№3-2025

ISSN 1999-9429

Известия ЮФУ

Технические науки

- Кибератаки и их обнаружение
- Методы защиты и технологии безопасности
- Криптографические системы и шифрование
- Машинное обучение и обработка данных
- Моделирование и управление рисками

ИЗВЕСТИЯ ЮФУ. ТЕХНИЧЕСКИЕ НАУКИ
IZVESTIYA SFedU. ENGINEERING SCIENCES

Свидетельство о регистрации средства массовой информации
ПИ № ФС77-28889 от 12.07.2007
Федеральная служба по надзору в сфере массовых коммуникаций, связи
и охраны культурного наследия
Научно-технический и прикладной журнал
Издается с 1995 года, до середины 2007 года под названием «Известия ТРТУ»
Подписной индекс ПС704

№ 3 (245). 2025 г.

Журнал включен в «Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук».

Учредитель Южный федеральный университет.
Издатель Южный федеральный университет.
Ответственный за выпуск Ищукова Е.А.
Технический редактор Ярошевич Н.В.
Оригинал-макет выполнен Ярошевич Н.В.

Дата выхода в свет 30.06. 2025 г. Формат $70\times108\ {}^{1}\!/_{16}$. Бумага офсетная.

Офсетная печать. Усл. печ. л. – 25,8. Уч.-изд. л. – 19,5.
Заказ № 10035. Тираж 250 экз.

Адрес издателя: 344090, г. Ростов-на-Дону, пр. Стачки, 200/1, тел. 8(863)243-41-66.

Адрес типографии: Отпечатано в отделе полиграфической, корпоративной и сувенирной продукции Издательско-полиграфического комплекса КИБИ МЕДИА ЦЕНТРА ЮФУ. 344090, г. Ростов-на-Дону, пр. Стачки, 200/1, тел. 8(863)243-41-66.

Адрес редакции: 347922, г. Таганрог, ул. Чехова, 22, ЮФУ, тел. +7 (928) 909-57-82, e-mail: iborodyanskiy@sfedu.ru, http://izv-tn.tti.sfedu.ru/.

16+ Цена свободная

ISSN 1999-9429 (Print)
ISSN 2311-3103 (Online)

СОДЕРЖАНИЕ

РАЗДЕЛ I. КИБЕРАТАКИ И ИХ ОБНАРУЖЕНИЕ

РАЗДЕЛ II. МЕТОДЫ ЗАЩИТЫ И ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

РАЗДЕЛ III. КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ШИФРОВАНИЕ

РАЗДЕЛ IV. МАШИННОЕ ОБУЧЕНИЕ И ОБРАБОТКА ДАННЫХ

CONTENT

SECTION I. CYBERATTACKS AND THEIR DETECTION

SECTION II. METHODS OF PROTECTION AND SECURITY TECHNOLOGIES

SECTION III. CRYPTOGRAPHIC SYSTEMS AND ENCRYPTION

SECTION IV. MACHINE LEARNING AND DATA PROCESSING

Раздел I. Кибератаки и их обнаружение

УДК 004.056 DOI 10.18522/2311-3103-2025-3-6-16

А.В. Балыбердин

МУЛЬТИМОДАЛЬНЫЙ МЕТОД ИЗВЛЕЧЕНИЯ ПРИЗНАКОВ ДАННЫХ ДЛЯ КЛАССИФИКАЦИИ СЕТЕВЫХ АТАК

Система обнаружения вторжений (СОВ) является важным компонентом защиты корпоративной сети передачи данных (КСПД). СОВ анализирует сетевой трафик и выявляет сетевые атаки. В зависимости от методов детектирования, СОВ можно классифицировать на следующие виды систем: система сигнатурного анализа, система обнаружения аномалий (СОА) и гибридная система, объединяющая ранее рассмотренные системы. В последнее время активно развиваются системы обнаружения аномалий (СОВ). Для систем обнаружения аномалий сетевые атаки представляют собой аномальное поведение сетевого трафика, состоящего из набора признаков или атрибутов событий. Современные СОВ опираются на методы машинного и глубокого обучения, в связи с чем обнаружение сетевых атак и аномалий формулируется как задача классификации и кластеризации. Для решения данных задач необходимы методы оптимизации признакового пространства сетевого трафика. Целью работы является разработка метода извлечения признаков на основе мультимодального подхода представления данных сетевого трафика для классификации сетевых атак. В работе рассмотрен анализ релевантных исследований по методам извлечения признаков из различных областей. Задача исследования – повысить эффективность классификации с помощью метода мультимодального представления признаков сетевого трафика. Результатом работы является метод извлечения признаков данных на основе двух модальностей: спектрального представления признаков сетевого трафика и матрицы признаков изображений. Новизна представленного метода заключается в применении метода оконного преобразования Фурье для событий сетевого трафика, с последующим вычислением спектральных признаков для дискретных сигналов, а также преобразованием признаков данных в матрицу изображений и её расширением для оптимизации пространства признаков с помощью сверточной нейронной сети (convolutional neural network, CNN). Оценка мультимодального метода показала, что данный метод повысил точность классификации для несбалансированных классов сетевых атак.

Система обнаружения вторжений; корпоративная сеть передачи данных; набор признаков; извлечение признаков; мультимодальность; сверточная нейронная сеть; задача классификации и кластеризации; признаковое пространство; сетевые атаки.

A.V. Balyberdin

MULTIMODAL DATA FEATURE EXTRACTION METHOD FOR NETWORK ATTACK CLASSIFICATION

An intrusion detection system (IDS) is an important component of corporate data network (CDN) protection. IDS analyzes network traffic and detects network attacks. Depending on the detection methods, IDS can be classified into the following types of systems: signature-based analysis systems, anomaly detection systems (ADS), and hybrid systems combining the aforementioned approaches. Recently, anomaly detection systems (IDS) have been actively developing. For anomaly detection systems, network attacks are anomalous behavior of network traffic consisting of a set of features or event attributes. Modern IDS are based on machine and deep learning methods, and therefore the detection of network attacks and anomalies is formulated as a classification and clustering problem. To solve these problems, methods for optimizing the feature space of network traffic are required. The aim of the work is to develop a feature extraction method based on a multimodal approach to representing network traffic data for classifying network attacks. The paper considers the analysis of relevant studies on feature extraction methods from various fields. The objective of the study is to improve classification efficiency using a multimodal repre-

sentation of network traffic features. The result of the work is a method for extracting data features based on two modalities: a spectral representation of network traffic features and an image feature matrix. The novelty of the presented method lies in the application of the windowed Fourier transform method for network traffic events, followed by the calculation of spectral features for discrete signals, as well as the transformation of data features into an image matrix and its expansion to optimize the feature space using a convolutional neural network (CNN). Evaluation of the multimodal method showed that this method increased the classification accuracy for unbalanced classes of network attacks.

Intrusion detection system; enterprise data network; feature set; feature extraction; multimodality; convolutional neural network; classification and clustering problem; feature space; network attacks.

Введение. В настоящее время особое внимание уделяется вопросам обеспечения информационной безопасности в организации. Для их защиты применяют комплекс организационных и технических мер. Построение корпоративной сети передачи данных неразрывно связано с соблюдением требований информационной безопасности. Одним из таких требований является обязательное применение средств защиты информации для обеспечения мониторинга, контроля сети и выявления сетевых атак [1].

Для обнаружения сетевых атак применяют системы обнаружения вторжений (СОВ) [2]. Классическим подходом детектирования сетевых атак является обнаружение злонамеренного поведения на основе заранее известных шаблонов, паттернов и сигнатур. В связи с постоянным изменением сетевых атак возникают проблемы с поддержкой в актуальном состоянии значительного объема сигнатур и их обработкой СОВ. Увеличение объема базы сигнатур приводит к построению более сложных архитектур СОВ, а также повышаются требования к вычислительным ресурсам системы. Для решения данной проблемы активно развиваются системы обнаружения аномалий (СОА). СОА рассматривает сетевую атаку как аномалию, то есть некое поведение, которое не соответствует нормальному поведению объекта.

Обнаружение аномалий СОВ в академических исследованиях рассматривается как задача классификации и кластеризации на больших объемах данных [3]. Несмотря на значительное количество проведенных исследований, разработанные методы и методики не всегда показывают высокую эффективность обнаружения атак в реальной сети. Для построения эффективной модели используют различные способы и подходы, которые будут рассмотрены в исследовании.

В работе для повышения точности классификации представлен новый мультимодальный метод формирования признакового пространства. Для мультимодального метода проведена оценка и выполнен сравнительный анализ с классическим одномодальным представлением данных.

1. Постановка задачи. Одним из способов повышения эффективности модели является представление и оптимизация признаков набора данных [4]. Представление признаков зависит от методов, используемых в классификаторе. Признаки могут соответствовать атрибутам событий, а могут быть вычислены с применением различных методов [5].

Основной мотивацией данного исследования выступает проблема оптимизации и извлечения признаков сетевого трафика, которая влияет на точность классификации сетевых атак и аномалий.

В настоящее время применяют различные методы представления признакового пространства. Для извлечения признаков при классическом подходе используют один метод извлечения признаков [6], в то время как для гибридного подхода могут использовать два и более методов [7]. На основе анализа различных исследований можно сделать вывод, что извлечение признаков с помощью классического и гибридного подходов действительно повышают эффективность классификации.

В связи с развитием интеллектуальных методов вычислений активно развивается новый подход, в котором данные для классификатора представляются в виде различных модальностей с последующим объединением этих модальностей в единый вид.

Основной задачей работы является адаптация мультимодального подхода искусственного интеллекта (ИИ) к представлению признакового пространства сетевого трафика, с целью повысить эффективность классификации сетевых атак и аномалий.

2. Релевантные работы. Для обнаружения сетевых атак и аномалий СОВ используют различные виды событий: сетевой трафик и события пользовательской активности. Информативные признаки принято делить на две категории: параметрические и категориальные. К параметрическим признакам сетевого трафика относят признаки с числовыми значениями атрибутов такие как: количество переданных пакетов и байт, статистика сетевых соединений, порты для подключения, флаги, таймауты сессий и другие атрибуты сетевого трафика. Категориальные признаки представляют собой различные категории. К таким признакам можно отнести содержимое прикладных протоколов и журналов пользовательской активности.

Для формирования набора параметрических признаков используют различные технологии. К примеру, в работе [8] для анализа мобильного трафика и выделения набора признаков применяют нейронные сети с использованием многослойного автокодировщика. Для оценки качества сжатия передаваемых данных разработан интегральный показатель, предназначенный для выбора архитектуры многослойного автокодировщика. В работе [9] отмечается, что комбинирование статистических и кластерных методов для представления признакового пространства повышают эффективность обнаружения аномалий. Проведенный глубокий статистический анализ атрибутов трафика позволил на основе корреляционных свойств сформировать четыре атрибутных кластера. В результате удалось сократить признаковое пространство с 51 до 17 признаков.

Рассмотренные выше работы были направлены на сокращение признакового пространства, решая задачу снижения вычислительных ресурсов для анализа событий сетевого трафика. Для повышения эффективности модели можно использовать другой подход, направленный на увеличение количества признаков. К примеру, в работе [10] на основе оценок характеристики мультифрактального спектра фрактальной размерности сетевого трафика были введены новые экспериментальные признаки. В работе показано, что данные признаки повышают эффективность классификации компьютерных атак. В исследовании автор делает предположение об универсальности данного метода.

Как отмечалось выше, что в качестве источника категориальных признаков могут использоваться различные пользовательские журналы. В работе [10] для создания матрицы частоты событий применяют различные виды окон. С помощью окон выполняется разбиение логов на различные группы. Сформированная матрица подается на вход различных моделей машинного обучения. Другим способом извлечения признаков является разработанный метод на основе теории графов [11]. Отметим, что данный метод не требует большие вычислительные ресурсы и показал отличный результат при работе с моделью случайный лес.

В работе [12] для выделения признаков используется теорема Шеннона. С помощью метода производят вычисление энтропий для ранее выбранных признаков. Для обнаружения сетевых атак на вход классификатора направляются рассчитанные 14 энтропий. Применение вычисленных энтропийных свойств атрибутов данных повысил эффективность классификатора.

3. Метод обнаружения сетевых атак на основе мультимодального представления признаков данных. ***3.1. Мультимодальное представление признаков данных.*** В связи с развитием технологий искусственного интеллекта (ИИ) широко применяется мультимодальный подход представления данных для решения различных задач. Мультимодальность часто используется в больших языковых моделях (LLM) [13] и предполагает преобразование данных в различные виды модальностей такие как текст, изображение, звук и т.п..

Для СОВ также применяют мультимодальный подход. К примеру, в работе [14] представлена пространственно-временная модель формирования признакового пространства. Архитектура данной модели состоит из двух параллельных методов, построенных на нейронных сетях CNN и LSTM. Выходной слой набора признаков создается путем объединения извлеченных признаков из параллельных ветвей модели. Таким образом, формируется представление данных, состоящее из пространственно-временных признаков. Помимо пространственно-временных признаков могут использоваться другие мо-

дальности как это показано в работе [15]. Автор работы [15] для извлечения признаков использует две модальности: текст и изображение. Для текста извлечение признаков происходит с помощью Spark алгоритмов, а для изображения применяют глубокую сверточную нейронную сеть CNN. С помощью комбинации и объединения признаков разных модальностей удалось повысить точности классификации сетевых атак.

3.2. Описание методики обнаружения сетевых атак и аномалий с помощью мультимодального представления признаков сетевого трафика. Рассмотренные выше модальности применялись для анализа сетевого трафика, но для решения задачи классификации сетевых атак необходимо рассматривать задачу шире. Для этого поток событий сетевого трафика представляем в виде непрерывных или дискретных сигналов. Основываясь на данном предположении, можно рассмотреть другие области, для которых решается аналогичная задача извлечения признаков. К примеру, в медицинской сфере исследуются сигналы, полученные при проведении ЭКГ для выявления патологий. Так в работе [16] представлен широкий обзор методов извлечения признаков в медицинской области. В данной работе технологии извлечения признаков условно объединены в пять категорий или областей: временная область, частотная/спектральная область, частотно-временная область, область декомпозиции и глубокие признаки. В работе отмечается, что извлечение признаков с помощью частотно-временных методов является наиболее эффективным способом выявления патологии при анализе сигналов ЭКГ.

В текущей работе для представления признакового пространства используются две модальности: спектральное представление сетевого трафика и матрица изображений. Методика извлечения признаков с помощью мультимодального подхода представлена на рис. 1.

Рис. 1. Методика представления признаков данных с помощью разных модальностей

Сетевой трафик поступает на сенсор, который выполняет сбор и передачу «сырых» событий сетевого трафика для последующей нормализации и агрегации. В процессе нормализации «сырой» сетевой трафик парсится и раскладывается в соответствующие атрибуты проприетарного протокола Flow. При агрегации событий Flow происходит их объединение и удаление дублирующих данных. Далее нормализованный поток событий направляется на спектральный анализ и на преобразование признаков в изображение с последующим их извлечением. В дальнейшем полученные признаки объединяются и направляются в классификатор для обнаружения сетевых атак, таких как DDoS, U2R, R2L и BotNet.

3.3. Выделение спектральных признаков представления данных. Сетевой трафик представляет собой нестационарный процесс [17]. Известно достаточное количество работ, в которых рассматривается фрактальный анализ самоподобия нестационарных свойств сетевого трафика.

Данное исследование направлено на анализ спектральных характеристик сигналов сетевого трафика, вычисленных с помощью метода оконного преобразования Фурье. Для данного метода выберем следующие признаки:

- Суммарное количество переданных байт.
- Суммарное количество полученных байт.
- Суммарное количество переданных пакетов.
- Суммарное количество полученных пакетов.

Сетевой трафик будем рассматривать как дискретные сигналы, для которых можно использовать оконное преобразование Фурье (Short-Time fourier transform, STFT):

$$X(m,k) = \sum_{n=0}^{N-1} x[n] \cdot \omega[n-m] \cdot e^{-j\frac{2\pi}{N}kn},$$

где $x\,[n]$ – дискретный сигнал, $\omega[n-m]$ – оконная функция, N – длина окна, m – временной индекс, k – частотный индекс.

Для STFT существуют несколько видов окон: прямоугольное окно, окна Ханна, Хэмминга и Блэкмана. Для экспериментальной оценки мультимодального метода будем использовать окно Ханна.

На основе оконного преобразования Фурье вычисляем следующие признаки для представления данных:

- Спектральная мощность

$$P = \sum_{k=1}^{N} |X(k)|^2,$$

$X(k)$ – амплитуда частотного компонента k

- Спектральная плотность как показатель шумоподобного сигнала

$$F = \frac{\text{Среднегеометрическое } (|X(k)|)}{\text{Среднеарифметическое } (|X(k)|)}$$

- Спектральная энтропия мера хаотичности и неопределенности спектра

$$E = -\sum_{k=1}^{N} p(k) \cdot log_2 \ \big(p(k)\big),$$

где $p(k) = \frac{|X(k)|^2}{\sum_{k=1}^{N}|X(k)|^2}$ – нормированная спектральная мощность

3.4. Выделение признаков из изображений. В настоящее время активно применяют нейронные сети глубокого обучения для задач классификации [18]. Помимо этого, данные методы используют для извлечения признаков сетевого трафика. К примеру, сверточная сеть CNN эффективно извлекает признаки из изображений [19]. Анализируя структуру сетевого трафика, можно сделать вывод, что событие можно представить в виде вектора признаков. В работе [20] атрибуты набора данных KDD представлены в виде вектора признаков изображений. Матрица признаков изображений подается на вход сверточной сети CNN для выделения признаков и оптимизации признакового пространства.

В данном случае, события сетевого трафика можно записать в виде вектора признаков: $X_i = \{x_j, \dots, x_n\}$

Тогда матрица изображений признаков будет: $Y = \begin{matrix} X_i \\ X_n \end{matrix}$

В результате получаем матрицу признаков изображений nxn, которую можно использовать как входные данные для нейронной сети CNN.

Для повышения эффективности классификации расширяем признаковое пространство путем увеличения размерности матрицы изображений с помощью метода бикубической интерполяции. В таком случае новую матрицу можно представить в следующем виде:

$$f(x,y) = \sum_{i=0}^{N}\sum_{j=0}^{N} a_{ij}x^i y^i,$$

где x, y – элементы матрицы, a_{ij} – коэффициент определяется на основе ближайших значений.

3.5. Оценка эффективности мультимодального метода представления признаков сетевого трафика. Для проведения эксперимента будем использовать общедоступный набор данных CSE-CICIDS-2018. Набор данных CSE-CICIDS-2018 является обновлением CICIDS2017. Набор данных также имеет дисбаланс классов и структурно похож на прошлую версию набора. CSE-CICIDS-2018 состоит из большего количества клиентских и атакующих машин [21]. Суммарное количество экземпляров трафика составляет 16 233 002 объектов. Сетевой трафик собирался в течение 10 дней. Процентное распределение типа трафика представлено в табл. 1. Набор данных распределен по 10 csv файлам. Девять файлов состоят из событий сетевого трафика с 79 признаками и один файл с 83 признаками.

Таблица 1

Распределение сетевого трафика для CSE-CIC-IDS2018

№	Тип трафика	Распределение (%)
1	Безопасный	83,07
2	DDoS	7,786
3	DoS	4,031
4	Брутфорс	2,347
5	Ботнет	1,763
6	Проникновение	0,997
7	Веб-атака	0,006

Для оценки эффективности метода экспертно выделим 11 признаков из набора данных CSE-CICIDS-2018: Total Fwd Packet, Total Bwd packets, Total Length of Fwd Packet, Total Length of Bwd Packet, Fwd Header Length, Bwd Header Length, Flow Duration, Flow Bytes/s, Flow Packets/s, Fwd Packets/s, Bwd Packets/s.

Разделим 11 признаков на две модальности следующим образом:

1) Количественные данные пакетов для спектрального анализа: Total Fwd Packet, Total Bwd packets, Total Length of Fwd Packet, Total Length of Bwd Packet, Fwd Header Length, Bwd Header Length, Flow Duration.
2) Скорость потока пакетов для матрицы изображений признаков: Flow Bytes/s, Flow Packets/s, Fwd Packets/s, Bwd Packets/s.

Согласно разработанной методике (см. рис. 1) события сетевого трафика с набором признаков спектрального анализа преобразуются с помощью STFT метода и вычисляются новые признаки: спектральная мощность, спектральная плотность и спектральная энтропия.

Для набора признаков скорости потока пакетов формируется матрица признаков изображений с бикубическим преобразованием размерности матрицы.

В качестве классификатора используем нейронную сеть LSTM с одним общим входом. Структура LSTM представляет собой двухуровневую архитектуру с Dropout-слоем для снижения риска переобучения и адаптации выходного слоя для многоклассовой классификации. Обучающие и тестовые данные делятся соответственно на 70 и 30 от общего набора данных.

Результат работы классификатора LSTM при одномодальном представлении признаков сетевого трафика представлен в табл. 2.

Таблица 2

Классификатор LSTM с одномодальным представлением признаков сетевого трафика. 11 признаков CSE-CICIDS-2018

№	Class	Precision	Recall	F1-score	Support
1	BENIGN	0.78	0.97	0.86	1183
2	Botnet	0.58	0.47	0.52	104
3	Botnet - Attempted	0.00	0.00	0.00	253
4	DDoS	0.99	1.00	0.99	71
5	Portscan	0.83	0.40	0.54	48
6	accuracy			0.78	1659
7	macro avg	0.63	0.57	0.58	1659
8	weighted avg	0.66	0.78	0.70	1659

На рис. 2 представлен график изменений Accuracy и функции потерь в зависимости от количества эпох.

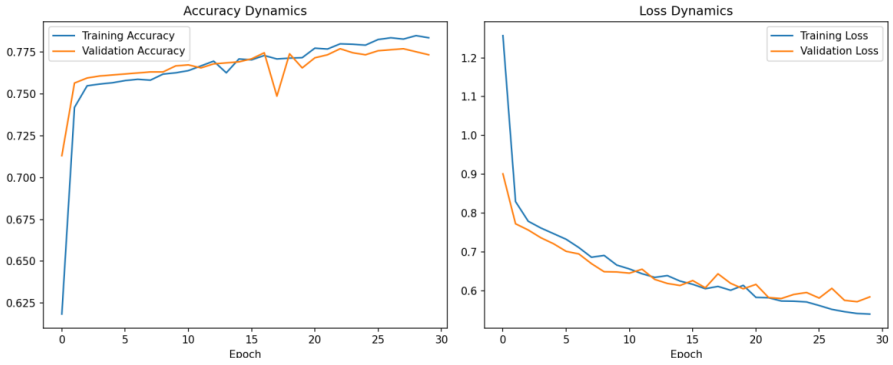


Рис. 2. Accuracy и функция потерь с одномодальным представлением сетевого трафика в зависимости от эпох. 11 признаков CSE-CICIDS-2018

В табл. 2 показаны результаты классификации с мультимодальным представлением признаков сетевого трафика.

Таблица 2

Классификатор LSTM с мультимодальным представлением признаков сетевого трафика. 11 признаков CSE-CICIDS-2018

№	Class	Precision	Recall	F1-score
1	BENIGN	0.78	0.96	0.86
2	Botnet	0.69	0.39	0.50
3	Botnet - Attempted	0.57	0.10	0.17
4	DDoS	0.99	0.97	0.98
5	Portscan	0.76	0.40	0.52
6	Accuracy			0.78
7	Macro Avg	0.76	0.57	0.61
8	Weighted Avg	0.75	0.78	0.73

На графике Accuracy и функции потерь можно заметить снижение времени обучения модели для набора данных CSE-CICIDS-2018 (рис. 3). Примерно с 15 эпохи начинается этап переобучения.

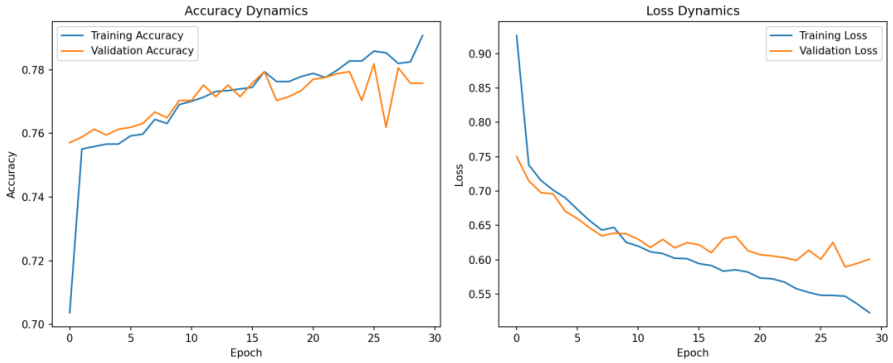


Рис. 3. Accuracy и функция потерь мультимодального представления сетевого трафика с одним общим входом в зависимости от эпох. 11 признаков CSE-CICIDS-2018

В табл. 3 представлен сравнительный анализ методов выделения признаков различной модальности. Мультимодальный метод извлечения признаков повысил оценку precision на 18,9% для классификации сетевой атаки Botnet. Также отметим значительное повышение точности обнаружения сетевой атаки Botnet – Attempted. Оценка precision показывает увеличение точности классификации при мультимодальном методе на 57%, для Recall – 10% и для F1-score – 17%.

Таблица 3

Сравнительный анализ одномодального и мультимодального метода

№	Class	Precision	Recall	F1-score	Precision	Recall	F1-score
		Одномодальный метод			Мультимодальный		
1	BENIGN	0.78	0.97	0.86	0.78	0.96	0.86
2	Botnet	0.58	0.47	0.52	**0.69**	0.39	0.50
3	Botnet - Attempted	0.00	0.00	0.00	**0.57**	**0.10**	**0.17**
4	DDoS	0.99	1.00	0.99	0.99	0.97	0.98
5	Portscan	0.83	0.40	0.54	0.76	0.40	0.52
6	accuracy			0.78			0.78
7	macro avg	0.63	0.57	0.58	**0.76**	0.57	**0.61**
8	weighted avg	0.66	0.78	0.70	**0.75**	0.78	**0.73**

Применение мультимодального метода представления данных со спектральными признаками и матрицей признаков изображений повысил точность классификации для несбалансированных классов сетевых атак: Botnet и Botnet-Attempted. Оценки по другим классам атак практически не изменились. На основе проведенных экспериментов можно сделать вывод о том, что мультимодальный метод можно использовать в качестве одного из способов повышения эффективности классификации сетевых атак и аномалий.

Заключение. В работе проведен анализ основных подходов и методов представления признакового пространства. Отмечается, что мультимодальный подход является новым способом повышения эффективности классификации. Данный подход используется во многих областях, где применяют большие языковые модели (LLM). В работе отмечается важность оптимизации признакового пространства и её влияния на классификацию.

В работе представлен новый метод извлечение признаков сетевого трафика, который отличается от других методов следующим:

- Признаковое пространство формируется на основе мультимодального представления данных сетевого трафика.
- Сформированы новые признаки на основе спектрального анализа оконного преобразования Фурье с помощью признаков транспортного уровня сетевого трафика.
- Матрица признаков изображений второй модальности формируется из признаков сетевого трафика с последующим повышением размерности с помощью метода бикубической интерполяции.

В работе выполнена проверка нового мультимодального метода представления признаков данных. Оценка метода показала, что новый метод извлечения признаков повысил точность классификации для несбалансированных классов сетевых атак на наборе CSE-CICIDS-2018.

Дальнейшие исследования будут направлены на снижение дисбаланса данных в классах с помощью методов аугментации данных с применением генеративных нейронных сетей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Васильев В.И., Кириллова А.Д., Кухарев С.Н.* Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4 (30). – С. 66-74. – DOI: 10.14529/secur180410. – EDN YUNKEP.
2. *Шелухин О.И., Сакалема Д.Ж., Филинова А.С.* Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие / под ред. О.И. Шелухина. – М.: Горячая линия-Телеком, 2018. – 220 с. – ISBN 978-5-9912-0323-4. Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111119.
3. *Шелухин О.И.* Сетевые аномалии. Обнаружение, локализация, прогнозирование. – М.: Горячая линия-Телеком, 2019. – 447 с. – ISBN 978-5-9912-0756-0.
4. *Varun Chandola, Arindam Banerjee, and Vipin Kumar.* Anomaly detection: A survey. ACM Comput. // Surv. – 2009. – 41, 3, Article 15 (July 2009). – 58 p. – https://doi.org/10.1145/1541880.1541882.
5. *Шелухин О.И., Судариков Р.А.* Анализ информативных признаков в задачах обнаружения аномалий трафика статистическими методами // T-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8, № 3. – С. 14-18. – EDN SGIHFZ.
6. *Xin R., Liu H., Chen P. et al.* Robust and accurate performance anomaly detection and prediction for cloud applications: a novel ensemble learning-based framework // J Cloud Comp. – 2023. – 12, 7. – https://doi.org/10.1186/s13677-022-00383-6.
7. *Alsaffar A.M., Nouri-Baygi M. & Zolbanin H.M.* Shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning // J Big Data. – 2024. – 11, 133. – https://ezpro.fa.ru:2117/10.1186/s40537-024-00994-7.
8. *Шелухин О.И., Маторин Ф.А*. Снижение размерности массивов данных с помощью многослойных автокодировщиков в задаче классификации мобильных приложений // Тр. учебных заведений связи. – 2024. – Т. 10, № 6. – С. 111-120. – DOI: 10.31854/1813-324X-2024-10-6-111-120. – EDN TOPDUA.
9. *Шелухин О.И., Раковский Д.И.* Выбор метрических атрибутов редких аномальных событий компьютерной системы методами интеллектуального анализа данных // T-Comm: Телекоммуникации и транспорт. – 2021. – Т. 15, № 6. – С. 40-47. – DOI: 10.36724/2072-8735-2021-15-6-40-47. – EDN YJDUYV.
10. *Шелухин О.И., Рябинин В.С., Фармаковский М.А.* Обнаружение аномальных состояний компьютерных систем средствами интеллектуального анализа данных системных журналов // Вопросы кибербезопасности. – 2018. – № 2 (26). – С. 33-43. – DOI: 10.21681/2311-3456-2018-2-33-43. – EDN XYHQUP.
11. *Слипенчук П.В.* Алгоритм извлечения характерных признаков из данных пользовательских активностей // Вопросы кибербезопасности. – 2019. – № 1 (29). – С. 53-58. – DOI: 10.21681/2311-3456-2019-1-53-58. – EDN YZFWPZ.
12. *Do E.H. and Gadepally V.N*. Classifying Anomalies for Network Security // ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020. – P. 2907-2911. – DOI: 10.1109/ICASSP40776.2020.9053419.

