин А.А., Куценко Э.В., Гоголицына М.С., Киселёв А.В., Мельник Г.И. Исследование химического состава дренажной воды из сепараторов бензина установок АТ..... 76

Ветшева А.Д., Дубков М.В. Моделирование фрагментации ионов в тандемном квадрупольном масс-спектрометре при работе во второй зоне диаграммы стабильности..... 82

Родионова О.А., Ветшева А.Д. Исследование коррозионной стойкости цинковых покрытий..... 86

Дубков М.В., Ветшев К.А. Исследование влияния параметров входной апертуры на аналитические характеристики трипольного масс-анализатора..... 90

Ветшев К.А., Максимов В.В., Онофраш Г.Д. Доступная спектроскопия: анализ современных конструкторских решений для создания малобюджетных портативных спектрометров..... 94

Воробьева Е.В., Медведева В.В. Исследование возможности очистки моделей сточных вод нефтеперерабатывающих предприятий методом пневматической сепарации..... 97

Воробьева Е.В., Агаршева Ю.С. Производство дополнительного высокооктанового компонента автомобиильного бензина в период дефицита толуола..... 101

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ. ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ»..... 106

Секция «МОДЕЛИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В САПР»..... 106

Бакулева М.А. Разработка программного модуля автоматизированной оценки качества на основе интеллектуальной системы распознавания дефектов..... 106

Кошелева М.С., Орешков В.И. Проблема деградации интеллектуальных цифровых двойников и пути ее решения..... 109

Боцман Т.Р., Бакулев А.В. Применение нейросетевых инструментов в радиолокации…. 113

Секция «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В КОНСТРУИРОВАНИИ ЭЛЕКТРОННЫХ СРЕДСТВ»..... 118

Скворцов С.В., Хрюкин В.И. Анализ влияния цифровой обработки сигналов на устойчивость системы с переменной структурой..... 118

Сапрыкин А.Н., Тихонов А.А. Архитектурные особенности параллельного генетического алгоритма многокритериальной QOS-маршрутизации в программно-конфигурируемых сетях..... 122

Бурцева С.Н. Разработка модульной системы распознавания речи с поддержкой диаризации и дообучения модели на базе VOSK..... 127

Сапрыкин А.Н. Архитектурные решения и методы синтеза конечных автоматов на VHDL в базисе ПЛИС..... 132

Костяева А.М. Алгоритмы и интерфейсные подходы к размещению компонентов в современных сапр проектирования печатных плат..... 138

Лейбович К.И. Обзор современных методов измерения частоты: от прямого счёта до цифровой обработки..... 142

Лейбович К.И., Тобратов Ю.М. Сравнительный анализ методов повышения точности измерения емкости конденсаторов..... 146

Морозов С.В., Шаганов Е.М. Разработка встроенного программного обеспечения устройства коммуникационного преобразования сетевых протоколов интернета вещей..... 150

Секция «ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ В ОБРАЗОВАНИИ»..... 153

Махмутходжаева Л.С. Национальные особенности цифровизации образования: опыт республики Узбекистан..... 153

Кострова Ю.С. Сравнительный анализ эффективности систем детекции ИИ-контента в образовательной среде..... 159

Малая О.П. Использование искусственного интеллекта в тренировках профессиональных навыков начинающих психологов..... 162

Федулов М.А. Возможности использования технологий искусственного интеллекта в образовании..... 166

Семыкина В.Н., Шефер О.Р. Возможности использования нейросети DEEPSEEK учителем на уроках физики..... 172

Кадырова Э.А., Севастьянов А.В. Искусственный интеллект в культуре и образовании: от теории к практике (чего нам ожидать и чего опасаться) 177

Секция «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ЗАЩИТА ИНФОРМАЦИИ»..... 191

Стенин А.С. Исследование методов восстановления удаленных и поврежденных данных в различных файловых системах..... 191

Ни В.В., Мещеряков В.А. Архитектура изолированного стенда для проведения сертификационных испытаний..... 194

Филимонов С.А. Разработка образовательной платформы на базе микросервисной DLP-системы для подготовки специалистов по кибербезопасности..... 200

Кузьмин Ю.М. Уточнение понятия «Безопасное ПО» для разработки и выбора мер защиты ПО..... 205

Конкин Ю.В. Анализ возможностей языка UML для моделирования сценариев реализации угроз безопасности информации..... 209

Спирьянов М.С., Кузьмин Ю.М. OSINT-разведка: как осуществляется и на чем основывается.....214

Семочкина О.С., Вилкова С.А., Кузьмин Ю.М. Перспективы использования Искусственного интеллекта в кибербезопасности образовательных платформ..... 218

Колесенков Н.А., Дедов В.О., Дергачева А.В. Таргетированные компьютерные атаки на ресурсы корпоративных систем и их особенности..... 223

Колесенков Н.А., Любакова А.Р., Макушева А.Р. Обеспечение информационной безопасности государственных информационных систем в соответствии с изменениями требований по защите инфомации..... 227

Милованов Г.А., Калинкина Т.И. Применение прозрачного шифрования и анализа DLP-систем для предотвращения утечек данных в АСУ ТП..... 231

Аколупин Р.О., Спирьянов М.С., Кузьмин Ю.М. CTF: навыки и направления работ в информационных системах и защите информации..... 235

Ларин Н.В., Мельник А.Ю., Прохоров В.О., Бубнов А.А. Анализ угроз кибербезопасности критической информационной инфраструктуры..... 239

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ОБРАЗОВАНИИ – СТНО-2026

Научное издание

В 11 томах

Том 3

Под общей редакцией О.В. Миловзорова.

Подписано в печать 15.06.26. Формат 60x84 1/8.
Бумага офсетная. Печать офсетная.
Гарнитура «Times New Roman».
Усл. печ. л..
Тираж 100 экз. Заказ №.

Рязанский государственный радиотехнический университет,
Редакционно-издательский центр РГРТУ,
390005, г. Рязань, ул. Гагарина, д. 59/1.

ISBN 978-5-7722-0446-7