13. *Wu J., Gan W., Chen Z., Wan S. and Yu P.S.* Multimodal Large Language Models: A Survey // 2023 IEEE International Conference on Big Data (BigData), Sorrento, Italy, 2023. – P. 2247-2256. – DOI: 10.1109/BigData59044.2023.10386743.
14. *Shi S., Han D., & Cui M.* A multimodal hybrid parallel network intrusion detection model // Connection Science. – 2023. – 35 (1). – https://doi.org/10.1080/09540091.2023.2227780.
15. *Ullah F., Turab A., Ullah S., Cacciagrano D., Zhao Y.* Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory // Sensors. – 2024. – 24 (13):4152. – https://doi.org/10.3390/s24134152.
16. *Singh A.K., Krishnan S.* ECG signal feature extraction trends in methods and applications // BioMed Eng OnLine. – 2023. – 22. – https://doi.org/10.1186/s12938-023-01075-1.
17. *Kotenko I., Saenko I., Lauta O., Kribel A.* An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity // Energies. – 2020. – Vol. 13, No. 19. – P. 5031. – DOI: 10.3390/en13195031. – EDN YVERBA.
18. *Гетьман А.И., Горюнов М.Н., Мацкевич А.Г. [и др.].* Применение глубокого обучения для обнаружения компьютерных атак в сетевом трафике // Тр. Института системного программирования РАН. – 2023. – Т. 35, № 4. – С. 65-92. – DOI: 10.15514/ISPRAS-2023-35(4)-3. – EDN CSLHAE.
19. *Jogin M., Mohana, Madhulika M.S., Divya G.D., Meghana R.K. and Apoorva S.* Feature Extraction using Convolution Neural Networks (CNN) and Deep Learning // 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018. – P. 2319-2323. – DOI: 10.1109/RTEICT42901.2018.9012507.
20. *Xiao Y., Xing C., Zhang T. and Zhao Z.* An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks // in IEEE Access. – 2019. – Vol. 7. – P. 42210-42219. – DOI: 10.1109/ACCESS.2019.2904620.
21. *Thakkar A., Lohiya R.* A review of the advancement in intrusion detection datasets // Procedia Comput Sci. – 2020. – 167. – P. 636-645.

REFERENCES

1. *Vasil'ev V.I., Kirillova A.D., Kukharev S.N.* Kiberbezopasnost' avtomatizirovannykh sistem upravleniya promyshlennykh ob"ektov (sovremennoe sostoyanie, tendentsii) [Cybersecurity of automated control systems of industrial facilities (current status, trends)], *Vestnik UrFO. Bezopasnost' v informatsionnoy sfere* [Bulletin of the Ural Federal District. Security in the Information Sphere**],** 2018, No. 4 (30), pp. 66-74. DOI: 10.14529/secur180410. EDN YUNKEP.
2. *Shelukhin O.I., Sakalema D.Zh., Filinova A.S.* Obnaruzhenie vtorzheniy v komp'yuternye seti (setevye anomalii): ucheb. posobie [Detection of intrusions in computer networks (network anomalies): a tutorial], ed. by O.I. Shelukhina. Moscow: Goryachaya liniya-Telekom, 2018, 220 p. ISBN 978-5-9912-0323-4. Lan': elektronno-bibliotechnaya sistema. Available at: https://e.lanbook.com/book/111119.
3. *Shelukhin O.I.* Setevye anomalii. Obnaruzhenie, lokalizatsiya, prognozirovanie [Network anomalies. Detection, localization, forecasting]. Moscow: Goryachaya liniya-Telekom, 2019, 447 p. ISBN 978-5-9912-0756-0.
4. *Varun Chandola, Arindam Banerjee, and Vipin Kumar.* Anomaly detection: A survey. ACM Comput., Surv., 2009, 41, 3, Article 15 (July 2009), 58 p. Available at: https://doi.org/10.1145/1541880.1541882.
5. *Shelukhin O.I., Sudarikov R.A.* Analiz informativnykh priznakov v zadachakh obnaruzheniya anomaliy trafika statisticheskimi metodami [Analysis of informative features in the problems of detecting traffic anomalies by statistical methods], *T-Comm: Telekommunikatsii i transport* [T-Comm: Telecommunications and transport], 2014, Vol. 8, No. 3, pp. 14-18. EDN SGIHFZ.
6. *Xin R., Liu H., Chen P. et al.* Robust and accurate performance anomaly detection and prediction for cloud applications: a novel ensemble learning-based framework, *J Cloud Comp*., 2023, 12, 7. Available at: https://doi.org/10.1186/s13677-022-00383-6.
7. *Alsaffar A.M., Nouri-Baygi M. & Zolbanin H.M.* Shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning, *J Big Data,* 2024, 11, 133. Available at: https://ezpro.fa.ru:2117/10.1186/s40537-024-00994-7.
8. *Shelukhin O.I., Matorin F.A.* Snizhenie razmernosti massivov dannykh s pomoshch'yu mnogosloynykh avtokodirovshchikov v zadache klassifikatsii mobil'nykh prilozheniy [Reducing the dimensionality of data arrays using multilayer autoencoders in the problem of mobile application classification], *Tr. uchebnykh zavedeniy svyazi* [Proceedings of educational institutions of communication], 2024, Vol. 10, No. 6, pp. 111-120. DOI: 10.31854/1813-324X-2024-10-6-111-120. EDN TOPDUA.
9. *Shelukhin O.I., Rakovskiy D.I.* Vybor metricheskikh atributov redkikh anomal'nykh sobytiy komp'yuternoy sistemy metodami intellektual'nogo analiza dannykh [Selection of metric attributes of rare anomalous events of a computer system using data mining methods], *T-Comm: Telekommunikatsii i transport* [T-Comm: Telecommunications and transport], 2021, Vol. 15, No. 6, pp. 40-47. DOI: 10.36724/2072-8735-2021-15-6-40-47. EDN YJDUYV.

10. *Shelukhin O.I., Ryabinin V.S., Farmakovskiy M.A.* Obnaruzhenie anomal'nykh sostoyaniy komp'yuternykh sistem sredstvami intellektual'nogo analiza dannykh sistemnykh zhurnalov [Detection of abnormal states of computer systems by means of intelligent analysis of system log data], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2018, No. 2 (26), pp. 33-43. DOI: 10.21681/2311-3456-2018-2-33-43. EDN XYHQUP.
11. *Slipenchuk P.V.* Algoritm izvlecheniya kharakternykh priznakov iz dannykh pol'zovatel'skikh aktivnostey [Algorithm for extracting characteristic features from user activity data], Voprosy kiberbezopasnosti [Cybersecurity Issues], 2019, No. 1 (29), pp. 53-58. DOI: 10.21681/2311-3456-2019-1-53-58. EDN YZFWPZ.
12. *Do E.H. and Gadepally V.N*. Classifying Anomalies for Network Security, *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020,* pp. 2907-2911. DOI: 10.1109/ICASSP40776.2020.9053419.
13. *Wu J., Gan W., Chen Z., Wan S. and Yu P.S*. Multimodal Large Language Models: A Survey, *2023 IEEE International Conference on Big Data (BigData), Sorrento, Italy, 2023,* pp. 2247-2256. DOI: 10.1109/BigData59044.2023.10386743.
14. *Shi S., Han D., & Cui M.* A multimodal hybrid parallel network intrusion detection model, *Connection Science,* 2023, 35 (1). Available at: https://doi.org/10.1080/09540091.2023.2227780.
15. *Ullah F., Turab A., Ullah S., Cacciagrano D., Zhao Y.* Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory, *Sensors,* 2024, 24 (13):4152. Available at: https://doi.org/10.3390/s24134152.
16. *Singh A.K., Krishnan S.* ECG signal feature extraction trends in methods and applications, *BioMed Eng OnLine,* 2023, 22. Available at: https://doi.org/10.1186/s12938-023-01075-1.
17. *Kotenko I., Saenko I., Lauta O., Kribel A.* An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity, *Energies,* 2020, Vol. 13, No. 19, pp. 5031. DOI: 10.3390/en13195031. EDN YVERBA.
18. *Get'man A.I., Goryunov M.N., Matskevich A.G. [i dr.].* Primenenie glubokogo obucheniya dlya obnaruzheniya komp'yuternykh atak v setevom trafike [Application of deep learning to detect computer attacks in network traffic], *Tr. Instituta sistemnogo programmirovaniya RAN* [Proceedings of the Institute for System Programming of the Russian Academy of Sciences], 2023, Vol. 35, No. 4, pp. 65-92. DOI: 10.15514/ISPRAS-2023-35(4)-3. EDN CSLHAE.
19. *Jogin M., Mohana, Madhulika M.S., Divya G.D., Meghana R.K. and Apoorva S.* Feature Extraction using Convolution Neural Networks (CNN) and Deep Learning, *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018,* pp. 2319-2323. DOI: 10.1109/RTEICT42901.2018.9012507.
20. *Xiao Y., Xing C., Zhang T. and Zhao Z.* An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks, *in IEEE Access,* 2019, Vol. 7, pp. 42210-42219. DOI: 10.1109/ACCESS.2019.2904620.
21. *Thakkar A., Lohiya R.* A review of the advancement in intrusion detection datasets, *Procedia Comput Sci*., 2020, 167, pp. 636-645.

Балыбердин Алексей Викторович – Финансовый университет при Правительстве РФ**;** e-mail:balyberdinav@gmail.com**;** г. Москва, Россия; аспирант.

Balyberdin Alexey Viktorovich – Financial University under the Government of the Russian Federation; e-mail:balyberdinav@gmail.com; Moscow, Russia; graduate student.

УДК 004.89 DOI 10.18522/2311-3103-2025-3-16-31

М.А. Лапина, Р.А. Дымуха, Н.Н. Кучеров, Е.С. Басан

ИССЛЕДОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СПУФИНГ-АТАК В ДЕЦЕНТРАЛИЗОВАННЫХ СЕТЯХ

Беспилотные летательные аппараты всё больше и больше появляются в нашей жизни и используются для различных целей, таких как доставка грузов, мониторинг, управление хозяйством, мониторинг и развлечения. Но вместе с ростом их популярности, увеличивается и число людей, которые намеренно хотят помешать работе БВС (беспилотным воздушным судам) и использовать в своих интересах и целях. Они используют различные виды атак, чтобы любыми способами

устранить или перехватить автономный летательный аппарат. Спуфинг-атаки являются одним из наиболее распространенных и опасных видов атак, так как позволяют злоумышленникам действовать незаметно, подделывая идентификаторы автономных летательных аппаратов или операторов, выдавая себя за легитимных участников системы. Целью таких атак может быть перехват управления, кража данных, саботаж или использование БВС для выполнения вредоносных действий, таких как шпионаж, нанесение ущерба или сбой в операциях. Но с каждым годом всё сложнее предотвращать атаки, так как они сложны в обнаружении и могут привести к серьезным последствиям, именно поэтому обнаружение спуфинг-атак на беспилотный аппарат при помощи машинного обучения активно исследуется и применяется. В статье рассматриваются спуфинг-атаки на БВС, проведен анализ спуфинга на автономные летательные аппараты, на основе открытого набора данных с помощью платформы Knime проведено исследование методов машинного обучения обнаружения спуфинг-атак. Результаты исследования демонстрируют, что способ обнаружения атак с помощью машинного обучения на основе ансамблевого метода, модели Tree Ensemble Learner и Random Forest Learner,, показавшие результаты 97.110% и 97.039% соответственно, является лучшим среди других методов, что позволит улучшить безопасность беспилотных летательных аппаратов, снижает нагрузку на операторов и повышает надежность системы в целом. В дальнейшем предложенный подход может быть расширен для обнаружения других видов кибератак, что сделает его универсальным методом защиты от воздействий злоумышленников.

Машинное обучение; Machine Learning; KNIME; поиск уязвимостей беспилотных воздушных судов; искусственный интеллект; данные; датасет; атаки на БВС; спуфинг.

M.A. Lapina, R.A. Dymuha, N.N. Kucherov, E.S. Basan

RESEARCH OF MACHINE LEARNING METHODS FOR DETECTING SPOOFING ATTACKS IN DECENTRALIZED NETWORKS

Unmanned aerial vehicles are appearing more and more in our lives and are used for various purposes such as cargo delivery, monitoring, household management, exploration and entertainment. But along with their growing popularity, the number of people who intentionally want to interfere with the operation of UAVs and use them for their own interests and purposes is also increasing. They use various types of attacks to eliminate or intercept the drone by any means. Spoofing attacks are one of the most common and dangerous types of attacks, as they allow attackers to act unnoticed, faking the identifiers of autonomous aircraft or operators, posing as legitimate participants in the system. The purpose of such attacks may be to intercept control, steal data, sabotage, or use UAVs to perform malicious actions such as espionage, damage, or malfunction operations. But every year it becomes more difficult to prevent attacks, as they are difficult to detect and can lead to serious consequences, which is why such a solution as detecting spoofing attacks on an unmanned vehicle using machine learning was invented. The article discusses spoofing attacks on UAVs, analyzes spoofing on autonomous aircraft, and studies machine learning methods for detecting spoofing attacks based on a dataset using the Knime platform. The results of the study demonstrate that the method of detecting attacks using machine learning based on the ensemble method, the Tree Ensemble Learner and Random Forest Learner models, which showed results of 97.110% and 97.039%, respectively, is the best among other methods, which will improve the security of unmanned aerial vehicles, reduce the burden on operators and increase the reliability of the system as a whole. In the future, the proposed approach can be expanded to detect other types of cyberattacks, which will make it a universal method of protection against intruders.

Machine learning; Machine Learning; KNIME; drone vulnerability search; artificial intelligence; data; dataset; drone attacks; spoofing.

Введение. В настоящее время, использование беспилотных воздушных судов (БВС) влечет за собой не только полезные свойства, но и ряд технических и социальных проблем, таких, как: проблемы с кибербезопасностью, конфиденциальностью и общественной безопасностью. БВС могут также использоваться злоумышленниками для проведения физических и кибератак, угрожающих социуму. При увеличении числа беспилотных летательных аппаратов становится все труднее выявлять и пресекать опасные беспилотные летательные аппараты, которые могут вызвать угрозу. Существуют разные виды атак на БВС, к ним можно отнести: спуфинг-атаки, человек посередине (MitM), атаки отказ в обслуживании, атаки прошивок, фишинговые атаки, атака на GPS-сигналы и атаки на

каналы связи [1, 2]. Исследование данных атак проводились Eldosouky A.R, Khan S.Z, Menaka P.A, Wesson K. [3–6]. В данной статье рассматривается один из самых распространённых видов атак – спуфинг атаки.

Спуфинг-атака – глушение и последующая подмена статического GPS-сигнала со спутника совершенно другим, более мощным, сигналом, который транслируется с наземной станции [7]. С помощью этого нового сигнала можно внести значительные изменения в заданные параметры. Таким образом, из-за получения ошибочных данных устройство быстро теряет ориентировку в пространстве. Такие атаки являются одним из наиболее распространенных и опасных видов атак на БВС, так как они позволяют злоумышленнику действовать незаметно, выдавая себя за легитимного участника системы. Спуфинг-атаки могут быть направлены на различные цели, включая перехват управления, кражу данных, саботаж или даже использование БВС для выполнения вредоносных действий [8].

Рис. 1. Timeline спуфиг-атак на БВС

Спуфинг-атаки представляют собой серьезную опасность для БВС. Эти действия были направлены на перехват управления БВС, позволяя себе легитимного оператора. В результате злоумышленник может получить контроль над БВС и использовать его для выполнения конкурентных действий, таких как шпионаж, саботаж или даже физическая атака. Первые спуфинг-атаки на БВС начали появляться в середине 2010-х годов, когда БВС стали более доступными и широко использовались в различных областях, таких как фотография, экономика, логистика и военные операции. Одной из первых известных атак стала атака на БВС, предпринятая для сельскохозяйственных угодий Диптихов. Злоумышленник перехватил управление БВС, изменил его маршрут и использовал его для сбора данных о состоянии полей конкурентов.

Эта атака продемонстрировала уязвимость БВС к спуфингу и необходимость разработки методов защиты. В связи с этим исследователи начали изучать способы обнаружения и предотвращения атак [9].

В 2011 году в Иран представил пресс-релиз, в котором говорилось об успешном перехвате американского БВС типа RQ-170 Sentinel. Среди прочих атак фигурировала и спуфинг-атака, в результате чего судно в автоматическом режиме, ориентируясь по глобальной системе навигации, начало возвращение домой. Поскольку истинный сигнал был заглушён ложным, RQ-170 Sentinel сел на иранский аэродром, приняв его за легитимный [9].

В 2012 году в Техасе американскими учеными была доказана практическая возможность взлома и перехват управления БВС путем GPS-спуфинга. Спуфинг-атака на GPS-атака, которая пытается обмануть GPS-приемник, широковещательно передавая немного более мощный сигнал, чем полученный от спутников GPS, такой, чтобы быть похожим на ряд нормальных сигналов GPS. Эти имитирующие сигналы изменены таким образом, чтобы заставить получателя неверно определять свое местоположение, считая его таким, какое отправит атакующий. Поскольку системы GPS работают, измеряя время, которое требуется для сигнала, чтобы атакующий точно знал, где его цель – так, чтобы имитирующий сигнал мог быть структурирован с надлежащими задержками сигнала [10].

В 2022 году Barak Davidovich, Ben Nassi и Yuval Elovici демонстрируют способность разработанного ими метода защищать БВС от атак с подменой GPS. Результаты исследования показывают, что они могут обеспечить высокий уровень безопасности

БВСа, летящего на высоте 50–100 м над городской местностью со средней скоростью 4 км/ч в условиях низкой освещенности. Предлагаемый метод может обеспечить уровень безопасности, который обнаруживает любую атаку с использованием GPS-спуфинга, при которой поддельное местоположение находится на расстоянии 1-4 м (в среднем 2,5 м) от реального местоположения. Преимущества данного метода включают тот факт, что он не требует никакого дополнительного оборудования или предварительных знаний о районе полета [11].

Схема, представленная на рис. 2, показывает механизм действия спуфинг-атаки. Злоумышленник через Wi-Fi-сигнал передает поддельный сигнал, имитирующий подлинный. В результате атаки соединение между оператором и БВС прерывается, так как БВС подключается к поддельному сигналу, следовательно оператор теряет управление БВС.

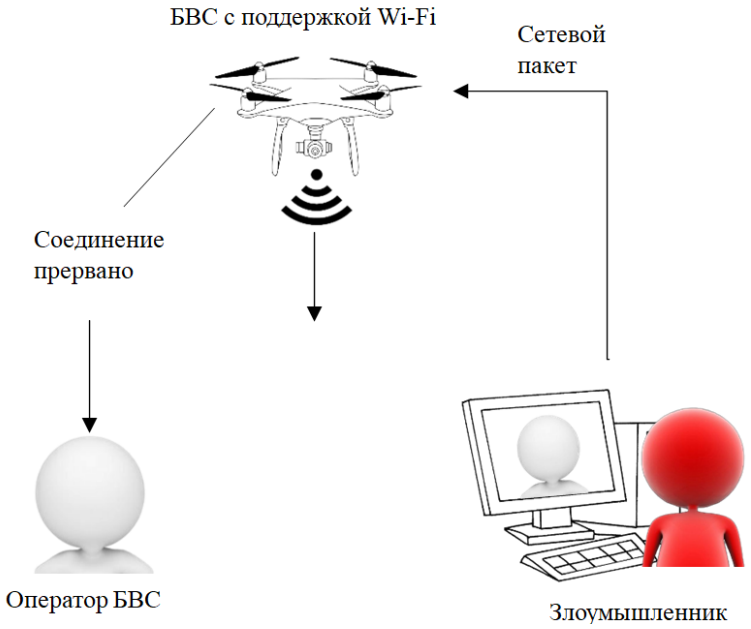


Рис. 2. Схема спуфиг-атаки на БВС

Для обнаружения атак на БВС применяется машинное обучение. В статье представлено исследование методов машинного обучения для обнаружения спуфинг-атак на БВС [12].

Для обнаружения спуфинга-атак необходимо определить параметры, которые будут анализироваться и проверяться на наличие аномалий или отклонений, указывающих на потенциальные угрозы.

Проведем анализ датасета, который использовался для исследования: drone_communication_dataset.csv [13].

Набор данных Drone Communication and Network Anomaly Detection содержит многомерные данные, собранные из моделируемой сети связи БВСов за период с 1 ноября 2019 года по 31 декабря 2024 года с почасовыми временными метками. Он включает в себя различные параметры связи, данные GPS, статистику сети и многоцелевые целевые индикаторы для различных сетевых аномалий. Набор данных предназначен для исследований и разработок в таких областях, как кибербезопасность, обнаружение аномалий IoT, связь БВС-БВС (D2D) и БВС-базовая станция (D2BS), а также оптимизация сети [13].

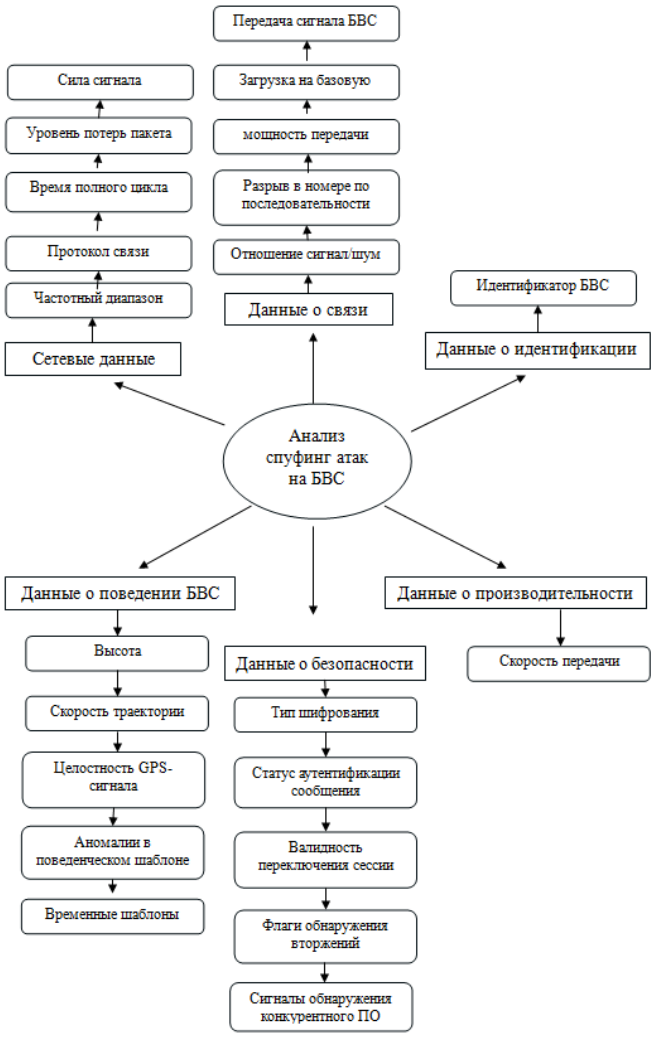


Рис. 3. Параметры, используемые при обнаружении спуфинг-атак

Набор данных содержит 45 289 записей и 35 столбцов. В табл. 1 приведено описание набора данных.

Таблица 1

Анализ набора данных

№	Название колонки	Тип данных	Описание	Метод получения
1.	timestamp	datetime	Время записи данных	Фиксируется при каждом измерении или передаче данных, записывается автоматически системой
2.	signal_strength	числовой, int/float	Уровень сигнала (в dBm). Отрицательные значения указывают на силу сигнала (чем ближе к 0, тем сильнее сигнал)	Измеряется сенсорами или приемниками сигнала

3.	packet_loss_rate	числовой, int/float	Процент потерянных пакетов данных.	Вычисляется как отношение потерянных пакетов к общему числу отправленных
4.	round_trip_time	числовой, int/float	Время (в мс) между отправкой запроса и получением ответа	Измеряется таймерами при передаче данных
5.	communication_protocol	категориальный, string	Протокол связи (например, ZigBee, LoRa, Wi-Fi)	Устанавливается в настройках устройства или определяется автоматически
6.	frequency_band	числовой (float)	Частота (в МГц или ГГц), на которой работает устройство	Указывается в конфигурации устройства
7.	encryption_type	категориальный, string	Тип шифрования данных (например, AES, RSA, Plain-text)	Устанавливается в настройках безопасности
8.	drone_gps_coordinates	категориальный, string	Географические координаты БВСа	Считываются с GPS-модуля БВСа
9.	altitude	числовой, int/float	Высота БВСа (в метрах)	Измеряется барометром или GPS
10.	speed_trajectory	числовой, int/float	Скорость движения БВСа (в м/с или км/ч)	Вычисляется на основе данных GPS или инерциальных датчиков
11.	transmission_power	числовой, int/float	Мощность передачи сигнала (в dBm)	Устанавливается в настройках передатчика
12.	message_authentication_status	бинарный, int	Статус аутентификации сообщения (1 – успешно, 0 – неудача)	Проверяется криптографическ ими алгоритмами
13.	session_key_validity	бинарный, int	Валидность сессионного ключа (1 – действителен, 0 – недействителен)	Проверяется системой безопасности
14.	signal_noise_ratio	числовой, int/float	Отношение сигнал/шум (в dB)	Измеряется приемником сигнала
15.	sequence_number_gap	числовой, int	Разрыв в последовательности номеров пакетов	Анализируется при приеме данных
16.	drone_identification	числовой (integer)	Уникальный идентификатор БВС	Присваивается при регистрации БВС
17.	data_rate	числовой, int/float	Скорость передачи данных (в кбит/с или Мбит/с)	Устанавливается в настройках связи
18.	network_traffic_volume	числовой, int/float	Объем сетевого трафика (в байтах или пакетах)	Измеряется сетевым оборудованием
19.	gps_signal_integrity	бинарный, int	Целостность GPS-сигнала (1 – хорошая, 0 – плохая)	Анализируется GPS-приемником
20.	uplink_downlink_quality	числовой, int/float	Качество связи (в условных единицах)	Измеряется приемопередатчи ком
21.	base_station_load	числовой, int/float	Нагрузка на базовую станцию (в %)	Мониторится базовой станцией
22.	port_scanning_attempts	числовой, int	Количество попыток сканирования портов	Фиксируется системами защиты

23.	drone_signal_handoff	бинарный, int	Факт передачи сигнала между станциями (1 – да, 0 – нет)	Логируется при переключении каналов
24.	malware_detection_signals	бинарный, int	Количество сигналов о вредоносном ПО	Анализируется антивирусными системами
25.	anomaly_in_behavioral_pattern	числовой, int	Уровень аномалии в поведении БВСа	Выявляется системами мониторинга
26.	intrusion_detection_flags	бинарный, int	Флаги обнаружения вторжений	Устанавливаются системами безопасности
27.	temporal_patterns	числовой, int	Временные закономерности в данных	Анализируются алгоритмами машинного обучения
28.	label_normal	бинарный, int	Метка нормального состояния (1 – норма, 0 – аномалия)	Присваивается вручную или алгоритмами
29.	label_spoofing	бинарный, int	Метка спуфинга (1 – атака, 0 – нет)	Определяется системами защиты
30.	label_mitm	бинарный, int	Метка атаки "человек посередине" (1 – атака, 0 – нет)	Выявляется криптографическ ими методами
31.	label_ddos	бинарный, int	Метка DDoS-атаки (1 – атака, 0 — нет)	Анализируется сетевыми системами
32.	label_gps_spoofing	бинарный, int	Метка GPS-спуфинга (1 – атака, 0 – нет)	Обнаруживается GPS-приемниками
33.	label_malware	бинарный, int	Метка вредоносного ПО (1 – обнаружено, 0 – нет)	Сканируется антивирусами
34.	label_jamming	бинарный, int	Метка глушения сигнала (1 – атака, 0 – нет)	Фиксируется приемниками сигнала
35.	label_protocol_exploit	бинарный, int	Метка эксплуатации уязвимостей протокола (1 – атака, 0 – нет)	Выявляется системами мониторинга

Существуют разные подходы и платформы, которые позволяют работать с моделями машинного обучения. В работе проводились исследования с применением платформы для анализа данных Knime [14]. Платформа предоставляет широкий выбор моделей машинного. На рис. 4 приведены модели машинного обучения, которые применялись для исследования.

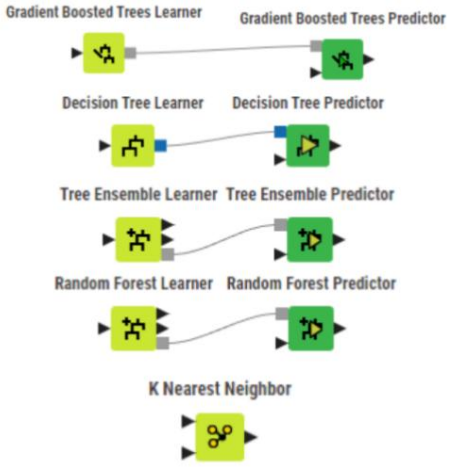


Рис. 4. Модели машинного обучения

В табл. 2 представлена сравнительная характеристика способа защиты от спуфинг-атак по критериям: удобство, приватность, скорость, цена, сложность обеспечения и эффективность

Таблица 2

Сравнительная характеристика способа защиты от спуфинг-атак

Методы защиты	Удобство	Приватность	Скорость	Цена	Сложность обеспечения	Эффективность
Криптографические методы	✔					✔
Аутентификация		✔				✔
Мониторинг сетевого трафика					✔	✔
Обнаружение аномалий					✔	✔
Защита GPS-сигналов		✔				✔
Регулярное обновление прошивки	✔				✔	
Физическая защита						✔

На основе данных из табл. 2, универсального способа защиты от спуфинг-атак не выявлено, однако машинное обучение позволяет анализировать данные и на их основе обнаруживать спуфинг-атаки

На примере Gradient Boosted Trees Learner рассмотрим структурную схему модели машинного обучения CSV Reader загружает данные из CSV-файла. Узел преобразует данные в таблицу, с которой происходить исследование. Затем данные поступают на узел Column Filter, который позволяет выбрать или исключить определенные столбцы из таблицы данных. В табл. 1 будут исключены такие калонки: label_normal, label_mitm, label_ddos, label_gps_spoofing, label_malware, label_jamming, label_protocol_exploit. Колонки убраны, так как в область исследования входит только спуфинг. Следующий нод, One to Many, преобразует данные из формата "один ко многим". Он создает отдельные строки для каждой категории, то есть кодирует данные. В наборе данных нужно закодировать категориальные данные, чтобы не возникало ошибок при исследовании. Поэтому будут кодироваться такие столбцы, как communication_protocol, encryption_type, drone_gps_coordinates. Узел Number to String конвертирует числовые значения в строки. В нем нужно преобразовать только целевую колонку, чтобы она могла использоваться узлом SMOTE. Узел SMOTE используется для балансировки несбалансированных данных. SMOTE создает синтетические примеры для меньшинственного класса, чтобы увеличить его представительство в данных. Узел PCA уменьшает размерность данных, сохраняя при этом наибольшую часть вариации. PCA преобразует данные в новые признаки, которые являются линейными комбинациями исходных признаков. Узел X-Partitioner разделяет данные на обучающую и тестовую выборки. Это важно для оценки производительности модели на данных, которые не использовались в процессе обучения. Подключается Gradient Boosted Trees Learner и к нему предиктор Gradient Boosted Trees Predictor. Узлы выполняют обучение Узел X-Aggregator объединяет результаты предсказаний обучающей и тестовой выборок в одну таблицу. Наконец, узел Scorer вычисляет метрики качества модели, такие как точность, полнота, F1-score и другие, на основе предсказаний и истинных значений.

На примере Gradient Boosted Trees Learner была представлена методика организации 10 исследований с разными моделями машинного обучения. Ниже представлены 5 моделей, показавших лучшие результаты.

1. **Gradient Boosted Trees Learner** изучает деревья с градиентным усилением с целью классификации. Алгоритм использует очень мелкие деревья регрессии и специальную форму усиления для построения ансамбля деревьев [15].

Исследование Gradient Boosted Trees Learner на изменение PCA для определения лучшей точности приведено на рис. 5.

Gradient Boosted Trees Learner	
PCA	F1-score
29	0,791
27	0,792
25	0,791
23	0,782
21	0,771
19	0,801
17	0,665
15	0,664
13	0,634
11	0,715
9	0,609
7	0,59
5	0,586
3	0,578
1	0,63

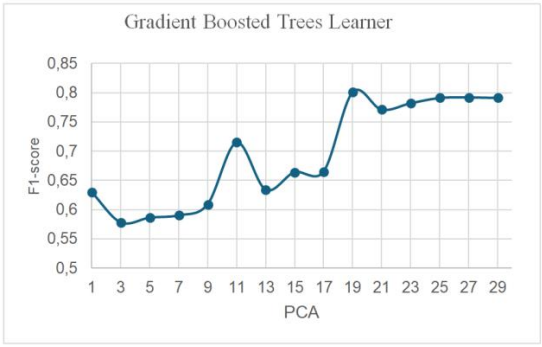


Рис. 5. Результаты изменения точности PCA модели Gradient Boosted Trees Leamey

На графике на рис. 5 показан результат изменения точности при изменении числа колонок в PCA. Наилучшим является PCA с 19 колонками и результатом 0,801.

2. **Decision Tree Learner** – этот узел индуцирует дерево решений классификации в основной памяти. Деревья решений строятся путем последовательного разделения данных на подмножества на основе значений признаков. Каждое разделение выбирается так, чтобы максимизировать однородность подмножеств относительно целевой переменной [16].

Исследование Decision Tree Learner на изменение PCA для определения лучшей точности, показано на рис. 6.

Decision Tree Learner	
PCA	F1-score
29	0,914
27	0,913
25	0,913
23	0,907
21	0,911
19	0,898
17	0,875
15	0,871
13	0,869
11	0,869
9	0,857
7	0,847
5	0,83
3	0,815
1	0,636

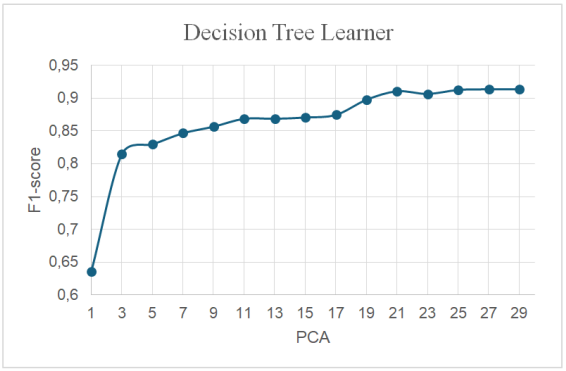


Рис. 6. Результаты изменения точности PCA модели Decision Tree Leamer

На графике показан результат изменения точности при изменении числа колонок в PCA. Наилучшим является PCA с 29 колонками и результатом 0,914.

3. **Tree Ensemble Learner** изучает ансамбль деревьев решений (например, варианты случайного леса). Обычно каждое дерево строится с различным набором строк (записей) и/или столбцов (атрибутов). Ансамбль деревьев решений – это метод машинного обучения, который объединяет множество деревьев решений для повышения точности предсказаний [17].

Исследование Tree Ensemble Learner на изменение PCA для определения лучшей точности, показано на рис. 7.

Tree Ensemble Learner	
PCA	F1-score
29	0,941
27	0,936
25	0,928
23	0,945
21	0,948
19	0,926
17	0,883
15	0,866
13	0,86
11	0,866
9	0,849
7	0,869
5	0,862
3	0,838
1	0,635

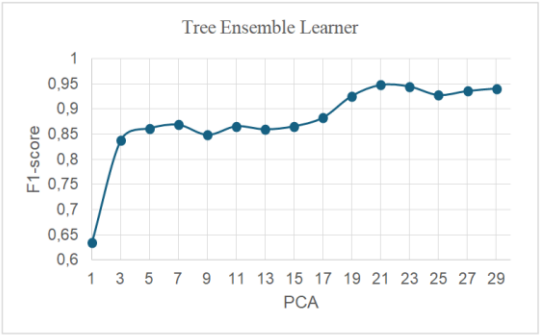


Рис. 7. Результаты изменения точности PCA модели Tree Ensemble Learner

На графике показан результат изменения точности при изменении числа колонок в PCA. Наилучшим является PCA с 21 колонками и результатом 0,948.

4. **Random Forest Learner** изучает случайный лес, состоящий из выбранного количества деревьев решений. Каждая из моделей дерева решений строится с различным набором строк (записей), и для каждого разделения в дереве используется случайно выбранный набор столбцов (описывающих атрибуты) [18].

Исследование Random Forest Learner на изменение PCA для определения лучшей точности, показано на рис. 8.

Random Forest Learner	
PCA	F1-score
29	0,973
27	0,975
25	0,974
23	0,974
21	0,973
19	0,966
17	0,953
15	0,945
13	0,935
11	0,931
9	0,922
7	0,898
5	0,88
3	0,838
1	0,614

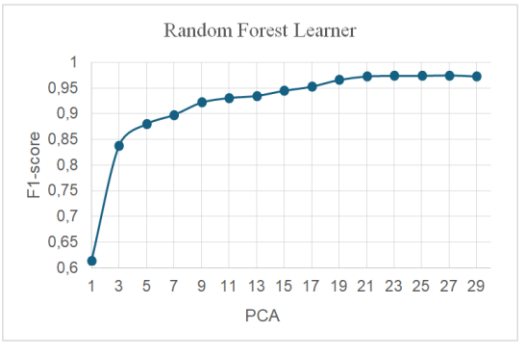


Рис. 8. Результаты изменения точности PCA Random Forest Learner

На данном графике показан результат изменения точности при изменении числа колонок в PCA. Наилучшим является PCA с 27 колонками и результатом 0,975.

5. **K Nearest Neighbor** классифицирует набор тестовых данных на основе алгоритма k ближайших соседей с использованием обучающих данных. Базовый алгоритм использует дерево KD и, следовательно, должен демонстрировать разумную производительность [19].

Исследование K Nearest Neighbor на изменение PCA для определения лучшей точности, как показано на рис. 9.

На данном графике показан результат изменения точности при изменении числа колонок в PCA. Наилучшим является PCA с 21 колонками и результатом 0,864.

K Nearest Neighbor	
PCA	F1-score
29	0,863
27	0,863
25	0,862
23	0,863
21	0,864
19	0,859
17	0,858
15	0,858
13	0,855
11	0,849
9	0,842
7	0,825
5	0,785
3	0,759
1	0,636

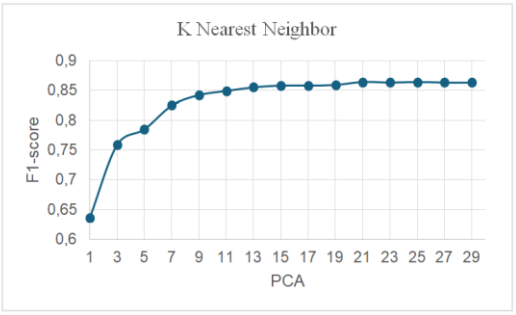


Рис. 9. Результаты изменения точности PCA K Nearest Neighdor

В табл. 3 представлены данные результатов исследования для выбранных моделей обучения.

Таблица 3

Сравнительная таблица результатов PCA

№	Модель	PCA	F1-score
1	Gradient Boosted Trees Learner	19	0,801
2	Decision Tree Learner	29	0,914
3	Tree Ensemble Learner	21	0,948
4	Random Forest Learner	27	0,975
5	K Nearest Neighbor	21	0,864

По результатам выбора наилучшей конфигурации PCA проведена настройка моделей машинного обучения. В табл. 4 представлены две модели машинного обучения на основе деревьев: Tree Ensemble Learner и Random Forest Learner

Таблица 4

Результаты исследования моделей Tree Ensemble Learner и Random Forest Learner

Tree Ensemble Learner	Дерево	Random Forest Learner	Дерево
Глубина дерева	Accuracy, %	Глубина дерева	Accuracy, %
20	83,926	20	84,598
25	87,774	25	87,652
30	90,878	30	90,388
35	93,112	35	92,396
40	94,855	40	93,992
45	95,897	45	95,208

Окончание табл. 4

50	96,465	50	96,172
55	96,799	55	96,663
60	97,072	60	97,011
65	97,103	65	97,031
70	97,11	70	97,039

Таким образом, две модели машинного обучения на основе деревьев: Tree Ensemble Learner и Random Forest Learner, показали близкий результат. При изменении настроек, обе модели выдавали лучшие результаты по мере увеличения глубины дерева, но при этом, достигнув определенного уровня, у моделей изменения стали минимальны. Это значит, что дальнейшее увеличение глубины может привести к тому, что деревья могут начать запоминать данные, следовательно, к переобучению.

В табл. 5 представлены результаты исследования модели машинного обучения K Nearest Neighbor.

Таблица 5

Результаты исследования модели K Nearest Neighbor

K Nearest Neighbor	
K	Accuracy, %
1	88,73
3	85,497
5	83,561
7	81,949
9	80,666

Таким образом, из таблицы видно, что наилучшим результатом является 3 ближайших соседа, которых следует учитывать.

В табл. 6 представлены результаты исследования модели машинного обучения Gradient Boosted Trees Learner.

Таблица 6

Результаты исследования модели Gradient Boosted Trees Learner

Gradient Boosted Tree Learner	
Глубина дерева	Accuracy, %
20	84,595
25	92,576
30	90,92
35	90,711
40	90,319

Таким образом, из таблицы видно, что наилучшим результатом будет глубина дерева равная 25.

В табл. 7 представлены результаты исследования модель машинного обучения Decision Tree Learner.

Таблица 7

Результаты исследования модели Decision Tree Learner

Decision Tree Learner	
Глубина дерева	Accuracy,%
1	0,863
3	0,863
5	0,862
7	0,863
9	0,864

Таким образом, из таблицы видно, что наилучшим результатом будет глубина дерева равная 1.

Таблица 8

Сравнительная таблица результатов исследования моделей

№	Модель	Accuracy, %
1	K Nearest Neighbor	85,497
2	Tree Ensemble Learner	97,11
3	Random Forest Learner	97,039
4	Decision Tree Learner	91,863
5	Gradient Boosted Trees Learner	92,576

Рассмотрим механизмы борьбы с переобучением. Исследуя модели машинного обучения, было замечено, что модель переобучается, поэтому возникла необходимость найти способ решения этой проблемы избегая замены датасета. В Knime есть отдельные блоки, которые предотвращают этот процесс, они позволяют выполнить кросс-валидацию, которая является стандартным методом для борьбы с переобучением. X-Partitioner и X-Aggregator – цикл перекрестной проверки, настроенный на пятикратное повторение. Это означает, что он делит набор данных на пять равных частей, и в каждой интеграции он использовал четыре части для обучения (80% данных) и одну часть для тестирования (20% данных). Узел X-Aggregator собирает все прогнозы на основе тестовых данных и предоставляет обобщенную оценку производительности модели [20].

Заключение. В настоящее время беспилотные летательные аппараты используют в различных сферах жизни: фермерство, доставка, строительство, видеосъемка и многое другое. Но использование БВС приносит человеку не только выгоду и удобство, но и проблемы. Например, проблемы с кибербезопасностью, конфиденциальностью и общественной безопасностью. БВС используются злоумышленниками для проведения физических и кибератак, что приводит к потере контроля над БВС и утечке важной информации. С ростом числа беспилотных систем усложняется идентификация и нейтрализация потенциально опасных устройств, создающих угрозу безопасности.

В работе проведено исследование методов обнаружения спуфинг-атак на БВС на основе машинного обучения. Наилучший результат показали модели Tree Ensemble Learner и Random Forest Learner, основанные на ансамблевом методе машинного обучения, показавшие результаты 97.110% И 97.039% соответственно. Это связанно с тем, что их особенностью является моделирование сложности задач в зависимости от данных, устойчивостью к шуму и высокой гибкостью. Предложенный подход отличается простотой реализации благодаря импользованию платформы Knime, которая позволяет решать алгоритмические блоки с предустановленным кодом. Это минимизирует необходимость глубоких знаний в программировании, позволяя сосредоточиться на оптимизации параметров моделей для повышения качества детектирования атак.

Благодарность: *Исследование выполнено за счет гранта Российского научного фонда № 25-71-30007, https://rscf.ru/project/25-71-30007/.*

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Савинкова С.А.* Разработка метода отслеживания перемещений объектов // Вестник современных исследований. – 2021. – №. 1-6. – С. 28-36.
2. GPS: глушилки, спуфинг и уязвимости // SavePearlHarbor. – URL: https://savepearlharbor.com/?p=264385 (дата обращения: 03.04.2025).
3. *Eldosouky A.R., Ferdowsi A., Saad W.* Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing // IEEE Internet of Things Journal. – 2019. – Vol. 7, No. 4. – P. 2840-2854.
4. *Khan S.Z., Mohsin M., Iqbal W.* On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions // PeerJ Computer Science. – 2021. – Vol. 7. – P. e507.
5. *Arthur M.P.* Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS // 2019 international conference on computer, information and telecommunication systems (CITS). – IEEE, 2019. – P. 1-5.
6. *Wesson K.D., Shepard D.P., Bhatti J.A., Humphreys T.E.* An evaluation of the vestigial signal defense for civil GPS anti-spoofing // Proceedings of the 24th International Technical Meeting of the Satellite Division of The institute of navigation (ION GNSS 2011). – 2011. – P. 2646-2656.
7. *Савинкова С.А.* Разработка метода отслеживания перемещений объектов // Вестник современных исследований. – 2021. – №. 1-6. – С. 28-36.
8. Спуфинг БВСов // Спуфинг БВСов (БВС). – URL: https://protectionsystem.ru/spoofing (дата обращения: 03.04.2025).
9. Иранские хакеры смогли получить управление американским БПЛА и посадить его на своей территории. – https://habr.com/ru/articles/135150/ (дата обращения: 05.06.2025).
10. *Humphreys T.* Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing // University of Texas at Austin (July 18, 2012). – 2012. – P. 1-16.
11. *Davidovich B., Nassi B., Elovici Y.* Towards the detection of GPS spoofing attacks against drones by analyzing camera's video stream // Sensors. – 2022. – Vol. 22, No. 7. – P. 2608.
12. What is machine learning? // IBM. – URL: https://www.ibm.com/think/topics/machine-learning (дата обращения: 03.04.2025).
13. Drone Communication Dataset // kaggle. – URL: https://www.kaggle.com/datasets/datasetengineer/drone-communication-dataset (дата обращения: 04.04.2025).
14. Что такое KNIME и как его использовать // Skypro. – URL: https://sky.pro/media/chto-takoe-knime-i-kak-ego-ispolzovat/ (дата обращения: 03.04.2025).
15. Gradient Boosted Trees Learner // Knime. – URL: https://hub.knime.com/knime/extensions/org.knime.features.ensembles/latest/org.knime.base.node.mine.treeensemble2.node.gradientboosting.learner.classification.GradientBoostingClassificationLearnerNodeFactory2 (дата обращения: 03.04.05).
16. Decision Tree Learner // Knime. – URL: https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.decisiontree2.learner2.DecisionTreeLearnerNodeFactory3 (дата обращения: 03.04.05).
17. Tree Ensemble Learner // Knime. – URL: https://hub.knime.com/knime/extensions/org.knime.features.ensembles/latest/org.knime.base.node.mine.treeensemble2.node.learner.classification.TreeEnsembleClassificationLearnerNodeFactory2 (дата обращения: 03.04.05).
18. Random Forest Learner // Knime. – URL: https://hub.knime.com/knime/extensions/org.knime.features.ensembles/latest/org.knime.base.node.mine.treeensemble2.node.randomforest.learner.classification.RandomForestClassificationLearnerNodeFactory2 (дата обращения: 03.04.05).
19. K Nearest Neighbor // Knime. – URL: https://hub.knime.com/knime/extensions/ org.knime.features.base/latest/org.knime.base.node.mine.knn.KnnNodeFactory2 (дата обращения: 03.04.05).
20. *Zul M.I., Yulia F., Nurmalasari D.* Social media sentiment analysis using K-means and naïve bayes algorithm // 2018 2nd International conference on electrical engineering and informatics (ICon EEI). – IEEE, 2018. – P. 24-29.

REFERENCES

1. *Savinkova S.A.* Razrabotka metoda otslezhivaniya peremeshcheniy ob"ektov [Development of a method for tracking the movement of objects], *Vestnik sovremennykh issledovaniy* [Bulletin of Modern Studies], 2021, No. 1-6, pp. 28-36.
2. GPS: glushilki, spufing i uyazvimosti [GPS: jammers, spoofing and vulnerabilities], *SavePearlHarbor*. Available at: https://savepearlharbor.com/?p=264385 (accessed 03 April 2025).
3. *Eldosouky A.R., Ferdowsi A., Saad W.* Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing, *IEEE Internet of Things Journal,* 2019, Vol. 7, No. 4, pp. 2840-2854.

4. *Khan S.Z., Mohsin M., Iqbal W.* On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions, *PeerJ Computer Science,* 2021, Vol. 7, pp. e507.
5. *Arthur M.P.* Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS, *2019 international conference on computer, information and telecommunication systems (CITS)*. IEEE, 2019, pp. 1-5.
6. *Wesson K.D., Shepard D.P., Bhatti J.A., Humphreys T.E.* An evaluation of the vestigial signal defense for civil GPS anti-spoofing, *Proceedings of the 24th International Technical Meeting of the Satellite Division of The institute of navigation (ION GNSS 2011),* 2011, pp. 2646-2656.
7. *Savinkova S.A.* Razrabotka metoda otslezhivaniya peremeshcheniy ob"ektov [Development of a method for tracking the movement of objects], *Vestnik sovremennykh issledovaniy* [Bulletin of modern studies], 2021, No. 1-6, pp. 28-36.
8. Spufing BVSov [Spoofing of UAVs], *Spufing BVSov (BVS)* [Spoofing of UAVs (UAVs)]. Available at: https://protectionsystem.ru/spoofing (accessed 03 April 2025).
9. Iranskie khakery smogli poluchit' upravlenie amerikanskim BPLA i posadit' ego na svoey territorii [Iranian hackers were able to gain control of an American UAV and land it on their territory]. Available at: https://habr.com/ru/articles/135150/ (accessed 05 June 2025).
10. *Humphreys T.* Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing, University of Texas at Austin (July 18, 2012), 2012, pp. 1-16.
11. *Davidovich B., Nassi B., Elovici Y.* Towards the detection of GPS spoofing attacks against drones by analyzing camera's video stream, *Sensors,* 2022, Vol. 22, No. 7, pp. 2608.
12. What is machine learning?, *IBM*. Available at: https://www.ibm.com/think/topics/machine-learning (accessed 04 April 2025).
13. Drone Communication Dataset, *kaggle*. Available at: https://www.kaggle.com/datasets/datasetengineer/drone-communication-dataset (accessed 04 April 2025).
14. Chto takoe KNIME i kak ego ispol'zovat' [What is KNIME and how to use it], *Skypro*. Available at: https://sky.pro/media/chto-takoe-knime-i-kak-ego-ispolzovat/ (accessed 03 April 2025).
15. Gradient Boosted Trees Learner, *Knime*. Available at: https://hub.knime.com/knime/extensions/org.knime.features.ensembles/latest/org.knime.base.node.mine.treeensemble2.node.gradientboosting.learner.classification.GradientBoostingClassificationLearnerNodeFactory2 (accessed 03 April 2025).
16. Decision Tree Learner, *Knime*. Available at: https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.decisiontree2.learner2.DecisionTreeLearnerNodeFactory3 (accessed 03 April 2025).
17. Tree Ensemble Learner, *Knime*. Available at: https://hub.knime.com/knime/extensions/org.knime.features.ensembles/latest/org.knime.base.node.mine.treeensemble2.node.learner.classification.TreeEnsembleClassificationLearnerNodeFactory2 (accessed 03 April 2025).
18. Random Forest Learner, *Knime*. Available at: https://hub.knime.com/knime/extensions/org.knime.features.ensembles/latest/org.knime.base.node.mine.treeensemble2.node.randomforest.learner.classification.RandomForestClassificationLearnerNodeFactory2 (accessed 03 April 2025).
19. K Nearest Neighbor, *Knime*. Available at: https://hub.knime.com/knime/extensions/org.knime.features.base/latest/org.knime.base.node.mine.knn.KnnNodeFactory2 (accessed 03 April 2025).
20. *Zul M.I., Yulia F., Nurmalasari D.* Social media sentiment analysis using K-means and naïve bayes algorithm, *2018 2nd International conference on electrical engineering and informatics (ICon EEI)*. IEEE, 2018, pp. 24-29.

Лапина Мария Анатольевна – Северо-Кавказский федеральный университет; e-mail: mlapina@ncfu.ru; г. Ставрополь, Россия; к.ф.-м.н.; доцент кафедры вычислительной математики и кибернетики; ORCID: 0000-0001-8117-9142.

Дымуха Регина Андреевна – Северо-Кавказский федеральный университет; e-mail: dymuharegina@gmail.com; г. Ставрополь, Россия; кафедра информационной безопасности автоматизированных систем; студент; ORCID: 0009-0005-2107-4636.

Кучеров Николай Николаевич – Северо-Кавказский федеральный университет; e-mail: nik.bekesh@gmail.com; г. Ставрополь, Россия; к.т.н.; ведущий научный сотрудник департамента науки Северо-Кавказского федерального университета; ORCID: 0000-0003-0337-0093.

Басан Елена Сергеевна – Южный федеральный университет; e-mail: ele-barannik@yandex.ru; г. Таганрог, Россия; к.т.н.; доцент кафедры безопасности информационных технологий им. О.Б. Макаревича,ORCID: 0000-0001-6127-4484.

Lapina Maria Anatolyevna – North Caucasus Federal University; e-mail: mlapina@ncfu.ru; Stavropol, Russia; cand. of phys. and math. sc.; associate professor of the Department of Computational Mathematics and Cybernetics; ORCHID: 0000-0001-8117-9142.

Dymuha Regina Andreevna – North Caucasus Federal University; e-mail: dymuharegina@gmail.com; Stavropol, Russia; the Department of Information Security of Automated Systems; student; ORCHID: 0009-0005-2107-4636.

Kucherov Nikolay Nikolaevich – North Caucasus Federal University; e-mail: nik.bekesh@gmail.com; Stavropol, Russia; cand. of eng. sc.; leading researcher at the Department of Science; ORCHID: 0000-0003-0337-0093.

Basan Elena Sergeevna – Southern Federal University; e-mail: ele-barannik@yandex.ru; Taganrog, Russia; cand. of eng. sc.; associate professor of the Information Technology Security Department named after O.B. Makarevich; ORCHID: 0000-0001-6127-4484.

УДК 004.891.2 DOI 10.18522/2311-3103-2025-3-31-41

А.Е. Анпилогова, В.А. Анпилогов

СИСТЕМА АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА И МОНИТОРИНГА ИНЦИДЕНТОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Автоматизация документооборота - ключевой элемент оптимизации процессов и повышения эффективности. Автоматизация документооборота на базе искусственного интеллекта улучшает управление инцидентами экономической безопасности, оптимизируя рабочие процессы и снижая затраты. Переход на автоматизированный документооборот в России связан со сложной нормативно-правовой базой и масштабными затратами на внедрение на предприятиях. Автоматизация помогает соблюдать требования законодательства и снижает риски юридических и финансовых последствий. Интеграция цифровых подписей повышает эффективность утверждения документов. Внедрение систем автоматизации поддерживает национальные цели цифровой трансформации. Автоматизация документооборота сокращает зависимость от бумажных процессов и способствует созданию централизованных цифровых хранилищ. Внедрение систем автоматизации документооборота требует стратегического подхода и тщательного планирования. Автоматизация документооборота обеспечивает экономию времени, сокращение ошибок и повышение соответствия нормативным стандартам. В статье рассмотрены теоретические основы BPM, интеграция цифровых технологий и нормативные аспекты, специфичные для России. Предложенная система сочетает мониторинг с ИИ и IoT, обеспечивает обработку данных в реальном времени, автоматизирует создание юридических документов и отчетов. Система автоматизации рабочих процессов базируется на интеграции данных, технологиях искусственного интеллекта и seamless-решениях. Система объединяет технологии мониторинга, алгоритмы распознавания лиц и анализа поведения, централизованную базу данных и модуль связи. Система формирует отчеты и юридические документы, заверенные QES, и обеспечивает взаимодействие с правоохранительными органами и службами безопасности. Результаты внедрения: снижение операционных расходов на 30–40% и уменьшение потерь на 50%. Система соответствует стандартам цифровой трансформации и поддерживает модернизацию национальной экономики.

Инцидент экономической безопасности; автоматизация документооборота; распознавание образов; анализа поведения; технлогии искусственного интеллекта.

A.E. Anpilogova, V.A. Anpilogov

A SYSTEM FOR AUTOMATING DOCUMENT FLOW AND MONITORING ECONOMIC SECURITY INCIDENTS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Automation of document flow is a key element of process optimization and efficiency improvement. Automation of document flow based on artificial intelligence improves the management of economic security incidents by optimizing work processes and reducing costs. The transition to automated document flow in Russia is associated with a complex regulatory framework and large-scale implementation costs at

enterprises. Automation helps to comply with legal requirements and reduces the risks of legal and financial consequences. Integration of digital signatures increases the efficiency of document approval. The implementation of automation systems supports national digital transformation goals. Automation of document flow reduces dependence on paper processes and facilitates the creation of centralized digital repositories. The implementation of document automation systems requires a strategic approach and careful planning. Document automation provides time savings, reduced errors and increased compliance with regulatory standards. The article discusses the theoretical foundations of BPM, integration of digital technologies and regulatory aspects specific to Russia. The proposed system combines monitoring with AI and IoT, provides real-time data processing, automates the creation of legal documents and reports. The workflow automation system is based on data integration, artificial intelligence technologies and seamless solutions. The system combines monitoring technologies, facial recognition and behavior analysis algorithms, a centralized database and a communication module. The system generates reports and legal documents certified by QES and ensures interaction with law enforcement agencies and security services. Implementation results: a 30–40% reduction in operating costs and a 50% reduction in losses. The system complies with digital transformation standards and supports the modernization of the national economy.

Economic security incident; document flow automation; pattern recognition; behavior analysis; artificial intelligence technologies.

Введение. Управление документацией долгое время было ключевым элементом организационной деятельности, но с развитием систем автоматизации документооборота произошла настоящая революция в этой сфере. Эти системы оптимизируют процессы создания, обработки и архивирования документов, интегрируя их с современными бизнес-методами. Для России переход на автоматизированный документооборот — это не только эффективное решение, но и необходимость из-за сложной нормативно-правовой базы и масштабных предприятий [1].

Системы автоматизации помогают соблюсти строгие требования законодательства, снижая риски юридических и финансовых последствий. Особенно это важно для крупных предприятий, таких как в энергетике и госуправлении, где автоматизация ускоряет обработку больших объемов документов, снижая ошибки и освобождая персонал для более важных задач. Интеграция цифровых подписей повышает эффективность утверждения документов. Внедрение таких систем также поддерживает национальные цели цифровой трансформации, такие как "Цифровая экономика Российской Федерации" [2]. Это сокращает зависимость от бумажных процессов и способствует созданию централизованных цифровых хранилищ, что важно для модернизации экономики и госуправления.

В этой статье рассматриваются тонкости внедрения систем автоматизации документооборота в России на примере инцидентов с неоплатой топлива. Анализируя задействованные технологические, нормативные и организационные факторы, исследование направлено на обеспечение всестороннего понимания того, как такие системы могут трансформировать практику документирования. Благодаря этому исследованию статья призвана предложить практическую информацию организациям, ориентирующимся на переход к автоматизации, а также внести свой вклад в продолжающийся диалог о цифровой трансформации в России.

Теоретические основы автоматизации. Автоматизация документооборота основана на ключевых теоретических основах из управления бизнес-процессами (BPM), информационных систем и технологий автоматизации [3]. Она является результатом цифровой трансформации, которая подразумевает переход от ручных бумажных процессов к цифровым решениям, что способствует повышению эффективности и улучшению организационных процессов [4]. Цифровая трансформация включает интеграцию цифровых технологий в различные сферы бизнеса, что кардинально изменяет операции и способы предоставления ценности клиентам. В России эта трансформация поддерживается государственной программой "Цифровая экономика Российской Федерации", которая направлена на модернизацию отраслей через внедрение цифровых технологий [2]. Эта инициатива создает теоретическую и практическую основу для перехода организаций на автоматизированные системы, обеспечивая соответствие бизнес-процессов современной цифровой инфраструктуре.

Теоретические основы автоматизации документооборота опираются на концепции управления бизнес-процессами, которые подчеркивают важность систематизированных рабочих процессов. В рамках BPM задачи выполняются по заранее установленным правилам, что в контексте документооборота включает утверждение документов, их проверку и архивирование. Автоматизация этих процессов устраняет задержки и узкие места, а также позволяет адаптировать рабочие процессы к требованиям организации и законодательству. Применение BPM в автоматизации документооборота позволяет эффективно мониторить и оптимизировать процессы. В отличие от традиционных систем, где трудно отслеживать поток документов, автоматизация предоставляет аналитику в реальном времени, что позволяет оперативно улучшать процессы на основе данных. Это соответствует принципу непрерывного совершенствования в BPM, где автоматизация является частью постоянных усилий по улучшению операционной деятельности [5].

Нормативные требования и автоматизация. В России строгие нормативные требования, такие как Федеральный закон № 402-ФЗ [6] (о бухгалтерском учете) и Федеральный закон № 152-ФЗ [7] (о защите персональных данных), определяют стандарты обработки, хранения и защиты документов. Несоответствие этим требованиям может привести к штрафам, что делает важным внедрение комплаенс-требований в системы управления документами [8].

Автоматизированные системы помогают решать сложные требования российского законодательства, например, Федеральный закон № 125-ФЗ [9] "Об архивном деле", который требует долгосрочного хранения определенных документов, таких как финансовые отчеты и трудовые договоры. Такие системы обеспечивают надежное хранение этих документов, снижая риск нарушений и улучшая управление рисками.

Кроме того, автоматизация документооборота снижает риски утечек данных, потери документов и несанкционированных изменений [10].

Системная интеграция и автоматизация. Последним теоретическим столпом, поддерживающим автоматизацию документооборота, является концепция системной интеграции [11]. Современные организации полагаются на различные информационные системы — от платформ планирования ресурсов предприятия (ERP) до платформ управления взаимоотношениями с клиентами (CRM) — для управления своими операциями. Системы автоматизации документооборота наиболее эффективны, когда они легко интегрируются с существующими системами, создавая единую цифровую среду, в которой данные могут свободно передаваться между различными подразделениями и функциями [12].

Теория системной интеграции подчеркивает важность интероперабельности – способности различных систем работать вместе, не требуя интенсивного ручного вмешательства [13]. Для российских организаций это особенно важно из-за широкого использования устаревших систем, которые изначально могут не поддерживать современные технологии автоматизации.

Далее мы сосредоточимся на описании разработанной нами системы, демонстрирующей ее передовые возможности и практическое применение.

Архитектура и функциональность системы. Архитектура системы автоматизации рабочих процессов базируется на интеграции данных, искусственном интеллекте и seamless-решениях, обеспечивающих эффективное управление инцидентами в режиме реального времени. Система объединяет технологии мониторинга, включая камеры наблюдения и IoT-датчики, чтобы собирать данные из нескольких источников. Алгоритмы распознавания лиц и анализа поведения позволяют выявлять аномалии, такие как подозрительные действия или использование поддельных номеров, прогнозируя потенциальные риски с высокой точностью [14].

Для обработки данных используется централизованная база, которая служит хранилищем для всех записей – временных меток, видеоматериалов, информации о нарушениях. Она также поддерживает интеграцию с внешними системами, например, государственными базами, что расширяет возможности принятия решений и правоприменения. Процесс документирования автоматизирован: система формирует отчеты и юридические документы, заверенные QES для соблюдения нормативных стандартов.

Модуль связи обеспечивает взаимодействие между платформой, правоохранительными органами и службами безопасности, позволяя передавать уведомления, отчеты и обновления в реальном времени. Прогнозная аналитика, встроенная в систему, выявляет сценарии высокого риска, что позволяет стратегически распределять ресурсы, сокращая число инцидентов и повышая операционную эффективность. Система построена на принципах сквозной автоматизации, надежности и нормативного соответствия [15]. Она исключает ручное вмешательство, автоматизируя сбор данных, обнаружение аномалий, создание документов и отчетов, что оптимизирует рабочий процесс. Благодаря защищенным цифровым подписям и интеграции с внешними базами данных система соответствует нормативным стандартам.

Модульная архитектура обеспечивает гибкость и интеграцию с существующей инфраструктурой, включая видеонаблюдение и внешние базы данных. Автоматизация рутинных процессов снижает эксплуатационные расходы на 30–40%, а прогнозная аналитика и обнаружение аномалий помогают сократить потери, связанные с кражами и нарушениями, на 50%. Например, это включает потери топлива, недостачи товаров, незаконное проникновение на объекты и другие риски, приводящие к финансовым убыткам.

Практическое применение системы. Практическое применение системы демонстрирует ее эффективность: она подключает камеры наблюдения, IoT-устройства и алгоритмы ИИ к централизованной базе данных, создавая бесперебойный процесс управления инцидентами. Например, при краже топлива система анализирует видеозаписи, сопоставляет данные с базами нарушителей, генерирует отчет с цифровой подписью и передает его правоохранительным органам в реальном времени.

Первым шагом является получение уведомления от кассы о том, что состоялось нарушение, касса передает начальные данные о номере колонки, времени и другую информацию, которая может быть необходима.

Псевдокод операции (листинг 1):

```
    Функция get_violation_notification():
        Описание:
            Получает уведомление о нарушении с кассы.
        Возвращает:
            Словарь с информацией о нарушении (номер колонки,
время и т.д.)
        Шаг 1: Установить URL для запроса.
        Шаг 2: Выполнить HTTP-запрос к URL.
            Если запрос успешен (код ответа 200):
                Шаг 3: Преобразовать ответ в JSON.
                Шаг 4: Проверить, является ли результат словарём.
                    Если результат корректен: вернуть словарь.
                    Если результат не корректен: вернуть ошибку
«Не удалось получить уведомление о нарушении».
```

Листинг 1 – Операция получения уведомления

Далее системе необходимо извлечь кадр из видео для его последующего анализа (листинг 2).

```
    Функция analyze_video(video_path, timestamp):
        Описание:
            Извлекает кадр из видео на основе времени нарушения
и сохраняет его как изображение.
        Входные данные:
            video_path (строка): Путь к видеозаписи.
            timestamp (строка): Время нарушения (в секундах).
```

```
        Выходные данные:
            Путь к изображению нарушения (строка).
        Алгоритм:
        1. Открыть видеозапись, используя указанный путь
(video_path).
        2. Получить частоту кадров (frame_rate) из видео.
        3. Рассчитать номер кадра (frame_number) по формуле:
               frame_number = frame_rate * timestamp.
        4. Установить позицию воспроизведения видео на указанный
кадр (frame_number).
        5. Считать кадр:
            Если кадр успешно считан:
                Сохранить кадр как изображение (например,
"incident_image.jpg").
                Вернуть путь к сохраненному изображению.
            Если возникла ошибка:
                Вернуть ошибку «Не удалось извлечь кадр из видео».
```

Листинг 2 – Извлечение кадра из видео

Следующим шагом идет извлечение номера машины из фотографии. Для этого используются методы компьютерного зрения и распознавания текста (листинг 3).

```
    Функция open_img(img_path):
        Описание: Открывает изображение по заданному пути и ото-
бражает его.
        1. Прочитать изображение по пути img_path.
        2. Преобразовать изображение из BGR в RGB.
        3. Отключить оси графика.
        4. Отобразить изображение.
        5. Вернуть изображение.
    Функция carplate_extract(image, carplate_haar_cascade):
        Описание: Извлекает номерной знак с использованием кас-
када Хаара.
        1. Применить каскад Хаара для обнаружения объектов (но-
мерных знаков) на изображении.
        2. Для каждого обнаруженного прямоугольника:
            - Вырезать область изображения, соответствующую но-
мерному знаку.
        3. Вернуть вырезанный фрагмент изображения.
    Функция enlarge_img(image, scale_percent):
        Описание: Увеличивает изображение на заданный процент.
        1. Рассчитать новые размеры изображения:
            - Ширина = текущая ширина * (scale_percent / 100).
            - Высота = текущая высота * (scale_percent / 100).
        2. Изменить размер изображения.
        3. Вернуть изменённое изображение.
    Функция preprocess_image(image):
        Описание: Предобрабатывает изображение для дальнейшего
анализа.
        1. Преобразовать изображение в оттенки серого.
        2. Применить размытие Гаусса для устранения шума.
        3. Применить пороговую фильтрацию (Оцу) для бинаризации
изображения.
        4. Вернуть бинаризованное изображение.
```

```
    Основная функция main():
        Описание: Основной процесс извлечения и распознавания
номерного знака.
        1. Вызвать open_img для открытия изображения.
        2. Загрузить каскад Хаара для распознавания номерного
знака.
        3. Вызвать carplate_extract для извлечения номерного
знака из изображения.
        4. Вызвать enlarge_img для увеличения изображения номер-
ного знака.
        5. Отобразить увеличенное изображение номерного знака.
        6. Преобразовать изображение номерного знака в оттенки
серого.
        7. Применить функцию preprocess_image для бинаризации
изображения.
        8. Отобразить бинаризованное изображение.
        9. Использовать pytesseract для распознавания текста
(номерного знака) на бинаризованном изображении.
        10. Вывести распознанный номер автомобиля.
    Функция open_img(img_path):
        Описание: Открывает изображение по заданному пути и ото-
бражает его.
```

Листинг 3 – Извлечение номера машины из фотографии

В данном примере используется метод Хаар каскада с пред обученной моделью распознавания автомобильных номеров на изображении [16] (рис. 1), и распознавание текста.

Рис. 1. Распознаваемый автомобильный номер

Система распознает на кадре автомобиль, дальше проходясь по своим инструкциям, выдает нам обрезанное изображение с номером. Далее для простоты изображение переводится в черно-белый формат (рис. 2).

Рис. 2. Выделенный автомобильный номер

И уже с таким изображением работает распознавание текста, в конечном результате мы получаем вывод: “A000AA00”. Следующим шагом является занесение всех имеющихся данных в базу данных (листинг 4).

```
    Функция insert_violation_into_db(pump_id, timestamp,
car_number, image_path):
        Описание: Вставляет информацию о нарушении в базу данных.
        1. Открыть соединение с базой данных:
            - Подключиться к базе данных с использованием пре-
доставленных данных (имя базы данных, пользователь, пароль,
хост, порт).
        2. Создать курсор для выполнения SQL-запросов.
        3. Сформировать SQL-запрос для вставки данных:
            - SQL-запрос: Вставить данные о нарушении (номер ко-
лонки, время нарушения, номер машины и путь к изображению).
        4. Выполнить SQL-запрос, передав параметры:
            - Запрос выполняется с переданными значениями
(pump_id, timestamp, car_number, image_path).
        5. Применить изменения (коммит) в базе данных.
        6. Закрыть курсор и соединение с базой данных.
```

Листинг 4 – Занесение всех имеющихся данных в БД

Далее необходимо по шаблону сгенерировать документ, который будет в последствии отправлен органам власти (листинг 5).

```
    Функция generate_official_request(pump_id, timestamp,
amount, car_number, image_path):
        Описание: Генерирует официальный запрос в формате DOCX.
        1. Создать новый документ:
            Использовать библиотеку для работы с DOCX (например,
python-docx).
        2. Добавить заголовок:
            Добавить заголовок «Официальный запрос о краже топ-
лива» в верхней части документа.
        3. Добавить введение:
            Добавить текст с обращением к сотрудникам правоохра-
нительных органов.
        4. Добавить описание нарушения:
            Вставить информацию о заправке, колонке, времени на-
рушения, сумме и номере машины.
        5. Вставить изображение:
            Добавить изображение нарушения (фото) с указанного
пути с определённым размером.
        6. Сохранить документ:
            Сохранить сгенерированный документ в формате DOCX по
указанному пути (например, 'official_request.docx').
```

Листинг 5 – Генерация документа по шаблону

И последним шагом является отправка сгенерированного отчета по почте, например с использованием SMTP сервера от Яндекса (листинг 6).

```
    Функция send_email(to_addr, subject, text, attachments):
        Описание: Отправляет электронное письмо с вложениями.

        1. Создать объект сообщения:
            - Использовать MIMEMultipart для создания сообщения,
которое будет содержать текст и вложения.
```

```
        2. Установить заголовки сообщения:
            - Установить адрес отправителя ('From').
            - Установить адрес получателя ('To').
            - Установить тему письма ('Subject').
        3. Добавить основной текст письма:
            - Использовать MIMEText для добавления текста письма
с кодировкой 'utf-8'.
        4. Добавить вложения:
            - Для каждого пути вложения из списка:
                - Создать MIMEBase объект для передачи бинарных
данных.
                - Открыть файл и установить его данные как по-
лезную нагрузку.
                - Применить кодировку base64 для файла.
                - Добавить заголовок с названием вложения.
                - Прикрепить файл к сообщению.
        5. Подключиться к SMTP-серверу:
            - Создать соединение с SMTP-сервером (например, с
сервером Yandex).
            - Включить TLS для защиты соединения.
            - Авторизоваться на сервере.
            - Отправить сообщение.
            - Завершить сессию.
```

Листинг 6 – Отправка сгенерированного отчета

Далее представлена диаграмма последовательности (диаграмма 1).

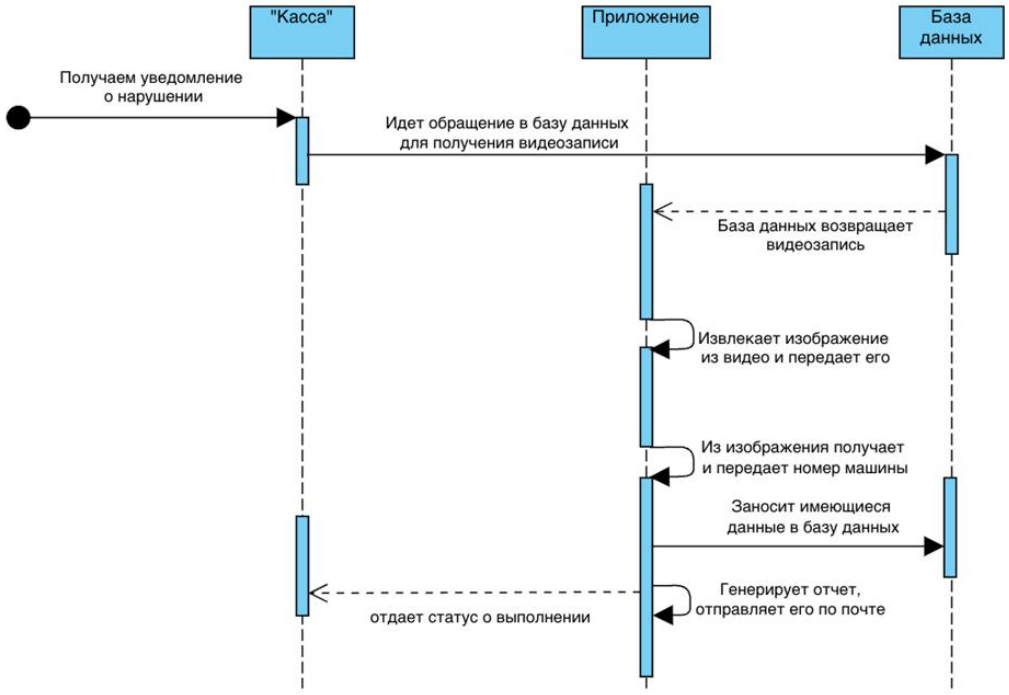


Диаграмма 1 – Диаграмма последовательности

Преимущества и вызовы автоматизации. Внедрение систем автоматизации рабочего процесса приносит значительные преимущества, такие как экономия времени, сокращение ошибок и повышение соответствия нормативным стандартам через безопасную обработку документов. Однако при этом возникают определенные вызовы, включая необходимость обеспечения безопасности данных, высокие начальные затраты на настройку и проблемы с интеграцией с устаревшими системами [17]. Эти проблемы требуют стратегического подхода и тщательного планирования.

С технической стороны система использует сложный стек технологий, включая искусственный интеллект (ИИ), машинное обучение (ML), оптическое распознавание символов (OCR) и интеграцию через API для обработки и обмена данными в реальном времени. Для обеспечения успешной работы системы критически важны такие факторы, как высокая доступность, удобство обслуживания и надежность. Высокая доступность гарантирует бесперебойную работу, удобство обслуживания – возможность адаптации к меняющимся требованиям, а надежность – стабильность функционирования, что критично для поддержания доверия и эффективности в условиях сложных операционных процессов [18].

Оценка системы автоматизации документооборота в контексте управления инцидентами включает ключевые показатели: время обработки, частота ошибок и удовлетворенность пользователей. Время обработки измеряет скорость выявления и уведомления о нарушениях, частота ошибок – точность системы в обнаружении аномалий, а удовлетворенность пользователей оценивает удобство и оперативность.

Будущее этих систем связано с ключевыми тенденциями [19], такими как интеграция блокчейна для повышения безопасности данных и улучшения доверия между организациями. Также достижения в области искусственного интеллекта и интернета вещей улучшат обработку данных в реальном времени, делая системы более эффективными и интеллектуальными.

Выводы и рекомендации по внедрению. Внедрение систем автоматизации документооборота представляет собой значительный шаг вперед для организаций, стремящихся повысить свою операционную эффективность, точность и соответствие нормативным требованиям. Это исследование акцентирует внимание на архитектуре, функциональности и принципах таких систем, подчеркивая их способность оптимизировать сложные процессы через сквозную автоматизацию. Использование передовых технологий, таких как искусственный интеллект, машинное обучение и интернет вещей, позволяет существенно сократить время отклика, снизить эксплуатационные расходы и минимизировать потери, связанные с кражами и мошенничеством.

Одним из основных преимуществ предложенной системы является ее способность значительно сократить экономические издержки. За счет автоматизации таких рутинных процессов, как отчетность об инцидентах, обнаружение аномалий и управление базами данных, операционные расходы могут быть снижены на 30-40%. Кроме того, потери от краж, включая кражу топлива, могут быть уменьшены на 50%, что обеспечит более быструю окупаемость инвестиций. Такая экономия не только оправдывает первоначальные затраты на внедрение, но и позволяет компаниям эффективно перераспределять ресурсы на цели роста и инновации.

Из этого исследования вытекает несколько практических рекомендаций для организаций, рассматривающих возможность автоматизации. Во-первых, уделите приоритетное внимание интеграции искусственного интеллекта и прогнозной аналитики для упреждающего устранения рисков и оптимизации распределения ресурсов. Во-вторых, обеспечьте надежные меры безопасности данных, включая шифрование и технологии блокчейн, для защиты конфиденциальной информации и обеспечения соответствия нормативным требованиям [20]. В-третьих, инвестируйте в системы обучения и поддержки сотрудников и заинтересованных сторон, чтобы максимально повысить удобство использования системы и ее принятие. Наконец, оцените масштабируемость решения, чтобы убедиться, что оно остается адаптируемым к меняющимся потребностям бизнеса и технологическим достижениям.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рынок СЭД/ECM-систем в России: аналитический отчет TAdviser // TAdviser.ru. – 2023. – URL: https://www.tadviser.ru/a/465353 (дата обращения: 10.12.2024).
2. Цифровая экономика Российской Федерации. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: https://digital.gov.ru (дата обращения: 10.12.2024).
3. *Kirchmer M*. High-Performance Through Business Process Management: Strategy Execution in a Digital World. – Springer, 2021. – 235 p.
4. *Mergel I., Edelmann N., Haug* N. Defining digital transformation: Results from a systematic literature review // Government Information Quarterly. – 2022. – Vol. 39, No. 4. – P. 101550.
5. *vom Brocke J., Mendling J., Rosemann M. (eds.).* Business Process Management Cases: Digital Innovation and Business Transformation in Practice. – Springer, 2021. – 768 p.
6. Федеральный закон № 402-ФЗ "О бухгалтерском учете".
7. Федеральный закон № 152-ФЗ "О персональных данных".
8. *Anagnostopoulos I.* FinTech and RegTech: Impact on regulators and banks // Journal of Economics and Business. –2020. – Vol. 100. – P. 105832.
9. Федеральный закон № 125-ФЗ "Об архивном деле".
10. SIEM и Log Management: обзор решений для управления безопасностью. Cloudnetworks.ru. – URL: https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/ (дата обращения: 10.12.2024).
11. *Lacity M.C., Willcocks L.P.* Robotic Process Automation and Risk Mitigation. – Palgrave Macmillan, 2020. – 213 p.
12. *Richards M*. Fundamentals of Software Architecture: An Engineering Approach. – O'Reilly Media, 2020. – 412 p.
13. *Weske M.* Business Process Management: Concepts, Languages, Architectures. – 3rd ed. – Springer, 2020. – 03 p.
14. *van der Aalst W.M. et al.* Object-Centric Process Mining: Dealing with Divergence and Convergence in Data // ACM Transactions on Management Information Systems. – 2023. – Vol. 14, No. 2. – P. 1-35.
15. *Mansar S. L., Reijers H.A.* Best Practices in Business Process Redesign // Business Process Management Journal. – 2023. – Vol. 15, No. 4. – P. 38-50.
16. *Koci V., Horalek J., Kuchar M.* A review of license plate recognition methods based on deep learning // IEEE Access. – 2023. – Vol. 11. – P. 54311-54330.
17. *Syed R., Suriadi S., Adams M., Bandara W.* A systematic literature review of the challenges of implementing Robotic Process Automation (RPA) // Communications of the Association for Information Systems. – 2020. – Vol. 47, No. 1. – P. 12.
18. Top Strategic Technology Trends 2024 // Gartner. – 2023. – URL: https://www.gartner.com/en/information-technology/insights/top-technology-trends (дата обращения: 10.12.2024).
19. Gartner. BPM Trends. – URL: https://www.gartner.com (дата обращения: 10.12.2024).
20. *Casino F., Dasaklis T. K., Patsakis C.* A systematic literature review of blockchain-based applications: Current status, classification and open issues // Telematics and Informatics. – 2020. – Vol. 52. – P. 101412.

REFERENCES

1. Rynok SED/ECM-sistem v Rossii: analiticheskiy otchet TAdviser [Market of EDMS/ECM systems in Russia: analytical report of TAdviser], *TAdviser.ru,* 2023. Available at: https://www.tadviser.ru/a/465353 (accessed 10 December 2024).
2. TSifrovaya ekonomika Rossiyskoy Federatsii. Ofitsial'nyy sayt Ministerstva tsifrovogo razvitiya, svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii. Available at: https://digital.gov.ru (accessed 10 December 2024).
3. *Kirchmer M*. High-Performance Through Business Process Management: Strategy Execution in a Digital World. Springer, 2021, 235 p.
4. *Mergel I., Edelmann N., Haug* N. Defining digital transformation: Results from a systematic literature review, *Government Information Quarterly,* 2022, Vol. 39, No. 4, pp. 101550.
5. *vom Brocke J., Mendling J., Rosemann M. (eds.).* Business Process Management Cases: Digital Innovation and Business Transformation in Practice. Springer, 2021, 768 p.
6. Federal'nyy zakon № 402-FZ "O bukhgalterskom uchete" [Federal Law No. 402-FZ "On Accounting"].
7. Federal'nyy zakon № 152-FZ "O personal'nykh dannykh" [Federal Law No. 152-FZ "On Personal Data"].
8. *Anagnostopoulos I.* FinTech and RegTech: Impact on regulators and banks, *Journal of Economics and Business,*2020, Vol. 100, pp. 105832.
9. Federal'nyy zakon № 125-FZ "Ob arkhivnom dele" [Federal Law No. 125-FZ "On Archival Affairs"].

10. SIEM i Log Management: obzor resheniy dlya upravleniya bezopasnost'yu [SIEM and Log Management: an overview of security management solutions]. Cloudnetworks.ru. Available at: https://cloudnetworks.ru/inf-bezopasnost/siem-log-management/ (accessed 10 December 2024).
11. *Lacity M.C., Willcocks L.P.* Robotic Process Automation and Risk Mitigation. Palgrave Macmillan, 2020, 213 p.
12. *Richards M*. Fundamentals of Software Architecture: An Engineering Approach. O'Reilly Media, 2020, 412 p.
13. *Weske M.* Business Process Management: Concepts, Languages, Architectures. 3rd ed. Springer, 2020, 03 p.
14. *van der Aalst W.M. et al.* Object-Centric Process Mining: Dealing with Divergence and Convergence in Data, *ACM Transactions on Management Information Systems,* 2023, Vol. 14, No. 2, pp. 1-35.
15. *Mansar S. L., Reijers H.A.* Best Practices in Business Process Redesign, *Business Process Management Journal,* 2023, Vol. 15, No. 4, pp. 38-50.
16. *Koci V., Horalek J., Kuchar M.* A review of license plate recognition methods based on deep learning, *IEEE Access,* 2023, Vol. 11, pp. 54311-54330.
17. *Syed R., Suriadi S., Adams M., Bandara W.* A systematic literature review of the challenges of implementing Robotic Process Automation (RPA), *Communications of the Association for Information Systems,* 2020, Vol. 47, No. 1, pp. 12.
18. Top Strategic Technology Trends 2024, *Gartner,* 2023. Available at: https://www.gartner.com/en/information-technology/insights/top-technology-trends (accessed 10 December 2024).
19. Gartner. BPM Trends. Available at: https://www.gartner.com (accessed 10 December 2024).
20. *Casino F., Dasaklis T. K., Patsakis C.* A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics,* 2020, Vol. 52, pp. 101412.

Анпилогова Анастасия Евгеньева – ЮРИУ РАНХиГС; e-mail: abramoves.ae@gmail.com; г. Ростов-на-Дону, Россия; тел.: +79889402282; экономический факультет (экономическая безопасность); студент.

Анпилогов Виктор Александрович – Южный федеральный университет, e-mail: vanpilogov@sfedu.ru; г. Таганрог, Россия; тел.: +79885744400; кафедра вычислительной техники; магистрант.

Anpilogova Anastasia Evgenyeva – URUI RANEPA; e-mail: abramoves.ae@gmail.com; Rostov-on-Don, Russia; phone: +79889402282; Faculty of Economics (Economic Security); student.

Anpilogov Viktor Aleksandrovich – Southern Federal University; e-mail: vanpilogov@sfedu.ru; Taganrog, Russia; phone: +79885744400; the Department of Computer Science; master's student.

УДК 004.056 DOI 10.18522/2311-3103-2025-3-41-54

И.А. Ерёмин, А.Е. Якушина, И.Л. Щербов

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

В рамках данного исследования была детально проанализирована типовая структура объекта информатизации, что позволило квалифицированным специалистам глубже понять механизмы и аспекты, посредством которых различные категории объектов и субъектов обработки информации, которые могут подвергаться угрозам безопасности. Основным механизмом построения комплексной системы защиты информации является модель угроз. Данная модель направлена на выявление и идентификацию потенциальных угроз, их последующий анализ и минимизации рисков их реализации, связанных с нанесением ущерба объекту информатизации. В рамках настоящего исследования для построения модели угроз рассмотрены отечественная база знаний ФСТЭК и международные базы знаний ATT&CK и CAPEC, содержащие в себе исчерпывающую информацию о тактиках и техниках, применяемых злоумышленниками при осуществлении атак на объекты информатизации. В процессе исследования были детально классифицированы различные тактики, используемые злоумышленниками. Особое внимание уделялось определению основных тактик, определяющих точки входа объекта информатизации, которые используются для дальнейшего проведения атаки. В контексте разработки эффективной модели угроз представляется целесообразным проведение комплексного анализа данных, содержащихся в базах знаний, и их

последующего совместного использования в процессе построения модели угроз на объектах информатизации. Данный подход позволяет систематизировать и структурировать информацию, что способствует более точному и обоснованному построению модели осуществления потенциальных угроз на разных этапах атаки на объект информатизации. Для построения комплексной системы защиты информации была рассмотрена система поддержки принятия решений. Проведен анализ современных научных исследований, посвященных применяемым методам при построении систем поддержки. В результате работы была приведена взаимосвязь между базами знаний тактик и техник, а также общеизвестных уязвимостей методом онтологии, которая позволяет построить модель комплексной атаки угрозы, и определить объекты воздействия, на которые воздействует злоумышленник на различных этапах комплексной атаки, критичность применяемой уязвимости и платформы, на которой данная уязвимость реализуема, и определение негативных последствий.

Объект информатизации; комплексная система защиты информации; модель угроз; тактики и техники атак; неопределенность данных; система поддержки принятия решений.

I.A. Eremin, A.E. Yakushina, . I.L. Sherbov

MODELING OF SECURITY THREATS FOR BUILDING A COMPREHENSIVE INFORMATION PROTECTION SYSTEM AT OBJECT OF INFORMATIZATION

Within the framework of this study, the typical structure of the informatization facility was analyzed in detail, which allowed qualified specialists to better understand the mechanisms and aspects through which various categories of objects and subjects of information processing that may be subject to security threats. The main mechanism for building a comprehensive information security system is the threat model. This model is aimed at identifying and identifying potential threats, their subsequent analysis and minimizing the risks of their implementation associated with damage to the informatization facility. In the framework of this study, the domestic FSTEC knowledge base and the international ATT&CK and CAPEC knowledge bases are considered to build a threat model. They contain comprehensive information about the tactics and techniques used by intruders in carrying out attacks on informatization facilities. In the course of the research, various tactics used by the attackers were classified in detail. Special attention was paid to the definition of the main tactics that determine the entry points of the informatization object, which are used to further carry out the attack. In the context of developing an effective threat model, it seems advisable to conduct a comprehensive analysis of the data contained in knowledge bases and their subsequent joint use in the process of building a threat model at informatization facilities. This approach makes it possible to systematize and structure information, which contributes to a more accurate and reasonable construction of a model for the implementation of potential threats at different stages of an attack on an informatization facility. To build a comprehensive information security system, a decision support system was considered. The analysis of modern scientific research devoted to the applied methods in the construction of support systems is carried out. As a result of the work, the relationship between knowledge bases of tactics and techniques, as well as well-known vulnerabilities, was shown using the ontology method, which allows us to build a model of a complex threat attack, and identify the targets affected by an attacker at various stages of a complex attack, the criticality of the vulnerability used and the platform on which this vulnerability is implemented, and the definition of negative consequences.

Object of informatization, an integrated information security system, a threat model, tactics and techniques of attacks, data uncertainty, a decision support system.

Введение. Указом Президента Российской Федерации от 2 июля 2021 г. № 400 утверждена стратегия национальной безопасности Российской Федерации. Информационная безопасность впервые выделена в качестве одного из стратегических национальных приоритетов, направленных на обеспечение и защиту национальных интересов Российской Федерации. В стратегии целью обеспечения информационной безопасности определено укрепление суверенитета Российской Федерации в информационном пространстве [1].

Состояние информационной безопасности характеризуется постоянным, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности государства [2].

Защита информации на объектах информатизации (ОИ) с целью противодействия киберпреступности является составной частью обеспечения национальной безопасности. Решение данной задачи базируется на проведении детального анализа действующего ОИ и осуществлении оценки риска для обеспечения защиты уязвимостей активов от вероятных угроз [3].

Согласно ГОСТ Р 51275-2006, объект информатизации (ОИ) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [4].

В общем виде структура ОИ представлена на рис. 1.

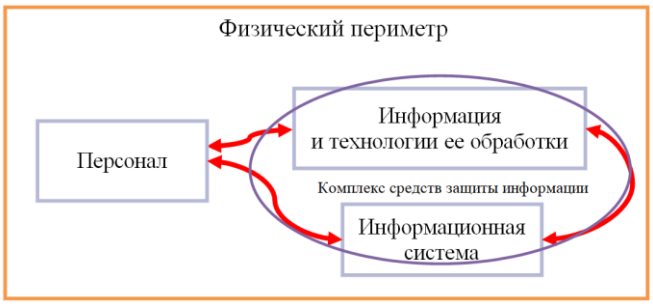


Рис. 1. Структура объекта информатизации

Учитывая, что построение комплексной системы защиты информации (КСЗИ) на ОИ начинается с инвентаризации активов, рассмотрим их более детально.

1. Физический периметр определяется как система, включающий в себя нормативно-правовые документы, инженерно-технические конструкции, структурные подразделения, целью которых является обеспечение физической безопасности объекта информатизации. Данная система направлена на предотвращение несанкционированного проникновения в здания (на территорию), минимизацию рисков повреждения инфраструктуры и нейтрализацию внешних угроз.

2. Информационная система представляют собой совокупность взаимосвязанных элементов и включает в себя аппаратные средства, сетевое оборудование, программно-аппаратные платформы и прикладное программное обеспечение. Её функциональное назначение заключается в выполнении основных задач, направленных на выполнение уставных функций организации.

3. Информация и технологии её обработки взаимосвязана с вычислительной системой, выступая ключевым активом для выполнения как производственных, так и управленческих функций организации. Эта взаимозависимость обусловлена тем, что процессы обработки, хранения и передачи данных реализуются исключительно через работу программных и аппаратно-программных компонентов вычислительной системы.

4. КСЗИ включает в себя специализированные технические устройства, программные обеспечения и программно-аппаратные компоненты выполняющие функции защиты информации от утечки по техническим каналам и защиты от несанкционированного доступа.

5. Персонал включает в себя, работников, связанных с организацией договорными отношениями (трудовой договор, контракт и т.п.). К этой категории следует относить как работников, числящихся по штатному расписанию организации, так и работников других учреждений, выполняющих в организации те или иные виды работ. Это могут быть работники частных охранных компаний, клиринговых компаний и т.д.

Каждый актив ОИ может иметь уязвимости, при условии внешнего воздействия (реализации угрозы), на которые возможно наступление негативных последствий, выраженных в нарушении конфиденциальности, целостности или доступности информации.

Противодействие подобным внешним воздействиям (угрозам) требует осуществление системного анализа и декомпозиции целей атакующего, исследования функциональных возможностей вредоносного программного обеспечения (ВПО) и реконструкцию последовательности его воздействия на активы ОИ, шаблонов атак и используемых тактик и техник, уязвимостей программного обеспечения и оборудования. Результатом данного анализа является формализованный документ – модель угроз (МУ). Данная модель является основополагающим этапом проектирования многоуровневых защитных механизмов, направленных на блокировку конкретных векторов атак, минимизацию реализации угроз и снижение рисков нанесения ущерба организации.

Методы и методики исследования. В данном исследовании проведен анализ тактик и техник атак на объекты информатизации применяемых злоумышленниками, с целью максимально эффективного использования предоставленной в них информации, для формирования модели угроз информации во время проектирования КСЗИ на ОИ.

В методическом документе ФСТЭК «Методика оценки угроз безопасности» от 5 февраля 2021 г. определен перечень тактик и техник угроз (ТТУ), который описывает возможную классификацию тактик и техник злоумышленника при применении им атак на объекты воздействий информационной инфраструктуры. Данная классификация адаптирована к национальным требованиям и регуляторным нормам, сохраняя концептуальное сходство с международными аналогами.

Тактика – это цель, которую ставит перед собой злоумышленник на различных этапах, при осуществлении атаки на информационную инфраструктуру. Техника описывает, конкретные методы и приемы того, как злоумышленник добиться цели применения выбранной тактики.

Проанализируем тактики, применяемые злоумышленниками отображенные в перечне ТТУ ФСТЭК (табл. 1) [5].

Таблица 1

Анализ тактик ТТУ ФСТЭК

№ П/п	Тактика	Цель	Описание
Т1	Сбор информации о системах и сетях	Получении информации для планирования последующих этапов атаки	Злоумышленник применяет пассивные и активные методы для сбора технических данных о целевой инфраструктуре
Т2	Получение первоначального доступа к компонентам систем и сетей	Создание точки входа для дальнейшего продвижения в сети	Предполагает эксплуатацию уязвимостей сетевых служб, фишинговых атак или подбора учетных данных для получения доступа к узлам инфраструктуры
Т3	Внедрение и исполнение ВПО в система и сетях	Эксплуатация ВПО и направлена на выполнение несанкционированных операций на локальных или удаленных ресурсах	Злоумышленник осуществляет инъекцию вредоносного кода в целевую систему через уязвимые интерфейсы или обманные методы

Окончание табл. 1

№ П/п	Тактика	Цель	Описание
Т4	Закрепление (сохранение доступа) в системе или сети	Получения постоянного доступа в целевую систему	После получения первоначального доступа, злоумышленник пытается закрепиться в системе посредством кражи существующих учетных данных или созданию новых учетных данных, добавление ВПО в автозагрузку
Т5	Управление ВПО и (или) компонентами, к которым ранее был получен доступ	Автоматизация управления ВПО и выполнения удаленных команд	После успешного закрепления на узле, злоумышленник, организует взаимодействие между скомпрометированным узлом и командным сервером злоумышленника
Т6	Повышение привилегий по доступу к компонентам систем и сетей	Выполнение действий требующих повышенных разрешений	Повышение привилегий состоит из методов, которые злоумышленники используют для получения разрешений более высокого уровня в системе или сети
Т7	Сокрытие действий и применяемых при этом средств от обнаружения	Скрытие действий атаки на всем этапе компрометации.	Скрытие от обнаружения и предотвращения средствами защиты
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям	Распространение доступа на другие компоненты инфраструктуры	Злоумышленник может использовать различные методы для кражи данных с узла, при этом используя методы по предотвращению обнаружения и защиты
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз	Нарушение конфиденциальности информации	Злоумышленник может использовать различные методы для кражи данных с узла, при этом используя методы по предотвращению обнаружения и защиты
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям	Нарушение доступности, целостности, конфиденциальности	Достижение злоумышленником конечной цели по нарушению доступности узла или нарушении целостности данных

Из проведенного анализа тактик можно сделать вывод, что тактики сбора информации, получения первоначального доступа, закрепления и распространения, создают необходимые условия для реализации последующих тактик, которые будут направлены на реализацию таких целей, как нарушение целостности, доступности и конфиденциально-

сти. Матрица MITTRE ATT&CK, как и перечень ТТУ ФСТЭК описывает тактики и техники, применяемые злоумышленниками, но кроме того в ней еще представлены процедуры, которые описывают, конкретные инструменты для реализации угроз на разных платформах. Дополнительно в матрице приводится информация о преступных группировках (хакерские кампании) и ВПО, используемое ими, методы по отслеживанию реализации техник и снижения риска их реализации. Структура матрицы MITTRE приведена на рис. 2 [6].

Рис. 2. Структура матрицы MITTRE ATT&CK

В перечне ФСТЭК (Приложение 11 Методики оценки угроз безопасности информации) объединены некоторые тактические категории, представленные в матрице MITTRE ATT&CK. Так в перечне ФСТЭК три тактики из матрицы MITTRE, а именно подготовка ресурсов, сбор данных учетных данных и сбор информации о внутренней инфраструктуре, частично объединены с тактиками сбора информации (Т1), повышения привилегий (Т6) и распространения доступа (Т8). Тактика сбор и вывод информации (Т9) из перечня ФСТЭК в свою очередь включает в себя сразу две тактики ATT&CK – сбор данных и эксфильтрацию данных. Техники из перечня ТТУ ФСТЭК имеют некоторое пересечение с матрицей MITTRE. Так несколько аналогичных техник объединены в одну и сгруппированы по определенным тактикам, что упрощает анализ применяемых техник злоумышленниками при определенной тактике, но предоставляет меньшую детализацию возможных действий злоумышленника, и соответственно усложняет подбор смягчающих мер и способов обнаружения. Так одна техника описанная в ТТУ ФСТЭК может содержать в себе 10-15 аналогичных техник из матрицы MITTRE. При этом у ФСТЭК есть и свои уникальные техники (Т3.7 – Подмена файлов легитимных программ и библиотек непосредственно в системе), которые не встречаются в матрице MITTRE.

Рассмотрим, например технику Т4.1 ФСТЭК, которая описывает несанкционированное создание или кражу существующих учетных данных, и найдем ей аналогичные техники в матрице MITTRE. На рис. 3 приведены техники из матрицы MITTRE и тактики атак, при которых они могут быть применены. CAPEC – база описаний шаблонов последовательных атак, используемые злоумышленниками для негативного воздействия при использовании уязвимостей активов ОИ. Шаблоны классифицированы на 9 групп механизмов атак. В каждой группе механизма описаны соответствующие шаблоны атак.

Каждый шаблон имеет описание атаки, ближайшие атаки соответствующего механизма атак и объекты воздействия [7]. Объекты воздействия CAPEC частично соответствует модели объектов воздействия ФСТЭК. Анализ соответствия объектов воздействия приведен в табл. 2.

Для моделирования угроз безопасности необходимо сопоставление возможных негативных последствий угроз безопасности информации (УБИ), объектов воздействия угроз, общеизвестных уязвимостей, тактики и техники реализаций угроз, и шаблоны атак. Из проведенного анализа можно сделать вывод о целесообразности сочетания рассмотренных баз знаний о тактиках, техниках и шаблонов внешних воздействий злоумышленников. Основными исходными данными для общеизвестных уязвимостей и не-

достатков программного и аппаратного обеспечения выступают следующие источники: база данных угроз (БДУ) ФСТЭК, CWE и CVE [8-10]. Для оценки уязвимостей используется шкала CVSS [11], которая определяет их уровень критичности и числовую оценку – критический (9.0-10.0), высокий (7.0-8.9), средний (4.0-4.9), низкий (0.1-3.9).

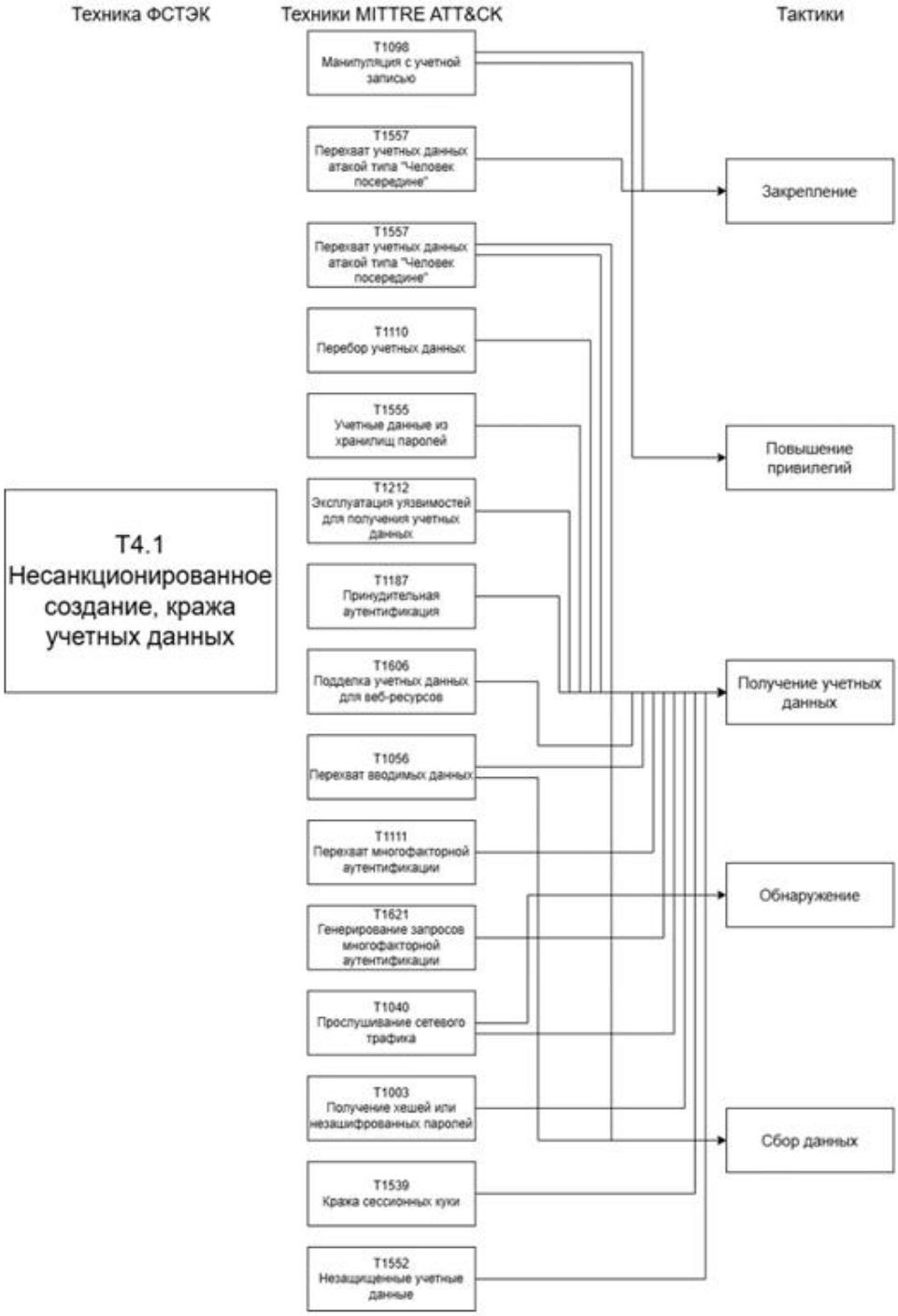


Рис. 3. Тактики и техники матрицы MITTRE

Таблица 2

Соответствия объектов воздействия ФСТЭК и CAPEC

Уровень воздействия ФСТЭК	Категория CAPEC	Примеры интерфейсов воздействия	Примечание
Аппаратный	Аппаратное обеспечение	USB порты, RJ-45	Полное соответствие. Охватывает физические устройства, микросхемы
Сетевой	Коммуникации	TCP/UDP порты	Полное соответствие. Фокус на сетевые протоколы и передачу данных
Системный	Программное обеспечение	Ядро ОС	Частичное соответствие. CAPEC включает системное ПО в общую категорию «Software»
Прикладной	Программное обеспечение	API	Частичное соответствие. CAPEC включает прикладное ПО в общую категорию «Software»
Пользовательский	Социальная инженерия	Электронная почта	Полное соответствие. Оба стандарта выделяют человеческий фактор как цель
-	Цепочка поставок	Библиотека обновления ПО	Описание объектов воздействия определяются с учетом состава и содержания услуг, предоставляемых поставщиком услуг
-	Физическая безопасность	Считыватели RFID	Нет соответствия в модели ФСТЭК

Учитывая вышеизложенное, можно сделать вывод, что для принятия обоснованного решения по организации защиты ОИ необходимо обработать и систематизировать значительный объём информации, охватывающей различные области знаний, на основе которой можно будет спроектировать эффективную систему защиты информации.

Для того, чтобы минимизировать вероятность принятия ошибочного решения, вызванного человеческим фактором, в условиях современного развития информационных технологий целесообразно при разработке системы защиты ОИ использовать системы поддержки принятия решений (СППР) [12]. При этом необходимо отметить, что некоторая часть информации, накопленной в базах знаний системы, имеет свойство неопределенности, что в целом характерно для задач, которые необходимо решать в условиях большого объема исходной информации, необходимой для принятия решения.

Условно источники неопределенности, возникающие при создании и эксплуатации СППР, можно разделить на следующие категории:

- недостаточная база знаний (данных) в предметной области;
- недостаточная информация о конкретной ситуации;
- неоднозначность в формулировании терминов (определений).

Рис. 4. Источники неопределенностей

Возникновение неопределенностей обусловлено, как объективными, так и субъективными факторами.

К объективным факторам можно отнести:

- несовершенство (пробелы) в действующем законодательстве;
- применение документов, носящих рекомендательный характер;
- неоднозначность (отсутствие единого подхода баз данных) в классификации применяемых действий злоумышленников;
- появление новых уязвимостей;
- существование уязвимостей нулевого дня и т.п.

К субъективным факторам можно отнести:

- отличающиеся мнения экспертов в области знаний;
- некорректное отображение информации при её передаче в цепочке знаний: эксперт-инженер программист;
- сложность систематизации инженером знаний большого объема исходной информации;
- сложность составления алгоритмов для написания программ из-за большого объема разнородной и противоречивой информации.

Учитывая рассмотренные факторы, для успешного решения задач в СППР, необходимо применять методы и алгоритмы, которые наиболее оптимально могут быть применены для использования возможностей современных систем обработки большого объема информации.

Проанализируем ряд методов, которые могут быть использованы для решения задач в СППР информационной безопасности.

В работах [13, 14] в рамках неопределенности и динамических изменений внешних воздействий на ОИ, рассматривается метод байесовской сети. Данная модель отражает функционирование вычислительной системы в условиях внешних воздействий и делит ее на 4 кластера, где формируются риски УБИ, ликвидация рисков угроз, формирование рисков и ликвидаций последствий инцидента (рис. 5). Модель представляет совместное распределение вероятностей, в котором каждое ребро является условной зависимостью, а каждый узел – отдельной случайной величиной, отражающей события информационной безопасности. Одним из ключевых преимуществ байесовских сетей является их способность к наглядному представлению причинно-следственных связей и выявлять вероятность наступления негативных последствий в рамках неопределнности. Несовершенство метода состоит в том,

что для построения вероятностной модели необходимо выбирать релевантные события ИБ и установления зависимостей между ними, что в рамках большой масштабируемости сети усложняет экспертную оценку распределения вероятностей.

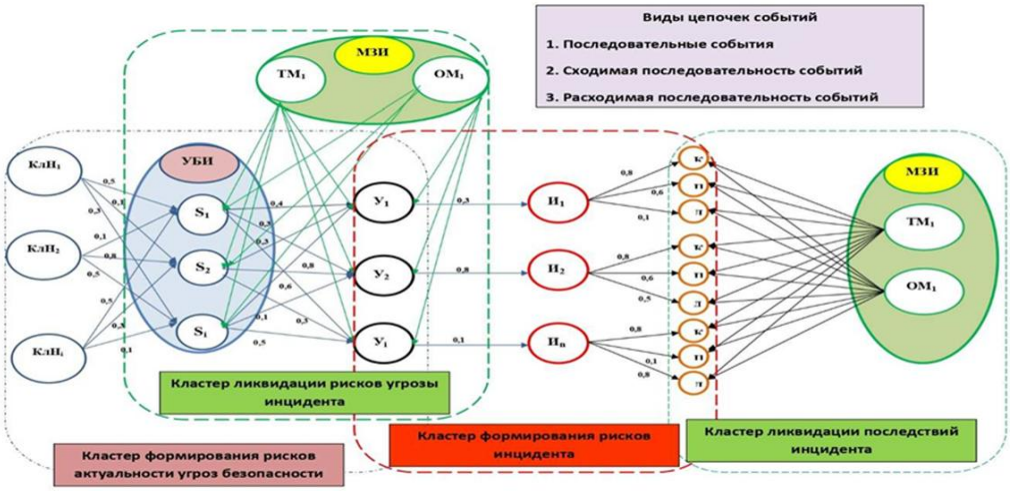


Рис. 5. Типовой модуль комплексной динамической модели функционирования защищенных информационных систем

В работе [15] рассматривается применение нечетких когнитивных карт и нейронных сетей. Нечеткая когнитивная карта является моделью ориентированного графа, где представляются концепты УБИ, объектов воздействия и применяемых средств защиты информации и связи между ними. Исходными данными являются экспертные оценки, формализованные и систематизированные шаблоны общедоступных баз знаний и практик. Коэффициент взаимосвязей между концептами определяется применением нечетких отношений, которые задаются на шкале от 0 до 1 [15–17]. Преимуществом использования нечетких когнитивных карт позволяет анализировать данные с их неопределенностью. Недостатком при использовании данного метода является, что оценка взаимосвязей между концептами УБИ проводят эксперты, что влечет за собой субъективность и при увеличении взаимосвязей концептов сложность такой оценки экспертами увеличивается.

Авторы приводят ряд критериев, на основе которых делают вывод, что нейронные сети являются эффективным инструментом по выявлению УБИ и уязвимостей. Достоинством нейронных сетей является то, что они обучаются на большем объеме данных и могут выявлять сложные паттерны, что обеспечивает высокую точность анализа, автоматизируют процесс анализа риска и адаптируются к изменениям актуальности УБИ. Соответственно эффективность нейронных сетей зависит от объема данных, на которых обучается сеть.

В работе [18–20] представлен метод онтологии, который позволяет сопоставить иерархически структурированного множества классов, описывающих предметную область и служащих основой для единой базы знаний, подчеркивает упорядоченный характер представления информации. В рамках исследования данная модель позволяет автоматизировать построение модели угроз, которая будет отражать связи негативных последствий УБИ, общеизвестных уязвимостей, сценарии реализации угроз, шаблоны атак. Систематизация знаний в виде классов и подклассов с определенными отношениями обеспечивает прозрачное понимание картины угроз, что позволяет выделить уязвимый интерфейс объекта воздействия, его критичность и корреляцию применяемых информационных технологий с уровнем компетенции злоумышленника, что соответственно способствует эффективной организации компенсирующих мер или применение средств защиты информации.

К негативным последствиям УБИ в следствии атаки на объекты воздействия {$ОБ_1$, $ОБ_2$,…, $ОБ_n$} может привести множество способов сценариев угроз {$ССУ_1$, $ССУ_2$,…, $ССУ_n$}, которые могут реализоваться множеством тактик {T_1, T_2,…, T_n} и техник {t_1, t_2,…, t_n}, а также множеством шаблонов {CAP_1, CAP_2,…, CAP_n}, в свою же очередь они реализуются через множество общеизвестных уязвимостей {{BDU_1, BDU_2,…, BDU_n}, {CWE_1, CWE_2,…, CWE_n}, {CVE_1, CVE_2,…, CVE_n}}. К тому же уязвимости могут иметь свойства критичности CVSS и множество платформ CPE {CPE_1, CPE_2,…, CPE_n}, под управлением которых функционирует программное обеспечение с обнаруженной уязвимостью. На рис. 6 приведен пример внешнего воздействия злоумышленника, где можно оценить актуальность уязвимостей посредством ее применимости к определенной платформе, критичность реализации уязвимости и отследить интерфейсы объектов воздействия.

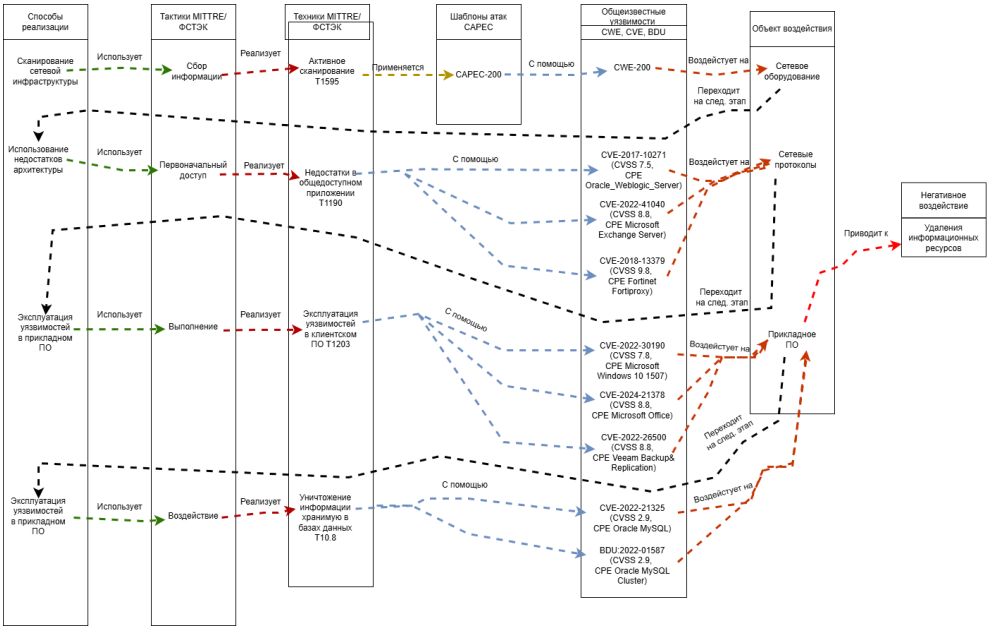


Рис. 6. Пример связей внешнего воздействия злоумышленника из различных баз знаний

Заключение. Применение эффективных методов и алгоритмов расчета защищенности активов ОИ от внешних воздействий позволяет противодействовать, как простым, так и комплексным компьютерным атакам.

В условиях постоянно усложняющихся угроз безопасности и расширения спектра потенциальных атак, обеспечение надежной защиты информационных активов остается первостепенной задачей. Рассмотренные в работе методы СППР, предназначенные для оценки угроз безопасности объектов информатизации, демонстрируют свои, как сильные стороны, так и недостатки в решении конкретных задач. На примере рассмотренных методов можно сделать вывод, что на различных стадиях проектирования КСЗИ на ОИ целесообразно применять именно те, которые наиболее точно и качественно отрабатывают поставленные задачи по подготовке варианта для принятия решения – построения модели угроз, модели нарушителя, технического задания и т.д.

Таким образом, при создании СППР выбор наиболее эффективных методов для решения задачи на определенных этапах проектирования КСЗИ на ОИ и разработка соответствующих алгоритмов, является актуальной научной технической задачей и требует дальнейшего исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02.07.2021 г. № 400.
2. Доктрина информационной безопасности Российской Федерации: Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.
3. *Ягнина О.А., Щербов И.Л., Якушина А.Е.* Принятие решения по организации защиты информации на объектах информатизации // Информатика и кибернетика. – 2022. – № 1 (27). – С. 31-35. – EDN VYNLED.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
5. Методический документ «Методика оценки угроз безопасности информации»: Утвержден ФСТЭК России 5 февраля 2021 г.
6. MITTRE ATT&CK общедоступная база знаний о тактиках и техника злоумышленников, основанная на реальных наблюдениях. – Режим доступа: https://attack.mitre.org/ (дата обращения: 15.04.2025).
7. CAPEC словарь известных схем атак, используемых противниками для использования известных недостатков в возможностях кибербезопасности. – Режим доступа: https://capec.mitre.org/ (дата обращения: 15.04.2025).
8. CWE список общедоступных уязвимостей программного-аппаратного обеспечения, разработанный сообществом. – Режим доступа: https://cwe.mitre.org/ (дата обращения: 16.04.2025).
9. CVE база данных общеизвестных уязвимостей. – Режим доступа: https://www.cve.org/ (дата обращения: 16.04.2025).
10. Банк данных угроз безопасности информации ФСТЭК. Содержит сведения об основных угрозах и уязвимостях. – Режим доступа: https://bdu.fstec.ru/threat (дата обращения: 16.04.2025).
11. CVSS общая система оценки уязвимостей. – Режим доступа: https://nvd.nist.gov/vuln-metrics/cvss (дата обращения: 16.04.2025).
12. *Щербов И.Л., Якушина А.Е*. Применение систем поддержки принятия решений при ликвидации ЧС // Пожарная и техносферная безопасность: проблемы и пути совершенствования. – 2019. – № 3 (4). – С. 234-239. – EDN TNHWWV.
13. *Баранов В.В.* Интегральная модель оценки защищенности объектов информатизации в условиях деструктивного воздействия // Вестник СибГУТИ. – 2022. – № 3 (59). – Режим доступа: https://cyberleninka.ru/article/n/integralnaya-model-otsenki-zaschischennosti-obektov-informatizatsii-v-usloviyah-destruktivnogo-vozdeystviya (дата обращения: 25.03.2025).
14. *Баранов В.В., Шелупанов А.А.* Методика и алгоритмы расчета защищенности элементов распределенных информационных систем в условиях деструктивного воздействия // Доклады ТУСУР. – 2022. – Т. 25, № 4. – С. 88-100. – DOI: 10.21293/1818-0442-2022-25-4-88-100.
15. *Паршенкова Ю.А., Максимова Е.А., Матвеев А.В*. Анализ рисков информационной безопасности на объектах критической информационной инфраструктуры с помощью нейронных сетей и нечетких когнитивных карт // Вестник Санкт-Петербургского университета ГПС МЧС России. – 2024. – №. 3. – С. 86-97. – Режим доступа: https://doi.org/10.61260/2218-130X-2024-3-86-97 (дата обращения: 25.03.2025).
16. *Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В*. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. – 2021. – № 3. – С. 110-133.
17. *Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д.* Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии. – 2018. – Т. 24, № 10. – С. 657-664. – DOI: 10.17587/it.24.657-664. – EDN YLHRUT.
18. *Абрамов Е.С., Геворгян Р.А.* Построение онтологической модели компьютерного преступления // Системный синтез и прикладная синергетика: Сб. научных работ XI Всероссийской научной конференции, п. Нижний Архыз, 27 сентября – 01 2022 года. – Ростов-на-Дону – Таганрог: ЮФУ, 2022. – С. 147-153. – DOI: 10.18522/syssyn-2022-29. – EDN MEWLTW.
19. *Brazhuk A.* Threat modeling of cloud systems with ontological security pattern catalog // International Journal of Open Information Technologies. – 2021. – Vol. 9, No. 5. – P. 36-41. – EDN JGZXIC.
20. *Глухов Н.И., Наседкин П.Н.* Аналитика внутренних угроз информационной безопасности предприятий // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2021. – Т. 24, № 1. – С. 33-41. – DOI: 10.21293/1818-0442-2021-24-1-33-41. – EDN VRETNT.

REFERENCES

1. O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii: ukaz Prezidenta Rossiyskoy Federatsii ot 02.07.2021 g. № 400 [On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation dated 07/02/2021 No. 400].
2. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii: Utverzhdena Ukazom Prezidenta Rossiyskoy Federatsii ot 5 dekabrya 2016 g. № 646 [Information Security Doctrine of the Russian Federation: Approved by Decree of the President of the Russian Federation No. 646 dated December 5, 2016].
3. *Yagnina O.A., Shcherbov I.L., Yakushina A.E.* Prinyatie resheniya po organizatsii zashchity informatsii na ob"ektakh informatizatsii [Decision-making on the organization of information protection at informatization facilities], *Informatika i kibernetika* [Informatics and Cybernetics], 2022, No. 1 (27), pp. 31-35. EDN VYNLED.
4. GOST R 51275-2006. Zashchita informatsii. Ob"ekt informatizatsii. Faktory, vozdeystvuyushchie na informatsiyu. Obshchie polozheniya [GOST R 51275-2006. Information protection. The object of informatization. Factors influencing information. General provisions].
5. Metodicheskiy dokument «Metodika otsenki ugroz bezopasnosti informatsii»: Utverzhden FSTEK Rossii 5 fevralya 2021 g. [Methodological document "Methodology for assessing information security threats": Approved by the FSTEC of Russia on February 5, 2021].
6. MITTRE ATT&CK obshchedostupnaya baza znaniy o taktikakh i tekhnika zloumyshlennikov, osnovannaya na real'nykh nablyudeniyakh [MITTRE ATT&CK a publicly available knowledge base on the tactics and techniques of intruders based on real observations]. Available at: https://attack.mitre.org/ (accessed 15 April 2025).
7. CAPEC slovar' izvestnykh skhem atak, ispol'zuemykh protivnikami dlya ispol'zovaniya izvestnykh nedostatkov v vozmozhnostyakh kiberbezopasnosti [CAPEC dictionary of known attack schemes used by opponents to exploit known flaws in cybersecurity capabilities]. Available at: https://capec.mitre.org/ (accessed 15 April 2025).
8. CWE spisok obshchedostupnykh uyazvimostey programmnogo-apparatnogo obespecheniya, razrabotannyy soobshchestvom [CWE list of publicly available software and hardware vulnerabilities developed by the community]. Available at: https://cwe.mitre.org/ (accessed 15 April 2025).
9. CVE baza dannykh obshcheizvestnykh uyazvimostey [CVE database of well-known vulnerabilities]. Available at: https://www.cve.org/ (accessed 15 April 2025).
10. Bank dannykh ugroz bezopasnosti informatsii FSTEK. Soderzhit svedeniya ob osnovnykh ugrozakh i uyazvimostyakh [The FSTEC Information Security Threat Database. Contains information about the main threats and vulnerabilities]. Available at: https://bdu.fstec.ru/threat (accessed 15 April 2025).
11. CVSS obshchaya sistema otsenki uyazvimostey [CVSS general vulnerability assessment system]. Available at: https://nvd.nist.gov/vuln-metrics/cvss (accessed 15 April 2025).
12. *Shcherbov I.L., Yakushina A.E.* Primenenie sistem podderzhki prinyatiya resheniy pri likvidatsii ChS [Application of decision support systems in emergency response], *Pozharnaya i tekhnosfernaya bezopasnost': problemy i puti sovershenstvovaniya* [Fire and technosphere safety: problems and ways of improvement], 2019, No. 3 (4), pp. 234-239. EDN TNHWWV.
13. *Baranov V.V.* Integral'naya model' otsenki zashchishchennosti ob"ektov informatizatsii v usloviyakh destruktivnogo vozdeystviya [An integral model for assessing the security of informatization facilities under conditions of destructive influence], *Vestnik SibGUTI* [Bulletin of SibGUTI], 2022, No. 3 (59). Available at: https://cyberleninka.ru/article/n/integralnaya-model-otsenki-zaschischennosti-obektov-informatizatsii-v-usloviyah-destruktivnogo-vozdeystviya (accessed 25 March 2025).
14. *Baranov V.V., Shelupanov A.A*. Metodika i algoritmy rascheta zashchishchennosti elementov raspredelennykh informatsionnykh sistem v usloviyakh destruktivnogo vozdeystviya [Methods and algorithms for calculating the security of elements of distributed information systems under conditions of destructive influence], *Doklady TUSUR* [Reports of TUSUR], 2022, Vol. 25, No. 4, pp. 88-100. DOI: 10.21293/1818-0442-2022-25-4-88-100.
15. *Parshenkova Yu.A., Maksimova E.A., Matveev A.V.* Analiz riskov informatsionnoy bezopasnosti na ob"ektakh kriticheskoy informatsionnoy infrastruktury s pomoshch'yu neyronnykh setey i nechetkikh kognitivnykh kart [Analysis of information security risks at critical information infrastructure facilities using neural networks and fuzzy cognitive maps], *Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii* [Bulletin of the Saint Petersburg University of the Ministry of Emergency Situations of Russia], 2024, No. 3, pp. 86-97. Available at: https://doi.org/10.61260/2218-130X-2024-3-86-97 (accessed 25 March 2025).
16. *Vasil'ev V.I., Vul'fin A.M., Kirillova A.D., Kuchkarova N.V.* Metodika otsenki aktual'nykh ugroz i uyazvimostey na osnove tekhnologiy kognitivnogo modelirovaniya i Text Mining [Methods for assessing current threats and vulnerabilities based on cognitive modeling and Text Mining technologies], *Sistemy upravleniya, svyazi i bezopasnosti* [Management, communication and security systems], 2021, No. 3, pp. 110-133.

17. *Vasil'ev V.I., Vul'fin A.M., Guzairov M.B., Kirillova A.D*. Interval'noe otsenivanie informatsionnykh riskov s pomoshch'yu nechetkikh serykh kognitivnykh kart [Interval assessment of information risks using fuzzy gray cognitive maps], *Informatsionnye tekhnologii* [Information Technologies], 2018, Vol. 24, No. 10, pp. 657-664. DOI: 10.17587/it.24.657-664. EDN YLHRUT.
18. *Abramov E.S., Gevorgyan R.A.* Postroenie ontologicheskoy modeli komp'yuternogo prestupleniya [Construction of an ontological model of computer crime], *Sistemnyy sintez i prikladnaya sinergetika: Sb. nauchnykh rabot XI Vserossiyskoy nauchnoy konferentsii, p. Nizhniy Arkhyz, 27 sentyabrya – 01 2022 goda* [System synthesis and applied synergetics: Collection of scientific papers of the XI All-Russian Scientific Conference, Nizhny Arkhyz settlement, September 27 – 01, 2022]. Rostov-on-Don – Taganrog: YuFU, 2022, pp. 147-153. DOI: 10.18522/syssyn-2022-29. EDN MEWLTW.
19. *Brazhuk A.* Threat modeling of cloud systems with ontological security pattern catalog, *International Journal of Open Information Technologies,* 2021, Vol. 9, No. 5, pp. 36-41. EDN JGZXIC.
20. *Glukhov N.I., Nasedkin P.N.* Analitika vnutrennikh ugroz informatsionnoy bezopasnosti predpriyatiy [Analytics of internal threats to information security of enterprises], *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radio Electronics], 2021, Vol. 24, No. 1, pp. 33-41. DOI: 10.21293/1818-0442-2021-24-1-33-41. EDN VRETNT.

Ерёмин Иван Александрович – Донецкий национальный технический университет; e-mail: Eremin-Ivan.TSI-20@yandex.ru; г. Донецк, Россия; тел.: +79498635241; магистрант.

Якушина Анна Евгеньевна – Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова; e-mail: yakuann@yandex.ru, г. Новочеркасск, Россия; тел.: +79494596928; магистрант.

Щербов Игорь Леонидович - Донецкий национальный технический университет; e-mail: scherbov@yandex.com; г. Донецк, Россия; тел.: +79493105787; к.т.н.; доцент.

Eremin Ivan Aleksandrovich – Donetsk National Technical University; e-mail: Eremin-Ivan.TSI-20@yandex.ru; Donetsk, Russia; phone: +79498635241; master’s student.

Yakushina Anna Evgenievna – Platov South Russian State Polytechnic University (NPI); e-mail: yakuann@yandex.ru; Novocherkassk, Russia; phone: +79494596928; master’s student.

Shcherbov Igor Leonidovich - Donetsk National Technical University; e-mail: scherbov@yandex.com; Donetsk, Russia; phone: +79493105787; cand. of eng. sc.; associate professor.

Раздел II. Методы защиты и технологии безопасности

УДК 004.056.5 DOI 10.18522/2311-3103-2025-3-55-62

М.А. Полтавцева, Д.В. Иванов

КЛАССИФИКАЦИЯ УЗЛОВ – ОБРАБОТЧИКОВ В СИСТЕМАХ БОЛЬШИХ ДАННЫХ В СООТВЕТСТВИИ С ПОДХОДОМ НУЛЕВОГО ДОВЕРИЯ

Кибербезопасность данных является одним из важнейших факторов успешной реализации национального проекта «Экономика данных и цифровая трансформация государства». Проблемы построения защищенных систем обработки больших данных заключаются в их гетерогенной природе, большом числе разнородных инструментов, высокой связности и высоком доверии между распределенными компонентами. Снижение внутреннего доверия и уменьшение поверхности атаки в соответствии с подходом zero-trust необходимо для повышения защищенности таких систем с наименьшим влиянием на их производительность. Целью работы является создание метода динамической классификации узлов и компонент обработки данных в гетерогенных системах больших данных на основе применения различных подходов к снижению доверия в отношении объектов, реализующих процесс обработки информации. Рассматривается подход нулевого доверия применительно к исследуемому классу систем, а также ставится задача расширенной реализации принципа минимальных привилегий уменьшения поверхности атаки. Представлена классификация узлов – обработчиков на основе выполняемых ими операций с данными, унифицированных согласно разработанной ранее концептуальной модели данных. Предлагается сопоставление узлов и применяемых в их отношении методов безопасности на основе необходимости доступа к семантике и компонентам данных для выполнения операций. На основе данной классификации разработан метод динамического определения класса узлов-обработчиков данных в процессе работы системы для ситуаций изменения компонентного состава системы обработки больших данных, типичной для многокомпонентных распределенных высоконагруженных систем. Результаты работы являются частью комплексного консистентного подхода к построению защищенных систем обработки больших данных.

Большие данные; системы обработки данных; гетерогенные системы больших данных; информационная безопасность; нулевое доверие; операции с данными; управление инфраструктурой.

M.A. Poltavtseva, D.V. Ivanov

CLASSIFICATION OF PROCESSING NODES IN BIG DATA SYSTEMS ACCORDING TO THE ZERO TRUST APPROACH

Data cybersecurity is one of the most important factors for the successful implementation of the national project 'Data Economy and Digital Transformation of the State'. The challenges of building secure big data systems lie in their heterogeneous nature, large number of heterogeneous tools, high connectivity and high trust between distributed components. Reducing the internal trust and reducing the attack surface according to the zero-trust approach is necessary to increase the security of such systems with the least impact on their performance. The aim of the paper is to create a method for dynamic classification of nodes and data processing components in heterogeneous big data systems based on the application of different approaches to trust reduction with respect to the objects realising the information processing process. The paper considers the zero trust approach as applied to the class of systems under study, as well as the task of extended implementation of the principle of minimum privilege to reduce the attack surface. The authors present a classification of nodes - handlers based on their operations with data, unified according to the previously developed conceptual data model. A comparison of nodes and security methods applied to them based on the need for access to semantics and data components to perform operations is proposed. Based on this classification, a method of dynamic node type determination during sys-

tem operation is developed for situations of changing component composition of a big data processing system, typical for multi-component distributed highly loaded systems. The results of the work are a part of the complex consistency approach to the construction of secure big data processing systems.

Big Data; data processing systems; heterogeneous big data systems; information security; zero-trust; data operations; infrastructure management.

Введение. На сегодняшний день можно говорить о синергии дух трендов: развития и повсеместной цифровизации с одной стороны и увеличения числа атак на информационные системы различной природы с другой. Появление и развитие систем больших данных во многом усугубило проблемы безопасности, так как для них свойственна концентрация большого числа разнородной конфиденциальной информации в одном месте. Также стоит отметить снижение безопасности, вызванное особенностями распределенной организации таких систем.

Ключевую сложность при обеспечении защиты систем обработки и хранения больших данных представляет собой их гетерогенная природа: сочетание различных инструментов и способов обработки информации в одном жизненном цикле. В силу большого числа самостоятельных компонентов, как правило – доверенных в отношении друг друга, для этого класса решений характерен рост вероятности реализации угроз, в том числе - угроз конфиденциальности данных, со стороны внутреннего привилегированного нарушителя. Поэтому построение безопасности этого класса систем на базе подхода нулевого доверия (zero-trust) является важной задачей. Целью данной работы является формирование динамического метода классификации узлов систем обработки и хранения больших данных на основе выполняемых ими информационных операций с целью определения требований к архитектуре безопасности и методу защиты.

Применение подхода минимального доверия к узлам – обработчикам данных в системах больших данных. Понятие «доверия» в информационной безопасности до конца не определено и имеет разное значение в зависимости от контекста [1]. С одной стороны, под доверием понимают уверенность в действиях и/или корректности с некоторой стороны (участника) [2], с другой – общепризнанным с 2010-х годов подходом zero-trust или нулевого доверия [3]. В любом случае необходимо отметить, что понятие доверия тесно связано с рисками информационной безопасности и может быть соотнесено с компонентами информационных систем [4], а следовательно – и систем управления большими данными. Так доверие в системах больших данных также имеет два значения: доверие пользователя (отправителя или получателя данных) к системе обработки и хранения больших данных, как уверенность в характеристиках данных при работе с системой: полноте, целостности, конфиденциальности и доступности данных; доверие компонентов системы управления больших данных друг к другу как между уровней представления, так и внутри этих уровней [5]. С этой точки зрения под степенью доверия в системах управления больших данных в соответствии подходом нулевого доверия (zero trust) будем понимать степень безусловной уверенности в характеристиках безопасности участников обработки данных и самой информации.

Реализация принципа минимальных привилегий [6], как и уменьшение поверхности атаки, приводит к уменьшению уязвимости систем обработки и хранения больших данных [7] и, таким образом, снижению рисков информационной безопасности и реализации подхода нулевого доверия [8]. Формирование и реализация оптимальной политики безопасности в системах обработки и хранения больших данных происходит в условиях не только ограничений бизнес-логики, определяющей не снижаемые риски в рамках конкретной технологии, но и в условиях технологических ограничений [9]. Поэтому корректно говорить скорее о стремлении к нулевому доверию (в идеологическом смысле), чем о его реализации. Особенностью данных систем является наличие группы привилегированных пользователей – администраторов, имеющих высокий уровень доступа к данным (в том числе, в силу несовершенства механизмов разграничения доступа) [10]. В таких условиях необходимо стремиться к уменьшению доступа привилегированных пользователей, выведя их за границы безусловного доверия в отношении обрабатываемых данных.

Несмотря на то, что приведенная выше концепция нулевого доверия, широко принята в информационной безопасности, а снижение доверия к среде в различных областях остается де-факто стандартом безопасности [11, 12], сегодня в силу сложности практической реализации она подвергается критике и нуждается в адаптации применительно к каждому конкретному классу систем [13]. В свою очередь минимизация доверия в отношении компонентов обработки информации является сложной задачей для систем больших данных, которым характерно несколько распределенных сред и инструментов, интегрированных в рамках управления общим циклом обработки и хранения данных.

Можно выделить три подхода для снижения требуемого уровня доверия компонентам обработки данных [14]: использование защитного контура или защита периметра [15, 16], сквозное шифрование уровня приложения [17, 18], обфускация (маскирование) данных [19]. На их основе в системе больших данных формируется гибридная архитектура безопасности. Следующим шагом становится классификация узлов обработчиков для распределения по архитектурным компонентам: обрабатывающим открытые данные, маскированные данные, зашифрованные данные.

Классификация узлов-обработчиков данных. Для решения поставленной задачи необходимо разделить узлы – обработчики данных для того, чтобы определить технологическую необходимость в доступе к семантике данных при выполнении операций. Рассмотрим необходимость доступа к семантике для всех типов операций, определенных в общей концептуальной модели данных для гетерогенных систем больших данных [20].

Создание Create:({d},Key)→di={Key,Value} само по себе подразумевает доступ к значению Value создаваемого агрегата, а значит – доступ к семантике.

Уничтожение Delete:(di)→∅ не предполагает доступа к семантике уничтожаемого агрегата.

Включение Incl:(di,{d})→di’ в общем случае не требует доступа к семантике включаемых фрагментов, однако подразумевает доступ к значению Value получаемого фрагмента, или, по крайней мере, его составляющим.

Исключение Extr:(di’,{Keyj})→(di, dj). Операция исключения в ряде случаев может быть выполнена без доступа к семантике, однако в большинстве случаев такой доступ потребуется. Проблема заключается в том, что при исключении нужно выделить новый агрегат из существующего, а значит получить доступ к содержимому (путь и составному) его значения (Value). Поэтому к этой операции относится, например, поиск. На более низком уровне детализации операция исключения может быть реализована с использованием сравнения (как например поиск) что также следует учитывать. В целом отнесем операцию исключения к требующим доступа к семантике.

Преобразование Transform:(di)→dj операция явно предполагающая доступ к семантике данных (например, со стороны пользователя или приложения, расчет показателей на основе данных).

Итоговая систематизация узлов – обработчиков данных в виде нечеткой классификации на основе технологического уровня и доступа к семантике для реализации принципа минимизации доверия представлена на рис. 1.

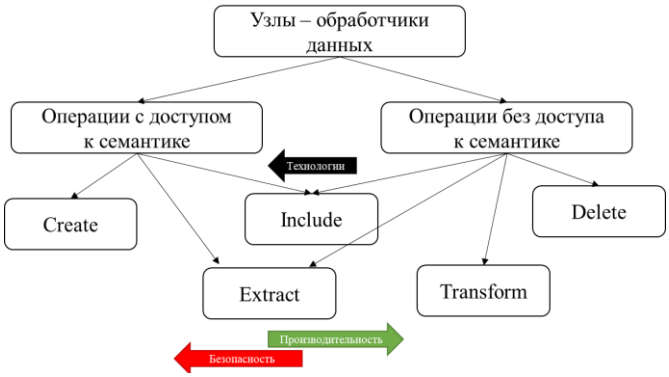


Рис. 1. Классификация узлов-обработчиков данных

Возможность выполнения операций включения и исключения без доступа к семантике зависит от двух факторов: особенностей выполнения операции на нижележащем уровне, уровне инструментов обработки и хранения данных и технологических возможностей, или наличия эффективного выполнения данной операции над зашифрованными данными без использования специфических алгоритмов (либо же интеграцией таких алгоритмов в узлы – обработчики данных).

Несмотря на то, что при использовании гомофонного шифрования достаточно сложные операции с данными могут производиться без доступа к семантике, их производительность остается низкой и их эффективное применение на сегодняшний день не может рассматриваться в широком круге систем обработки и хранения больших данных.

Классификация узлов – обработчиков данных на основе принципа минимизации доверия основывается в первую очередь на доступе к семантике данных, однако есть еще такой аспект, как динамичность систем обработки и хранения больших данных. Можно выделить по крайней мере два аспекта такой динамики:

1. Изменение маршрутов данных, и, как следствие, изменение операций, выполняемых на узле – обработчике (а значит, и его класса в соответствии с приведенной классификацией).

2. Изменение состава узлов – обработчиков из-за отказов и замены двух типов: отказа/замены/добавления узлов кластера в рамках используемого инструмента обработки и/или хранения данных, отказа/замены/добавления инструментов обработки и/или хранения данных.

Новые узлы или инструменты при подключении к системе должны быть автоматически отнесены к одной из приведенных выше категорий (классов). Следовательно, возникает требование их динамической классификации «на лету» на основе текущих данных, состояния системы и процессов обработки информации. Таким образом, требованиями к методу динамической классификации узлов-обработчиков данных на основе принципа минимизации доверия являются:

1. Учет конкретных операций, выполняемых согласно процессу, на классифицируемом узле обработки данных;

2. Учет технологических возможностей по защите данных на узле – обработчике на основе рассмотренных подходов: переносом в защищенный контур, маскированием или шифрованием;

3. Приоритезация рассмотренных подходов с точки зрения производительности и безопасности.

При этом маскирование (обфускация данных) и шифрование – это операции, зависимые, в свою очередь, от операций, которые выполняются над данными каждым отдельным узлом – обработчиком.

Для проведения такой классификации следует определить статус узлов – обработчиков $Node = \{n_1, \dots, n_N\}$ относительно архитектурных компонентов: множества маскированных узлов ($Node_m$), множества узлов применяющих сквозное шифрование ($Node_{en}$) и множества узлов функционирующих в защищенном контуре и проводящих обработку открытых данных ($Node_{op}$).

Сама по себе задача выбора оптимального метода маскирования является зависимой не только от операций над данными, но и от характеристик самих данных [21] и не может быть универсализирована. Однако практика применения маскирования позволяет выделить круг задач, в которых использование этого подхода можно унифицировать. Примером таких ситуаций служит обработка типовых корпоративных данных [22]. В этом случае конфиденциальные данные заменяются на идентификатор, сохраняющий их основные свойства: уникальность, статистическое распределение и др. В значимом числе случаев для решения задач и выполнения операций над данными достаточно знать характеристики данных, а не их значения. То есть, эти операции априори выполняются без доступа к семантике. При этом для получения маскированных значений $md_{i,j}$ на основе открытых исходных данных $d_{i,j}$на практике используются различные подходы:

Преобразование по определенному обратимому алгоритму:

$$\left(md_{i,j} = Fm_k\left(d_{i,j}\right) | (Fm_k \in Ms)\right) \vee \left(\exists (Fm_k^{-1}) | \left(d_{i,j} = Fm_k^{-1}\left(d_{i,j}\right)\right)\right). \quad (1)$$

Обратимое преобразование с использованием ключа:

$$\left(md_{i,j} = Fm_k\left(d_{i,j}, Key\right) | (Fm_k \in Ms)\right) \vee \left(\exists (Fm_k^{rev}) | \left(d_{i,j} = Fm_k^{rev}\left(d_{i,j}, Key\right)\right)\right). \quad (2)$$

Преобразование на основе таблицы подстановки:

$$\left(md_{i,j} = Fm_k\left(d_{i,j}, Tb\right) | (Fm_k \in Ms)\right) \vee \left(\exists (Fm_k^{rev}) | \left(d_{i,j} = Fm_k^{rev}\left(d_{i,j}, Tb\right)\right)\right). \quad (3)$$

Причем второй случай (2) описывает, фактически, маскирование с использованием методов шифрования, а в третьем случае (3) может использоваться простая функция сопоставления по порядку маскируемого значения с маскирующим. Отметим, что первый случай, представленный (1), является наименее приемлемым, т.к. требует сокрытия алгоритма маскирования, а не ключа. Выбор между вторым и третьим случаем должен производиться в условиях текущей стоимости и доступности ресурсов: объемов памяти и вычислительной мощности.

Если $d_{i,j} \in D$ – определенный тип фрагментов данных, обрабатываемый узлом $n_j \in Node$, то возможность его обработки в том или ином виде определяется производимыми с ним операциями. Определим подмножество операций с данными, не требующих доступа к семантике, в первую очередь с учетом маскирования, Op^{S-} как включение ($Incl$), исключение ($Extr$) и удаление ($Delete$). Остальные операции: создание ($Create$), трансформация ($Transform$) отнесем к подмножеству Op^{S+}, или требующих доступа к семантике.

При этом множество Op^{S+} также может быть разбито и часть операций из него перенесена в Op^{S-}, точнее подмножество Op^{S-E}, если это операции, которые могут быть эффективно выполнены над шифр текстом в условиях используемого метода шифрования. Методы шифрования, доступные для использования в конкретной системе $En = \{en_1, \dots, en_E\}$ характеризуются двумя множествами $en_e = \langle Op_e, To_e \rangle$ где Op_e – операции, которые могут быть выполнены над шифр текстом, а To_e – временные показатели (сложность) этих операций. Каждому фрагменту данных $d_i \in D$ может быть сопоставлена пара значений $\langle op_e, to_e \rangle$ или показано отсутствие поддержки операции над указанным типом данных в конкретном метод. То есть $\left((d_i \leftrightarrow \langle op_e, to_e \rangle) \vee \left(\nexists (d_i \leftrightarrow op_e)\right)\right) \forall (en_e \in En)$. Тогда при некотором заданном граничном значении временных затрат T_{lim} должно соблюдаться ограничение $T < T_{lim}$ где $T = F\left(D_j, Op_j, En_j\right)$, а D_j, Op_j, En_j – соответственно фрагменты данных, выполняемые операции и методы шифрования поддерживаемые узлом $n_j \in Node$, а D_j, Op_j фактически представляют собой отображения $d_{i,j} \leftrightarrow Op_{i,j}$ соотносящие типы фрагментов данных и операции над ними. Однако такая детализация является достаточно сложно реализуемой на практике и на данном этапе ограничимся условно универсальным разделением Op^{S-} и Op^{S+} на основе базовых операций модели данных, как приведено выше.

В итоге разделение узлов – обработчиков данных на три типа: обрабатывающих маскированные данные, зашифрованные данные или открытые данные в защищенном контуре может быть описано следующим образом:

1. Сформировать множества Op^{S-} и Op^{S+}.
2. Определить перечень операций Op, совершаемых с каждым типом фрагмента данных на узле – обработчике ($D \rightarrow \{Op_{d_i} = \{op_1 \dots op_n\}\}$).

- Если $\left(\forall \left(op_j \in Op_{d_i}\right)\right)\left(op_j \in Op^{S-}\right)$ или $Op_{d_i} \subseteq Op^{S-}$ узел вносится в список подлежащих сокрытию путем маскирования L^{Ms}.

- Если $\left(\exists\left(op_j \in Op_{d_i}\right)\right)\left(op_j \in Op^{S+}\right)$ узел вносится в список подлежащих обработке в открытом виде L^{Op}.

3. Для каждого узла $node \in L^{Ms}$
   - Если узел не соответствует критериям маскирования: ограниченный диапазон чувствительных значений, перенести в список подлежащих шифрованию L^{En}.

4. При подключении нового узла в системе или изменении графа обработки данных выполнить п.2 и 3.

Таким образом реализуется динамическая классификация узлов – обработчиков данных в процессе работы системы на три класса с точки зрения места в архитектуре безопасной обработки информации с минимизацией доверия. Более детально метод можно представить в виде основного подпроцесса классификации и подпроцесса – динамического планировщика, реализующего динамический аспект классификации на основании событий в системе.

Заключение. Сегодня с практической точки зрения при имплементации предложенного метода можно говорить скорее не об отдельных независимых узлах обработчиков данных, а об отдельных инструментах хранения и обработки информации, интегрированных в общую среду. Каждый из этих инструментов, в свою очередь, реализует замкнутый комплекс операций с данными в, как правило, распределенной среде и не имеет внутреннего механизма разделения узлов обработчиков конфиденциальных и открытых данных, либо же данных с разным уровнем конфиденциальности. Поэтому предложенная классификация в первую очередь должна применяться не к отдельным узлам, а к инструментам обработки в гетерогенной среде больших данных, сохраняя в этих условиях свою актуальность.

В заключении стоит отметить, что разработка принципов построения и архитектур безопасности в отношении гетерогенных систем больших данных сегодня высоко востребована на практике для новых цифровых систем. Интеграция подходов безопасности в отношении архитектур обработки данных, создание гибридных архитектур, в совокупности с автоматизацией отнесения узлов (и более крупных компонент) к определенному архитектурному блоку, автоматической авторизации на этой основе и применением методов защиты – ключевой аспект построения защищенных систем обработки и управления большими данными.

Исследование выполнено за счет гранта Российского научного фонда № 23-11-20003, https://rscf.ru/project/23-11-20003/, грант Санкт-Петербургского научного фонда (Соглашение №23-11-20003 о предоставлении регионального гранта).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Dumitru I.A.* Zero trust security // Proceedings of the International Conference on Cybersecurity and Cybercrime-2022. – Asociatia Romana pentru Asigurarea Securitatii Informatiei, 2022. – P. 99-104.
2. *Правиков Д.И., Щербаков А.Ю.* К вопросу об изменении парадигмы информационной безопасности // Системы высокой доступности. – 2018. – Т. 14, № 2. – С. 35-39.
3. *Малинский С.В.* Концепция безопасности Zero Trust: принципы и практика внедрения // Интеллектуальные транспортные системы. – 2022. – С. 430-437.
4. *Грызунов В.В. и др.* Обеспечение информационной безопасности интегрируемых информационных систем на базе доверия // Тр. учебных заведений связи. – 2024. – Т. 10, № 4. – С. 110-125.
5. *Полтавцева М. А., Зегжда Д.П., Калинин М.О.* Многоуровневая концепция безопасности систем управления большими данными // Вопросы кибербезопасности. – 2023. – № 5. – С. 25-36.
6. *Mishra K.N. et al.* Cloud and big data security system's review principles: A decisive investigation // Wireless Personal Communications. – 2022. – Vol. 126, No. 2. – P. 1013-1050.
7. *Awaysheh F.M. et al.* Security by design for big data frameworks over cloud computing // IEEE Transactions on Engineering Management. – 2021. – Vol. 69, No. 6. – P. 3676-3693.
8. *Stafford V.* Zero trust architecture // NIST special publication. – 2020. – Vol. 800. – 207 p.
9. *Attaallah A. et al.* Analyzing the Big Data Security Through a Unified Decision-Making Approach // Intelligent Automation & Soft Computing. – 2022. – Vol. 32, No. 2.

10. *Alani M.M.* Big data in cybersecurity: a survey of applications and future trends // Journal of Reliable Intelligent Environments. – 2021. – Vol. 7, No. 2. – P. 85-114.
11. *Wang Z., Yu X., Xue P., Qu Y., Ju L.* Research on Medical Security System Based on Zero Trust // Sensors. – 2023. – Vol. 23. – 3774. – 16 c. – DOI: 10.3390/s23073774.
12. *Daah C., Qureshi A., Awan I., Konur S.* Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework // Electronics. – 2024. – Vol. 13. – 865. – 49 p. – DOI: 10.3390/electronics13050865.
13. *Fernandez E.B., Brazhuk A.* A critical analysis of Zero Trust Architecture (ZTA) // Computer Standards & Interfaces. – 2024. – Vol. 89. – 103832. – 12 p. – DOI: 10.1016/j.csi.2024.103832.
14. *Poltavtseva M.A., Platonov V.V., Semyanov P.V.* Secure data processing architectures in big data systems. December 16-17, 2024. – 2024. – P. 104-108.
15. *Zhao Y. et al.* A zone-based data lake architecture for IoT, small and big data // Proceedings of the 25th International Database Engineering & Applications Symposium. – 2021. – P. 94-102.
16. *Awaysheh F.M. et al.* Security by design for big data frameworks over cloud computing // IEEE Transactions on Engineering Management. – 2021. – Vol. 69, No. 6. – P. 3676-3693.
17. *Roy P., Kumar R.* Multilevel Security Framework based on An Onion Encryption in Public Cloud Network // 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). – IEEE, 2021. – P. 1442-1446.
18. *Kuhn C. et al.* Onion routing with replies // Advances in Cryp-tology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27. – Springer International Publishing, 2021. – P. 573-604.
19. *Thirumalaisamy M. et al.* Interaction of secure cloud network and crowd computing for smart city data obfuscation // Sensors. – 2022. – Vol. 22, No. 19. – Art. 7169.
20. *Полтавцева, М.А., Калинин М.О., Зегжда Д.П.* Моделирование данных в задачах информационной безопасности поли-хранилищ // Проблемы информационной безопасности. Компьютерные системы. – 2023. – № 4 (57). – С. 122-132. – DOI: 10.48612/jisp/x468-hp82-adav.
21. *Duncan G. and Stokes L.* Data masking for disclosure limitation. // WIREs Comp Stat. – 2009. – Vol. 1. – P. 83-92. – DOI: 10.1002/wics.3.
22. *Jain R.B., Puri M.* An approach towards the development of scalable data masking for preserving privacy of sensitive business data // Artificial Intelligence and Evolutionary Computations in Engineering Systems. – Springer Singapore, 2020. – Vol. 1056. – P. 733-743. – DOI: 10.1007/978-981-15-0199-9.

REFERENCES

1. *Dumitru I.A.* Zero trust security, *Proceedings of the International Conference on Cybersecurity and Cybercrime-2022*. Asociatia Romana pentru Asigurarea Securitatii Informatiei, 2022, pp. 99-104.
2. *Pravikov D.I., Shcherbakov A.Yu.* K voprosu ob izmenenii paradigmy informatsionnoy bezopasnosti [On the issue of changing the paradigm of information security], *Sistemy vysokoy dostupnosti* [High Availability Systems], 2018, Vol. 14, No. 2, pp. 35-39.
3. *Malinskiy S.V.* Kontseptsiya bezopasnosti Zero Trust: printsipy i praktika vnedreniya [Zero Trust security concept: principles and implementation practices], *Intellektual'nye transportnye sistemy* [Intelligent Transport Systems], 2022, pp. 430-437.
4. *Gryzunov V.V. i dr.* Obespechenie informatsionnoy bezopasnosti integriruemykh informatsi-onnykh sistem na baze doveriya [Ensuring *information security of integrated information systems based on trust], Tr*. uchebnykh zavedeniy svyazi [Proceedings of educational institutions of communication], 2024, Vol. 10, No. 4, pp. 110-125.
5. *Poltavtseva M. A., Zegzhda D.P., Kalinin M.O.* Mnogourovnevaya kontseptsiya bezopasnosti sistem upravleniya bol'shimi dannymi [Multi-level concept of security of big data management systems], *Voprosy kiberbezopasnosti* [Issues of Cybersecurity], 2023, No. 5, pp. 25-36.
6. *Mishra K.N. et al.* Cloud and big data security system's review principles: A decisive investigation, *Wireless Personal Communications,* 2022, Vol. 126, No. 2, pp. 1013-1050.
7. *Awaysheh F.M. et al.* Security by design for big data frameworks over cloud computing, *IEEE Transactions on Engineering Management,* 2021, Vol. 69, No. 6, pp. 3676-3693.
8. *Stafford V.* Zero trust architecture, *NIST special publication,* 2020, Vol. 800, 207 p.
9. *Attaallah A. et al.* Analyzing the Big Data Security Through a Unified Decision-Making Approach, *Intelligent Automation & Soft Computing,* 2022, Vol. 32, No. 2.
10. *Alani M.M.* Big data in cybersecurity: a survey of applications and future trends, *Journal of Reliable Intelligent Environments,* 2021, Vol. 7, No. 2, pp. 85-114.
11. *Wang Z., Yu X., Xue P., Qu Y., Ju L.* Research on Medical Security System Based on Zero Trust, *Sensors,* 2023, Vol. 23, 3774, 16 p. DOI: 10.3390/s23073774.

12. *Daah C., Qureshi A., Awan I., Konur S.* Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework, *Electronics,* 2024, Vol. 13, 865, 49 p. DOI: 10.3390/electronics13050865.
13. *Fernandez E.B., Brazhuk A.* A critical analysis of Zero Trust Architecture (ZTA), *Computer Standards & Interfaces,* 2024, Vol. 89, 103832, 12 p. DOI: 10.1016/j.csi.2024.103832.
14. *Poltavtseva M.A., Platonov V.V., Semyanov P.V.* Secure data processing architectures in big data systems. December 16-17, 2024, 2024, pp. 104-108.
15. *Zhao Y. et al.* A zone-based data lake architecture for IoT, small and big data, *Proceedings of the 25th International Database Engineering & Applications Symposium,* 2021, pp. 94-102.
16. *Awaysheh F.M. et al.* Security by design for big data frameworks over cloud computing, *IEEE Transactions on Engineering Management,* 2021, Vol. 69, No. 6, pp. 3676-3693.
17. *Roy P., Kumar R.* Multilevel Security Framework based on An Onion Encryption in Public Cloud Network, *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N).* IEEE, 2021, pp. 1442-1446.
18. *Kuhn C. et al.* Onion routing with replies, *Advances in Cryp-tology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part II 27*. Springer International Pub-lishing, 2021, pp. 573-604.
19. *Thirumalaisamy M. et al.* Interaction of secure cloud network and crowd computing for smart city data obfuscation, *Sensors,* 2022, Vol. 22, No. 19, Art. 7169.
20. *Poltavtseva, M.A., Kalinin M.O., Zegzhda D.P.* Modelirovanie dannykh v zadachakh informatsionnoy bezopasnosti polikhranilishch [Data modeling in problems of information security of polystorage facilities], *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Problems of Information Security. Computer Systems], 2023, No. 4 (57), pp. 122-132. DOI: 10.48612/jisp/x468-hp82-adav.
21. *Duncan G. and Stokes L.* Data masking for disclosure limitation, *WIREs Comp Stat*., 2009, Vol. 1, pp. 83-92. DOI: 10.1002/wics.3.
22. *Jain R.B., Puri M.* An approach towards the development of scalable data masking for preserving privacy of sensitive business data, *Artificial Intelligence and Evolutionary Computations in Engineering Systems*. Springer Singapore, 2020, Vol. 1056, pp. 733-743. DOI: 10.1007/978-981-15-0199-9.

Полтавцева Мария Анатольевна – Санкт-Петербургский политехнический университет Петра Великого; e-mail: poltavtseva@ibks.spbstu.ru; г. Санкт-Петербург, Россия; тел.: +78125527632; д.т.н.; доцент; профессор института кибербезопасности и защиты информации; ORCID 0000-0001-9659-1244.

Иванов Денис Вадимович – Санкт-Петербургский политехнический университет Петра Великого; e-mail: vanov@ibks.spbstu.ru; г. Санкт-Петербург, Россия; тел.: +78125527632; к.т.н.; доцент института кибербезопасности и защиты информации; ORCID 0009-0008-7331-9721.

Poltavtseva Maria Anatolyevna – Peter the Great St. Petersburg Polytechnic University; e-mail: poltavtseva@ibks.spbstu.ru; Saint Petersburg; Russia; phone: +78125527632; dr. of eng. sc.; associate professor; professor at the Institute of Cyber Security and Information Protection; ORCID 0000-0001-9659-1244.

Ivanov Denis Vadimovich – Peter the Great St. Petersburg Polytechnic University; e-mail: vanov@ibks.spbstu.ru; Saint Petersburg; Russia; phone: +78125527632; cand. of eng. sc.; associate professor at the Institute of Cyber Security and Information Protection; ORCID 0009-0008-7331-9721.

УДК 004.7 DOI 10.18522/2311-3103-2025-3-62-81

А.М. Маевский, В.А. Рыжов, Т.А. Федорова, И.В. Кожемякин, Н.М. Буров

СТОХАСТИЧЕСКАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ ПОДВОДНОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ, ОСНОВАННАЯ НА ЛУВЕНСКОМ АЛГОРИТМЕ КЛАСТЕРИЗАЦИИ

Подводные беспроводные сенсорные сети (ПБСС) играют важную роль в мониторинге океанических процессов, подводной навигации, экологическом контроле и обеспечении безопасности. Однако особенности подводной среды, такие как высокая затухаемость сигналов, ограниченные ресурсы энергии и изменяющаяся топология сети, создают значительные сложности в организации эффективной передачи данных. Для оптимизации работы сети и продления ее срока службы используется метод кластеризации, позволяющий группировать узлы, снижать нагрузку

на коммуникационные каналы и повышать энергоэффективность. Однако в условиях выхода из строя узлов сети статическая кластеризация становится неэффективной, что требует внедрения динамической рекластеризации. Процедура перераспределения ролей узлов и перестройки топологии сети позволяет сохранять устойчивость связи и минимизировать потери данных, учитывая энергетически баланс всей сети в целом. В данной работе исследуются современные подходы к кластеризации и рекластеризации в ПБСС с учетом энергетического баланса, вероятности отказов узлов и помех в среде передачи. Развитие адаптивных методов управления ПБСС является актуальной задачей, направленной на повышение надежности, энергоэффективности и долговечности подводных сетей связи. В статье представлена стохастическая кроссуровневая модель для динамических трехмерных ПБСС произвольной топологии. Модель использует: новую технику кластеризации/рекластеризации базирующуюся на лувенском алгоритме, протокол маршрутизации, построенный на методе Дейкстра и метод управления доступом к среде на основе расписания передач (TDMA). Предложенная модель функционирования ПБСС положена в основу разработанного имитационного комплекса, позволяющего проводить оценку эффективности и надежности сети с учетом нарушения связности и уязвимостей для ПБСС различного масштаба и назначения. В рамках исследований выполнен параметрический анализ систематических расчетов функциональных характеристик ПБСС. Результаты анализа показали, что предложенная имитационная модель обеспечивает увеличение времени автономной работы сети и снижение числа потерянных сообщений по сравнению с моделями других авторов.

Подводные беспроводные сенсорные сети; стохастическая динамическая модель сети; имитационное моделирование; кластеризация; лувенский алгоритм; метод Дейкстра; метод управления доступом к среде на основе расписания передач.

A.M. Maevskij, V.A. Ryzhov, T.A. Fedorova, I.V. Kozhemyakin, N.M. Burov

STOCHASTIC DYNAMIC MODEL OF UNDERWATER WIRELESS SENSOR NETWORK BASED ON LOUVAIN CLUSTERING ALGORITHM

Underwater wireless sensor networks (UWSNs) play an important role in monitoring ocean processes, underwater navigation, environmental control and security. However, underwater environment features such as high signal attenuation, limited energy resources and changing network topology create significant challenges in organizing efficient data transmission. To optimize network operation and extend its service life, a clustering method is used to group nodes, reduce the load on communication channels and improve energy efficiency. However, in the event of network node failure, static clustering becomes ineffective, which requires the implementation of dynamic reclustering. The procedure of redistributing node roles and rebuilding the network topology allows maintaining communication stability and minimizing data losses, taking into account the energy balance of the entire network as a whole. This paper examines modern approaches to clustering and reclustering in UWSNs taking into account the energy balance, node failure probability and interference in the transmission medium. The development of adaptive UWSN control methods is an urgent task aimed at increasing the reliability, energy efficiency and durability of underwater communication networks. The article presents a stochastic cross-level model for dynamic three-dimensional PBSNs of arbitrary topology. The model uses a new clustering/reclustering technique based on the Louvain algorithm, a routing protocol built on the Dijkstra method, and a time-domain management (TDMA) method. The proposed PBSN operating model is the basis for the developed simulation complex, which allows assessing the efficiency and reliability of the network, taking into account the loss of connectivity and vulnerabilities for PBSNs of various scales and purposes. As part of the research, a parametric analysis of systematic calculations of the PBSN functional characteristics was performed. The results of the analysis showed that the proposed simulation model provides an increase in the autonomous network operation time and a decrease in the number of lost messages compared to the models of other authors.

Underwater wireless sensor networks; stochastic dynamic network model; simulation modeling; clustering; Louvain algorithm; Dijkstra's method; medium access control method based on the transmission schedule.

Введение. Акустические подводные беспроводные сенсорные сети (ПБСС) находят широкое применение в различных областях морской деятельности включая экологический мониторинг, разведку полезных ископаемых, управление подводными объектами и системами, распределенное тактическое наблюдение [1–3]. Однако создание и эксплуатация подобных сетей сопряжены с рядом технических и фундаментальных научных

проблем, связанных со сложностью передачи данных в динамически изменяющейся подводной среде. Для решения этих проблем требуется разработка специализированных алгоритмов и методов, обеспечивающих надежное и энергоэффективное функционирование проектируемых ПБСС.

Существует большое число исследований и обзоров, посвященных разработке протоколов системных уровней модели OSI для акустических подводных беспроводных сенсорных сетей. Целью этих работ являлось достижение лучших функциональных характеристик ПБСС, полученных по критериям энергоэффективности, надежности и производительности. Для достижения оптимальных результатов рассматривались решения задач, связанных с: контролем топологии сети [4–6], использованием мобильных узлов [4, 6–8], разработкой энергоэффективных протоколов маршрутизации/алгоритмов кластеризации [9–13], разработкой протоколов доступа к среде [14–17], оптимизацией протоколов канального уровня [18–22], модернизацией протоколов физического уровня (методов формирования и обработки сигнала) [23]. В рамках перечисленных направлений работ были получены результаты, показывающие определенный прогресс в решении проблем, ограничивающих возможности акустических ПБСС. Наряду с этим было отмечено, что рассматриваемая задача является многопараметрической и многокритериальной и требует комплексного решения. В настоящее время одновременный корректный учет большого числа взаимосвязанных параметров, ограничений и требований остается не реализованным; отмечается, что универсальных протоколов равноэффективных для различных практических приложений пока создать не удается.

Предлагаемая работа авторов нацелена на разработку комплексной стохастической модели функционирования ПБСС, учитывающей достаточно широкий набор проектных параметров и использующей в качестве целевой функции универсальную метрику сети, зависящую как от технических характеристик, топологии сети и физических параметров среды в акватории, так и от динамических особенностей функционирования всей сети в целом, в частности, от выбранных протоколов или динамической перестройки маршрутов.

Ранее авторами рассматривалось сравнение функциональных характеристик стационарной и гибридной архитектур ПБСС, включая анализ энергетических затрат, времени жизни узлов и влияния мобильных элементов на качество связи [16, 17]. С использованием аналитического вероятностного подхода было исследовано влияние проектных параметров (масштаба сети, размещения узлов, технических характеристик передающих и принимающих устройств) на основные функциональные характеристики сети. Было показано, что гибридные решения с мобильными шлюзами (например, волновыми глайдерами) повышают энергоэффективность, связность и надежность сетей [18].

В развитие выполненных исследований, в настоящей работе представлен имитационный подход, позволяющий моделировать функциональность динамических трехмерных гибридных акустических ПБСС произвольной топологии. Для управления функциями физического уровня, канала передачи данных, сетевого уровня в настоящей работе используется межуровневая архитектура платформы имитационного моделирования, основанная на технологии системных уровней модели OSI. Авторами предлагается новая реализация протоколов сетевого уровня (кластеризации и маршрутизации), основанная на применении лувенского алгоритма [19] и метода Дейкстра. Такой подход позволяет динамически адаптировать топологию сети к изменениям как в океанографической обстановке, так и в энергетическом балансе сети, что обеспечивает более равномерное распределение нагрузки по сети и увеличивает продолжительность ее жизни. Разработанный авторами алгоритм реализует динамическую рекластеризацию на основе мониторинга уровня энергии узлов сети, что позволяет динамически перераспределять роли между сенсорами, а также минимизировать число ретрансляций при передаче сообщений (для достижения необходимой надежности). На уровне канала передачи данных в предложенной модели используется метод управления доступом к среде основанный на расписании передач (TDMA).

Сравнение результатов имитационного моделирования, полученных с использованием разработанной стохастической динамической модели, с результатами моделей, базирующихся на протоколах LEACH, UCUBG, DBR, NUC-EB [22] PPWURC [23] ; показало, что предложенная авторами модель для определенных режимов обеспечивает достижение лучших функциональных характеристик для рассмотренных вариантов топологий ПБСС.

Формальная постановка задачи. В работе исследуется задача разработки и оптимизации топологии 3D ПБСС для мониторинга заданной акватории.

Предполагается, что гибридная ПБСС расположена в акватории в физически неоднородной среде и состоит из произвольной трехмерной сетки сенсоров, обыкновенных и референсных и мобильного шлюза, роль которого может выполнять либо волновой глайдер (ВГ), либо иной автономный мобильный шлюз.

Вся система разбита на кластеры, в каждом кластере есть свой, локализованный определенным образом референсный узел, к которому стекается информация от обыкновенных узлов, расположенных в данном кластере. Задачей обыкновенных сенсоров является измерение некоторого набора физических параметров окружающей среды, обработка этих данных и передача напрямую или через цепочку соседей этой информации на свой референсный узел. Обыкновенные агенты сначала передают сообщения референсным агентам своего кластера, а затем референсные агенты передают сообщения вверх, на мобильный шлюз.

Формально поставленную задачу можно описать следующим набором параметров:

♦ Акватория: задана площадь $S = n \times n$ (в планарной проекции) с глубиной h, где сенсоры распределены равномерно или по заданной схеме, определяемой особенностями мониторинга акватории. Например, распределение может учитывать градиенты температуры, солёности или морфологию морского дна.

♦ Подводная беспроводная сенсорная сеть включает множество из N сенсоров $B = \{b_1, b_2, \dots, b_N\}$, где каждый сенсор b обладает следующими характеристиками:

1. Координаты сенсора в пространстве $\overrightarrow{x_i} = (x_i, y_i, z_i)$, где x_i, y_i задают планарное положение, а z_i – глубину размещения. На первом этапе формируется начальная топология сети, которая определяется массивом координат всех сенсоров $\overrightarrow{x_i}$. Распределение узлов может быть равномерным или следовать заданной модели. Все сенсоры разделяются на набор кластеров, каждый из которых состоит из группы узлов, связанных друг с другом. В рамках кластера информация передаётся к центральному референсному узлу и далее на мобильный шлюз.

2. Технические параметры модема, такие как мощность модема P_{bi}, несущая частота f и полоса пропускания Δf. Эти характеристики используются в модели среды, позволяя рассчитать вероятность успешной доставки сообщения вдоль заданного ребра, соединяющего два сенсора. Разработанный имитационный комплекс позволяет использовать и другие технические параметры, такие как характеристики (например, направленность) антенны. В предлагаемой модели антенна считается ненаправленной.

3. Энергетическое состояние E_i сенсора: уровень оставшейся энергии сенсора, уменьшающийся при каждой передаче, приёме сообщений и в режиме ожидания.

Коммуникационная модель предполагает, что сенсоры обмениваются сообщениями, причем вероятность успешной передачи $p(b_i, b_j) = p(r_{ij})$ между двумя сенсорами b_i и b_j определяется в физической модели среды и зависит от:

- расстояния $r(b_i, b_j) = r_{ij}$ между сенсорами;
- технических характеристик модема, перечисленных выше;
- параметров среды, так что в модели среды может быть учтено затухание сигнала, эффекты многолучевого распространения, шумовые помехи и другие физические характеристики океана.

Модель коммуникации может учитывать стохастическую природу подводной среды, где вероятность успешной передачи сообщений определяется как стационарными параметрами, заданными в модели среды, так и изменяющимися условиями, включая временные и пространственные колебания параметров.

Топология: на начальном этапе формируется топология сети (массив координат в пространстве) на основе выбранной модели распределения.

Система моделирования поддерживает несколько различных моделей распределения сенсоров в пространстве:

Random (случайное распределение), рис. 1,а:

$$\overrightarrow{x_i} = (x_i, y_i, z_i), \qquad x_i, y_i \sim U(0, n), \qquad z_i = z_0$$

Regular (регулярная решётка), рис. 1.б:

$$x_i = i \cdot \text{step}, \qquad y_j = j \cdot \text{step}, \qquad z = z_0$$

Fluctuation Regular (регулярная решётка с отклонением), рис.1.в:

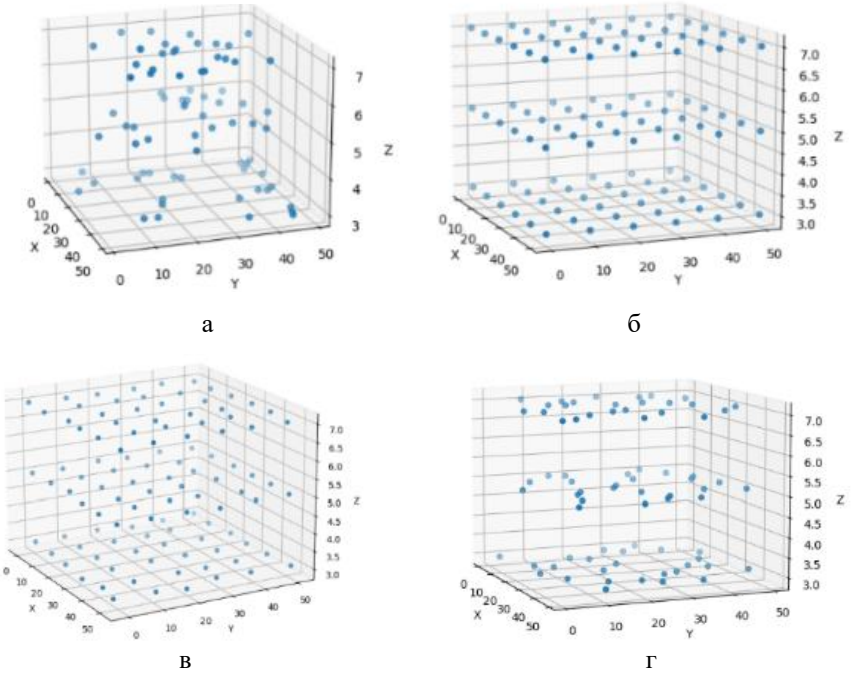
$$x_i = i \cdot s + \epsilon_x, \qquad y_j = j \cdot s + \epsilon_y, \qquad \epsilon_x, \epsilon_y \sim U(-\Delta, \Delta), \qquad z = z_0,$$

где – Δ задаёт амплитуду отклонений.

Pseudo Random (псевдослучайное распределение). Используется последовательность Халтона [31], рис.1.г:

$$(x_i, y_i) = a\ \ lton(b_1, b_2, i),$$

где b_1, b_2, i – взаимно простые основания последовательности Халтона, i – индекс сенсора.



а б в г

Рис. 1. Модели распределения сенсоров в акватории

Данный выбор топологий обоснован в первую очередь учетом особенностей реальной эксплуатации сети, где объекты не могут располагаться в точно заданных позициях.

Физическая модель. Известно, что одним из критериев производительности цифровых систем связи является зависимость вероятности появления ошибочного бита от отношения энергии сигнала, приходящейся на один бит – e_b, к спектральной плотности мощности аддитивного белого гауссовского шума – N_0. Это отношение e_b/N_0 определяется через среднюю мощность сигнала P_s и среднюю мощность шума P_n следующим образом [24]:

$$\frac{e_b}{N_0} = \frac{P_s}{P_n}\frac{B}{f_{bit}}, \tag{1}$$

где B – ширина полосы пропускания, f_{bit} – битовая скорость передачи информации.

Потери при распространении акустического сигнала частотой f на расстояние r от источника в простейшем случае могут быть определены как

$$A(r,f) = r^s a(f)^r,$$

где степень $s = 2$ для сферической волны и $s = 1$ для цилиндрической. Считая, что распространение происходит на глубокой воде и расширение фронта волны является сферическим, возьмем$s = 2$, $a(f)$ – связан с коэффициентом затухания сигнала выраженном в дБ/км по формуле

$$10\,log_{10}\,a(f) = \beta(f).$$

В пределах заданной акватории будем считать, что температура, соленость и кислотность постоянны, тогда коэффициент затухания $\beta(f)$ при заданной частоте звуковых колебаний f используется аппроксимированная формула Торпа с учётом данных для частот 0,1 - 100 кГц. [25]:

$$\beta(f) = \frac{0.1 \cdot f^2}{1+f^2} + \frac{40 \cdot f^2}{4100+f^2} + 2.75 \cdot 10^{-4} \cdot f^2 + 0.0003. \quad (2)$$

Отношение сигнал/шум на расстоянии r от передатчика обозначим $\Gamma(r)$ и определим через нормированное отношение сигнал /шум и потери при распространении сигнала как

$$\Gamma(r) = \frac{e_b}{N_0 A(r,f)} = \frac{e_b}{N_0 r^2 a(f)^r}.$$

В подводном канале с рэлеевским замиранием скорость возникновения битовой ошибки (BER) для двоичной фазовой модуляции BPSK может быть вычислена как [26]:

$$q_e(r) = \frac{1}{2}\left(1 - \sqrt{\frac{\Gamma(r)}{1+\Gamma(r)}}\right) = BER. \quad (3)$$

Тогда для пакета длиной N_{bit} вероятность успешной передачи на расстояние r будет равна

$$p(r) = \left(1 - q_e(r)\right)^{N_{bit}}. \quad (4)$$

Проектные параметры моделирования функциональных характеристик ПБСС. Для определения оптимальной архитектуры сети используется разработанная авторами математическая модель, основанная на вероятностном подходе и критериях оптимальности функционирования ПБСС с точки зрения связности, с учетом ограничений на максимальное число перепосылок N, необходимых для успешной доставки сообщений.

В дальнейшем в имитационной модели использованы следующие проектные параметры. Частота работы модема принята равной $f = 60$ кГц с полосой частот B =30 кГц, битовая скорость – $f_{bit} = 12{,}8$ кбит/с. Считается, что все передаваемые сообщения s имеют одинаковую длину $N_{bit} = 256$ бит. Суммарное время передачи сообщения и получения подтверждения о доставке определяется как $t_s = N_{bit}/f_{bit} = 0.02$ с.

Энергетические характеристики модемов приняты следующими:

$P_s = 25$Вт – максимальная излучаемая мощность передающего модема;

$E_s = P_s \cdot t_s$= 0.5Дж – энергия, необходимая для посылки одного сообщения;

$P_w = 0.3$ Вт – мощность, затраченная на ожидание и прием сообщения, эмпирическая цифра для процессорной системы, ожидающей прием сообщения;

$P_{inf} \approx P_w$ – мощность, затраченная на сбор информации. Это средняя мощность работающей процессорной системы с малым потреблением энергии;

$E_0 = 864$ кДж - емкость батареи напряжением 12В.

Формулы (1)- (4) используются для проектирования и оптимизации подводных беспроводных сенсорных сетей (ПБСС) в разработанном имитационном комплексе. На их основе можно определить:

- оптимальную несущую частоту передачи сигнала f для минимизации затухания;
- максимально допустимое расстояние r между узлами, обеспечивающее требуемую надежность работы сети (определяемое процентом успешно доставленных сообщений);
- вероятность успешной передачи данных для различных физических условий канала.

Эти факторы непосредственно влияют на эффективность и надежность сети.

Алгоритм работы сети с использованием Лувенского метода. Алгоритм работы сети может быть описан последовательностью шагов, представленных на рис. 2.

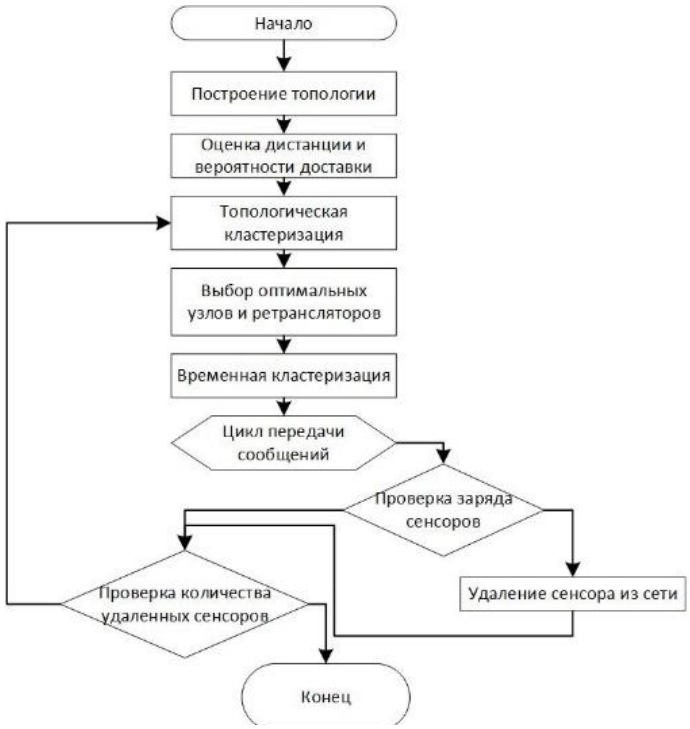


Рис. 2. Блок-схема работы Лувенского алгоритма

Далее более детально рассмотрим основные шаги представленного алгоритма.

Метод построения топологии ПБСС. Топология связей задаётся квадратной матрицей смежности (или матрицей связей), обозначаемой как $A = \{a_{ij}\}$, $i, j = 1, \dots, N$. Элементы этой матрицы a_{ij} указывают на существование связи между узлами b_i и b_j и принимают значения:

- $a_{ij} = 1$ означает, что между узлами b_i и b_j существует связь;
- $a_{ij} = 0$ означает, что связи между узлами i и j нет.

Матрицы смежности являются важным инструментом в анализе сетей, так как они предоставляют компактное и структурированное представление связей между узлами. В контексте оптимизации коммуникации в сетях, таких как сенсорные сети или мультиагентные системы, матрицы смежности играют ключевую роль, обеспечивая эффективные вычисления для маршрутизации, кластеризации и управления ресурсами.

Кроме матрицы смежности введем весовую матрицу W с элементами $w_{ij} = p(r_{ij})$, для всех узлов сети.

В основе алгоритма лежит оптимизация коэффициента модулярности M кластеров вершин. Она используется для оценки того, насколько хорошо сеть разделена на группы узлов, тесно связанных друг с другом, с минимальным числом связей между различными группами. Коэффициент модулярности M в оригинальном алгоритме представляет собой плотность ребер внутри кластера в диапазоне $[-1,1]$ в сравнении с количеством межкластерных ребер.

В контексте ПБСС модулярность M используется для создания энергоэффективной топологии. Сеть делится на группы сенсоров (кластеры), в которых узлы тесно связаны друг с другом и оптимально передают данные через центральные узлы (референсные сенсоры). Высокая модулярность помогает минимизировать энергопотребление: класте-

ризация снижает количество дальних передач, что уменьшает расход энергии. Увеличивается вероятность успешной передачи данных внутри кластеров. Динамическое обновление кластеров на основе модулярности позволяет учитывать изменения в энергосостоянии узлов или потери узлов.

Значение коэффициента модулярности M рассчитывается как:

$$M = \frac{1}{2m}\sum_{i,j}\left[a_{ij}w_{i,j} - \frac{w_i w_j}{2m}\right]\delta(c_i, c_j), \quad (5)$$

где

a_{ij} – элемент матрицы смежности равный 1 или 0 на данной итерации;

$w_{i,j}$ – вес ребра между вершинами i и j, которые могут объединиться в кластер;

w_i и w_j – сумма весов ребер i и j, инцидентных вершинам i и j, на которых элементы матрицы смежности равны 1 на данной итерации, так что имеют место формулы

$$\sum_k w_{jk}a_{ij} = w_j \text{ и } \sum_l w_{il}a_{ij} = w_i,$$

где вершины k и l – это все узлы сети, связанные с i и j соответственно;

m – общее количество рёбер в сети,

$\frac{w_i w_j}{2m}$ – средневзвешенная вероятность передачи сигнала от узлов i и j по всей сети;

Разность $\left[a_{ij}w_{i,j} - \frac{w_i w_j}{2m}\right]$ показывает, что если вероятность доставки между узлами i и j выше, чем средневзвешенная вероятность передачи сигнала от узлов i и j по всей сети, то эта разность положительна, и узлы имеет смысл сгруппировать в один кластер. Если эта разность отрицательна, то скорее всего узлы должны принадлежать разным кластерам.

$\delta(c_i, c_j)$ – индикатор принадлежности узлов i и j к одному кластеру.

Коэффициент модулярности отдельного кластера определяется как:

$$M_c = \frac{\sum_{i=1}^{n} w_i^c}{2m}\{c_i = c_j = c\} - \left(\frac{\sum_{i=1}^{k}\left(w_i^c + w_i^{c\prime}\right)}{2m}\{c_i = c\}\right)^2 = \frac{\Sigma_{\text{in}}}{2m} - \left(\frac{\Sigma_{\text{tot}}}{2m}\right)^2, \quad (6)$$

где M_c – модулярность кластера;

w_i^c – вес внутрикластерного ребра;

$\sum_{i=1}^{n} w_i^c = \Sigma_{\text{in}}$ – сумма весов ребер между узлами внутри сообщества с (каждое ребро учитывается дважды). Увеличение Σ_{in} приводит к повышению модулярности, так как узлы становятся более "связанными" в рамках кластера;

$w_i^{c\prime}$ – вес межкластерного ребра;

$\sum_{i=1}^{k}\left(w_i^c + w_i^{c\prime}\right) = \Sigma_{\text{tot}}$ – сумма всех весов ребер для узлов внутри сообщества (включая ребра, соединяющие узлы сообщества с узлами за его пределами). Чем меньше Σ_{tot}, тем меньше "утечек" связей за пределы кластера, что также повышает модулярность.

n – число внутрикластерных ребер;

k – общее число ребер, инцидентных всем вершинам кластера.

Так как узлы в разных сообществах не вносят вклад в модульность M, общее значение модульности можно записать как:

$$M = \sum_c M_c. \quad (7)$$

Метод кластеризации сети на основе Лувенского алгоритма. Лувенский алгоритм выбран исходя из его способности работать с динамическими 3D-сетями, где глубина и геометрия влияют на качество связи.

Этап 1. Локальная оптимизация модулярности. На первой стадии выполняется поиск локальных кластеров минимальных размеров с оптимальным значением функции модульности.

Выбирается произвольный кластер, из которого вершина переставляется по очереди в каждый соседний кластер. После перестановки подсчитывается изменение коэффициента модулярности ΔM до и после перестановки вершины и выбирается кластер с наибольшим изменением модулярности так, что $\Delta M > 0$, в котором закрепляется переставленная вершина. Если ни одна из перестановок не увеличивает модульность, то вершина остается в том же кластере. Данный пункт повторяется, пока изменения коэффициента не будут неизменными.

Пересчёт изменения модулярности ΔM:

$$\Delta M = \left[\frac{\Sigma_{in} + w_i}{2m} - \left(\frac{\Sigma_{tot} + w_i}{2m}\right)^2\right] - \left[\frac{\Sigma_{in}}{2m} - \left(\frac{\Sigma_{tot}}{2m}\right)^2\right]. \quad (8)$$

Для каждого узла вычисляется, как его перемещение из текущего кластера в другой (или создание нового кластера) повлияет на значение модулярности ΔM.

Выбор кластера с максимальным ΔM. Узел переносится в тот кластер, который обеспечивает наибольшее увеличение модулярности. Если перемещение узла не улучшает модулярность (или ухудшает её), узел остаётся в своём текущем кластере.

Формула ΔM обеспечивает сравнение текущего вклада узла i в модулярность с его вкладом после переноса.

Этап 2. Сжатие сети. Сжатие сети — это второй этап работы Лувенского алгоритма, следующее за локальной оптимизацией модулярности (M). Этот этап направлен на уменьшение размерности исходной сети путём формирования новой, более компактной сети. На этом этапе узлы, принадлежащие одному кластеру, объединяются в суперузлы.

Общая идея шагов на втором этапе, следующая:

Граф с кластерами преобразуется в мультиграф. Вершины кластеров объединяются в одну с преобразованием ребер между ними в петли, а кратные ребра между полученными вершинами заменяются одним. Новые веса петель и ребер пересчитываются как среднее арифметическое из весов старых ребер.

Этапы 1 и 2 повторяются, пока не будет достигнута оптимальная величина коэффициента модульности (когда изменений модульности больше не будет происходить).

В результате кластеризации сеть разбивается на k кластеров ($C_1, C_2, \ldots, C_k$), где каждый кластер содержит набор узлов B_i, определяемый в соответствии с оптимизацией модулярности.

Выбор референсного узла. Для этого из общего графа сети выделим подграф, содержащий только узлы, принадлежащие одному кластеру C_l. Для выбора референсного узла при первой кластеризации сети используется средневзвешенная вероятность передачи сигнала от узла i к узлу j, обозначаемая $w(b_j)$, которая показывает, сколько рёбер эффективно (с учетом вероятности доставки) соединяет узел b_j с другими узлами $b_i \in C_l$ внутри кластера. Формула расчёта средневзвешенной вероятности передачи сигнала на узел b_j:

$$w(b_j \in C_l) = \frac{1}{2m_l} \sum_{b_i \in C_l} w_{ij}, \quad (9)$$

где w_{ij} – вероятность успешной передачи данных между узлами b_i и b_j, принадлежащими одному и тому же кластеру C_l, Референсным узлом кластера назначается узел с наибольшей средневзвешенной вероятностью передачи сигнала. Она определяется по следующему правилу:

$$b_{ref(C_l)} = \arg\max_{b_j \in C_l} w(b_j \in C_l). \quad (10)$$

Благодаря наибольшему числу связей с другими узлами в своём кластере он становится наиболее эффективным выбором для управления передачей данных внутри кластера.

При разряде батарей сенсоров и появлении необходимости динамической рекластеризации сети, узлы с большим числом связей окажутся, очевидно, наиболее разряженными, поэтому кроме связности необходимо еще учитывать остаточную энергию сенсора. Обозначим ее как

$$\varepsilon_j = \frac{E_j}{E_0}, \quad (11)$$

E_0 (Дж) – начальный уровень заряда батареи сенсора, E_j(Дж) – текущее состояние заряда батареи, тогда формула расчёта средневзвешенной вероятности передачи сигнала на узел b_j заменится на формулу средневзвешенной эффективности работы узла:

$$Eff_{node}(b_j \in C_l) = \frac{1}{2m_l} \sum_{b_i \in C_l} w_{ij}\, \varepsilon_j. \quad (12)$$

Тогда референсным будет назначен узел

$$b_{ref(C_l)} = \arg\max_{b_j \in C_l} Eff_{node}(b_j \in C_l).$$

Для каждого кластера C_l создаётся следующая структура: $\{C_l \mapsto \{j \mid b_j\}, b_{ref(C_l)}\}$

Таким образом, каждый кластер представляется парой чисел, где:

- Первое значение j – узел, входящий в кластер.
- Второе значение $b_{ref(C_l)}$ – центральный (референсный) узел, который выполняет функции управления и координации передачи данных внутри этого кластера.

Этот подход обеспечивает эффективное управление кластером и минимизирует задержки и энергопотребление при передаче данных.

В контексте подводных сенсорных сетей, лувенский алгоритм используется для группировки сенсоров в кластеры, основываясь на следующих параметрах:

- Узлы, расположенные близко друг к другу, объединяются в один кластер для минимизации энергозатрат на передачу данных.
- Сенсоры с высокой остаточной энергией чаще выбираются в качестве референсных узлов (глав узлов).
- Учитывается вероятность успешной передачи сообщений между узлами, зависящая от расстояния, мощности сигнала и условий среды.

Использование модифицированного алгоритма Дейкстры для нахождения оптимальных путей передачи сообщений в кластере. Для повышения налдежности передачи данных в условиях подводной среды предложен алгоритм на основе метода Дейкстры, который вместо минимизации расстояния фокусируется на выборе маршрутов с максимальной вероятностью успешной передачи сообщений.

Шаги модифицированного алгоритма:

1. Инициализация. Узлы сенсоров представляются вершинами графа $G = (B, L)$, где B – множество сенсоров, а L – рёбра, представляющие возможные пути связи между сенсорами.

Каждое ребро l_{ij} между узлами i и j имеет вес, определяемый вероятностью успешной передачи сообщения $w_{ij} = p(r_{ij})$, которая в общем случае зависит от расстояния между узлами, акустических характеристик канала и мощности передающего модема и уровнем остаточной энергии узла передатчика ε_i и узла приемника ε_j, так что формула расчёта средневзвешенной вероятности передачи сигнала заменится на формулу средневзвешенной эффективности передачи по ребру:

$$\varepsilon_i = \frac{E_i}{E_0}, \qquad \varepsilon_j = \frac{E_j}{E_0}, \qquad Eff_{route}(b_i, b_j) = w_{ij}\varepsilon_i\varepsilon_j, \quad (13)$$

E_0 (Дж) – начальный уровень заряда батареи сенсора, E_i(Дж) и E_j(Дж) – текущее состояние заряда батареи,

Для каждого узла $b \in B$ вводится значение $D(b)$, отражающее текущую вероятность передачи сообщения от исходного узла до узла v. В начале $D(b) = 0$ для всех узлов, кроме исходного узла s, где $D(s) = 1$. Создается массив $Prev(b)$, который фиксирует предшествующий узел в оптимальном маршруте до b.

2. Выбор исходного узла. Алгоритм начинается с некоторого исходного узла s, который может быть референсным узлом кластера или узлом, откуда начинается передача данных. Узел s помещается в множество S, представляющее обработанные узлы.

3. Обновление вероятностей соседних узлов. Для каждого узла u, соседнего с s, пересчитывается вероятность успешной передачи:

$$D(u) = \max\left(D(u), D(s) \cdot Eff_{route}(b_i, b_j)\right), \quad (14)$$

где $Eff_{route}(b_s, b_u)$ – средневзвешенная эффективность передачи по ребру между узлами s и u. Если $D(u)$ обновлено, то в $Prev(v)$ записывается s.

4. Выбор следующего узла. Среди всех узлов, не входящих в S, выбирается узел b с максимальным значением $D(b)$:

$$b = \arg\max_{u \notin S} D\,(u). \quad (15)$$

Этот узел добавляется в множество S.

5. Повторение шагов. Алгоритм повторяет шаги 3–4 до тех пор, пока не будут обработаны все узлы в графе или пока не будет найден путь до целевого узла. Возможно еще ограничение, связанное с тем, что построение маршрута возможно только внутри кластера.

6. Реконструкция пути. После завершения работы алгоритма путь от исходного узла s до любого другого узла t реконструируется с помощью массива $Prev$, который фиксирует предшествующий узел на пути.

В результате в каждом кластере $C_k \subset B$ оказываются построены оптимальные пути с наибольшей эффективностью передачи сообщений от референсного сенсора $b_{ref(C_k)}$ к остальным сенсорам в кластере. Определим функцию пути $\mathcal{R}(b_i, b_j)$ как путь между двумя сенсорами b_i и b_j через цепочку промежуточных сенсоров ($b\_\{k\_1\}, b\_\{k\_2\}, \ldots$) с вероятностью передачи:

$$Eff_{route}(b_i, b_j) = \prod_{k=1}^{m} Eff_{route}(b_k, b_{(k+1)}), \quad (16)$$

где m – количество промежуточных сенсоров на пути, $p_{k(k+1)}$ – вероятность передачи между двумя последовательными сенсорами на пути. Модифицированный алгоритм Дейкстры находит путь $\mathcal{R}(b_i, b_{ref(C_k)})$ с наибольшей эффективностью передачи сообщения для каждого $(b_i \in C_k)$:

Для каждого узла учитывается остаток энергии, что позволяет избегать маршрутов через узлы с критически низким уровнем заряда. Сеть адаптируется к изменениям среды или расход энергии. Вероятности передачи $p(r_{ij})$ и веса рёбер постоянно обновляются.

Вместо одного оптимального пути могут быть рассчитаны несколько маршрутов с высокой вероятностью передачи, что повышает надёжность сети. Алгоритм применяется локально для кластеров, что снижает вычислительные затраты и повышает масштабируемость сети. Эта модификация алгоритма Дейкстры позволяет учитывать уникальные особенности подводной среды, что делает её особенно эффективной для подводных беспроводных сенсорных сетей.

Пример работы топологической кластеризации и иерархического присвоения уровня ретрансляции представлен на рис. 3

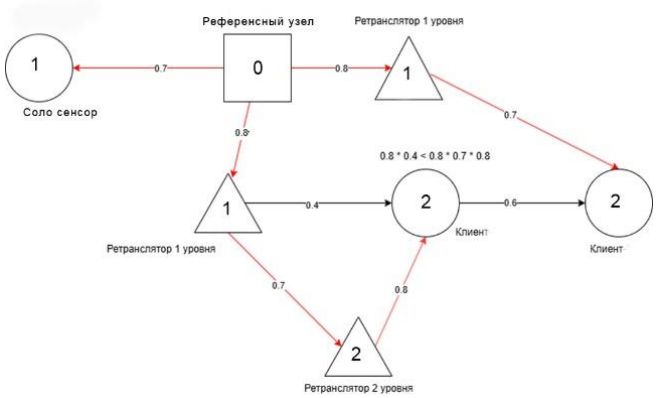


Рис. 3. Определение уровней ретрансляции в сети

Метод управления доступом к среде на основе расписания передач. В основе алгоритма реализующего протокол обмена сообщениями лежит принцип временного разделения (временных слотов) – TDMA (Time Division Multiple Access) [27], благодоря которому каждый сенсор сети может получить свои временные слоты для передачи сообщений.

Порядок формирования временных слотов. На первом этапе временные слоты выделяются для сенсоров, работающих в режиме соло (без ретрансляторов).

На следующем этапе временные слоты назначаются сенсорам-клиентам.

Алгоритм принимает на вход список всех сенсоров. Затем происходит итеративный перебор сенсоров, пока все не будут распределены по временным слотам. При распределении сенсора в слот проверяются следующие условия:

- Отсутствие интерференции: сенсор может быть назначен в слот только в том случае, если он находится на таком расстоянии, чтобы не создавать помех сенсорам, уже распределённым в данный временной слот.
- Уникальность адреса: в данном слоте не должно быть других сенсоров, отправляющих данные в тот же целевой сенсор.
- Учет минимального номера слота: номер текущего слота должен быть больше минимального допустимого номера для рассматриваемого сенсора.

В каждом TDMA-кадре каждый сенсор знает о своих собственных зарезервированных временных слотах в зависимости от его номера, а также о слотах, зарезервированных его соседними узлами. Таким образом, они могут запланировать активацию либо для передачи своего собственного пакета данных в течение зарезервированных слотов, либо для получения пакета данных от соседнего узла. Они спят в других оставшихся слотах, когда нет передачи или приема данных. Эта схема повторяется в течение каждого TDMA-кадра. Каждый TDMA-кадр T_{frame} разделен на количество слотов одинакового размера, t_{slot}. Количество слотов можно рассчитать, как:

$$N_{slot} = \frac{T_{frame}}{t_{slot}}. \quad (17)$$

Длина слота t_{slot} имеет вид

$$t_{slot} = t_s + T_C + \tau \quad (18)$$

и складывается из времени, необходимого для отправки сообщения $t_s = 0.02\ c$, задержки распространения сигнала $T_C = 2\,{}^{r}/_{v_c}$ и τ – это некоторое защитное время, которое используется для обеспечения того, чтобы отдельные передачи не мешали друг другу.

Каждому сенсору в течении одного кадра разрешено выходить в эфир только один раз (в одном из временных слотов). Это значит, что одна отправка сообщения занимает у любого сенсора время $T_{frame} = N_{slot} t_{slot}$. Время T_c пока сигнал распространяется в водной среде сенсор не может ни отправлять другие сообщения, ни получать, а вынужден находиться в режиме ожидания. Кроме того, он находится в режиме ожидания в течении $(N_{slot} - 1)t_{slot}$. После временного интервала T_{frame} сенсор b может переходить к отправке следующего сообщения или перепосылке данного сообщения тому же или другому соседу.

Описание алгоритма распределения сенсоров во временные слоты:

Инициализация. Первый сенсор из списка B назначается в первый временной слот $(i = 1)$: $b_1 \in T_1$. Это означает, что данный сенсор начинает процесс распределения временных слотов.

Распределение следующих сенсоров. Для каждого последующего сенсора распределение во временные слоты выполняется на основе следующего выражения. Пусть в слот T уже распределены сенсоры b_1, $b_2 \ldots b_{i-1}$. Тогда сенсор b_i можно распределить в тот же временной слот, если

$$T_{ts}(b) = \{b_i \in B \mid a_{i,i-1} \quad 0 \wedge b\,(b_i) \neq b\,(b_{i-1})\}, \quad (19)$$

где

$a_{i,i-1}$= 0 – сенсор b_i и ранее распределенный сенсор b_{i-1} могут оказаться в одном временном слоте, если они не связаны,

$b\ (b_i)$ – целевой сенсор, которому b_i передаёт сообщение. Условие $b\ (b_i) \neq b\ (b_{i-1})$ означает, что в одном временном слоте не должно быть двух сенсоров, передающих данные в один и тот же целевой сенсор.

Распределение ретрансляторов. Для каждого ретранслятора вычисляется его уровень ретрансляции k_b от референсного узла. Все сенсоры на данном уровне k_b рассматриваются для распределения в временные слоты. Ретранслятор может быть добавлен в временной слот только если он не создаёт интерференции с другими сенсорами в том же слоте.

Схематичное представление работы алгоритма представлено на рис. 4.

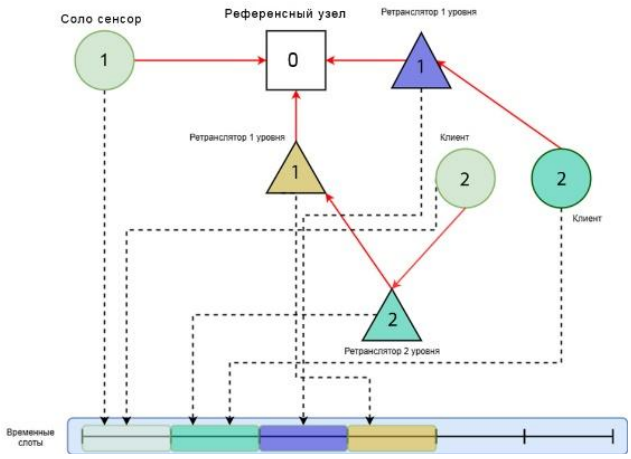


Рис. 4. Реализация TDMA протокола

На рис. 4 кружками отмечены обычные сенсоры, квадратом отмечен референсный узел в каждом кластере, треугольниками отмечены сенсоры ретрансляторы. Стоит также заметить, что на рисунке 4 одинаковым цветом выделены одинаковые временные слоты передачи сигнала.

Динамическая рекластеризация и процесс завершения работы ПБСС. Процесс динамической рекластеризации в подводной беспроводной сенсорной сети (ПБСС) является ключевым механизмом, обеспечивающим надежность и энергоэффективность системы при длительной эксплуатации. Сеть, состоящая из множества узлов, организованных в кластеры, функционирует до тех пор, пока достаточное количество узлов обладает энергетическим запасом для передачи данных.

На каждом этапе передачи данных происходит мониторинг уровня энергии узлов в сети. У каждого сенсора сети b_i есть текущее значение энергии E_i, и существует пороговое значение энергии $E_{\min}$, ниже которого узел считается "мертвым" и более не участвует в процессе передачи данных. Процесс динамической рекластеризации инициируется, когда хотя бы один узел в сети достигает критического уровня энергии:

$$E_i < E_{\min}. \tag{20}$$

В этом случае сеть перестраивает свою топологию, что включает пересчет вероятностей кластеризации, обновление всех матриц связей и построение новых топологических и временных кластеров.

Завершение работы сети. Процесс передачи данных продолжается в новой конфигурации до тех пор, пока количество активных сенсоров B_{alive} не упадет ниже определенного порогового значения $min(B_{alive})$ при котором сеть считается неработоспособной

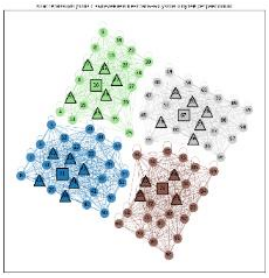
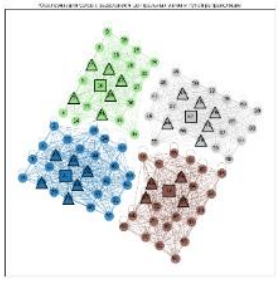
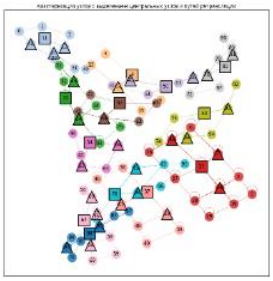
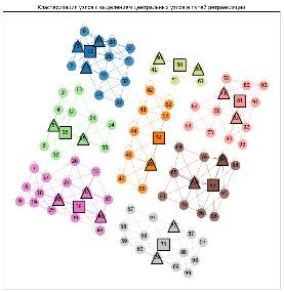
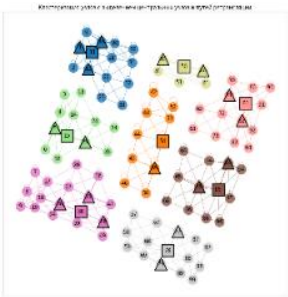
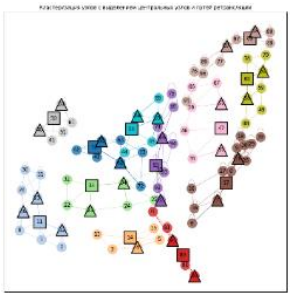
$$|B_{alive}| < min(B_{alive}). \tag{21}$$

Результаты работы имитационного комплекса моделирования сети ПБСС. Имитационный комплекс моделирования разработан на основе языка программирования Python с использованием дополнительных библиотек.

На первом этапе было проведено исследование зависимости количества кластеров от частоты передачи сигнала и размера акватории. Параметры сенсоров сети были взяты аналогично работам [16–18]. Был рассмотрен диапазон частот *f* от 20 kHz до 60 kHz., с расстояниями *r* между сенсорами от 1000 м. до 3000 м. Полученные результаты кластеризации сведены в табл. 1.

Таблица 1

Визуализация топологической кластеризации при различных частотах f и расстояниях r

f= 20 kHz, *r*=1000 м.	*f*= 20 kHz, *r*=2000 м.	*f*= 20 kHz, *r*=3000 м.
		
f= 40 kHz, *r*=1000 м.	*f*= 40 kHz, *r*=2000 м.	*f*= 60 kHz, *r*=1000 м.
		

Стоит отметить закономерность, что при увеличении расстояний между сенсорами, увеличивается количество кластеров и при предельно больших расстояниях каждый сенсор становится отдельным кластером. Как видно, при увеличении частоты сигнала при одинаковых размерах количество кластеров также увеличивается, что обусловлено большей потерей данных на больших частотах.

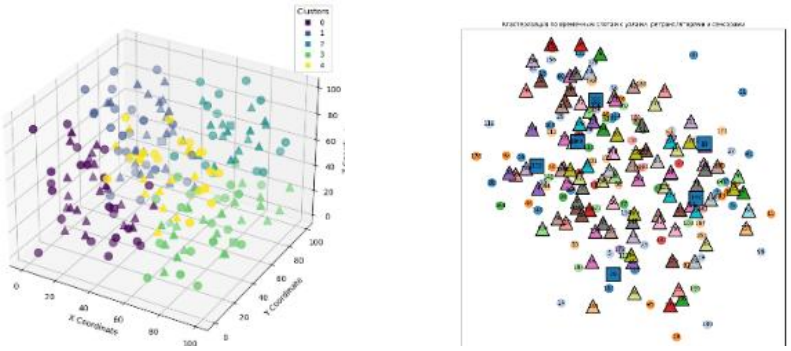
Следующим этапом было проведено сравнительное моделирование разработанного алгоритма в трех случаях: №1 с алгоритмами LEACH, UCUBG, DBR, NUC-EB [22]; №2 с алгоритмами LEACH, ICA, PPWURC и др. [23]; с ранее выполненными работами авторов [16–18]. Входные параметры моделирования № 1 и № 2 представлены в табл. 2.

Таблица 2

Входные параметры моделирования

	№1	№2	№3
Размер акватории (м.)	100×100×100	150*150*150	10000*10000
Начальная энергия (Дж.)	2000	40	864
Частота передачи сигнала (кГц)	10	40	60
Количество сенсоров (шт.)	200	30	100

Эксперимент 1. Рассматривался случай псевдослучайного распределения сенсоров на основе алгоритма Халтона. Результаты согласно параметрам из табл. 2 представлено на рис. 5.



а б

Рис. 5. Моделирование работы сети в эксперименте 1

В результате распределения было образовано 5 топологических кластеров, представленных на рис. 5,а, количество временных слотов (представленных на рис. 5,б – 8. В результате выполнения моделирования были получены данные о количестве выживших сенсоров в зависимости от количества итераций. Собранные данные были сравнены с другими исследованиями и отображены на одном графике, который представлен на рис. 6.

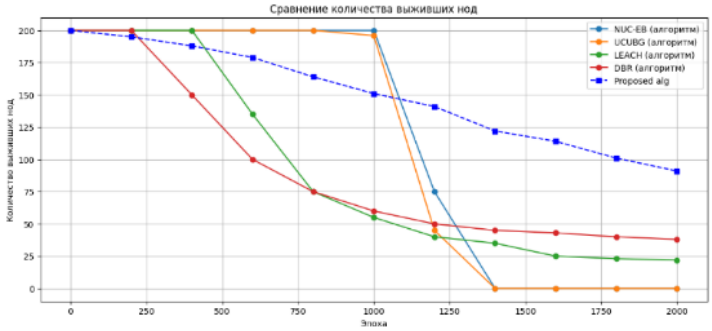


Рис. 6. График количества выживших сенсоров в зависимости от количества эпох (синяя пунктирная линия – предложенный алгоритм кластеризации)

Эксперимент 2. Рассматривался случай случайного распределения сенсоров в акватории. Результаты согласно параметрам из табл. 2 представлены на рис. 7, 8.

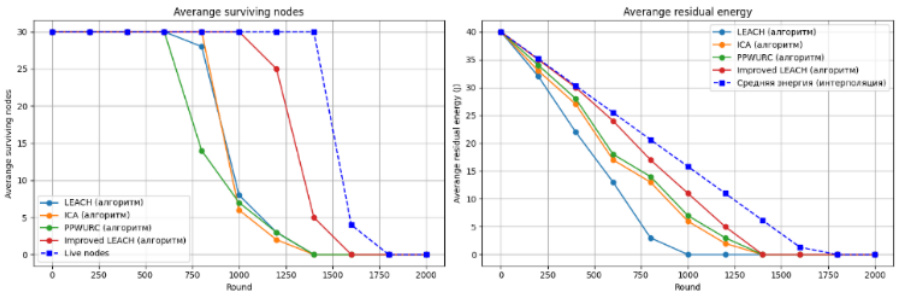


Рис. 7. Графики количества выживших сенсоров в зависимости от количества эпох и средней энергии сенсоров в сети (синяя пунктирная линия – предложенный алгоритм кластеризации)

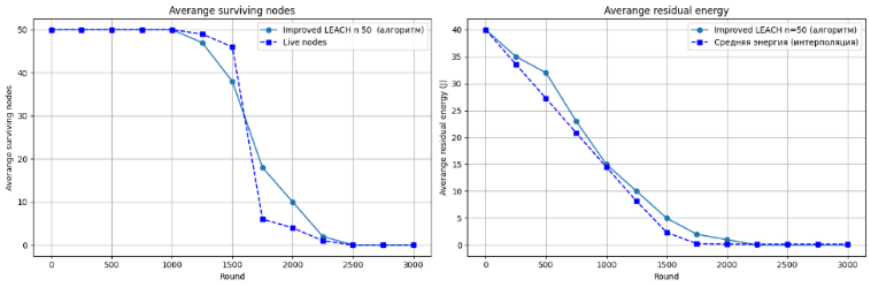


Рис. 8. Графики количества выживших сенсоров в зависимости от количества эпох и средней энергии сенсоров в сети (синяя пунктирная линия – предложенный алгоритм кластеризации)

Результаты, полученные в ходе второго эксперимента, демонстрируют существенное увеличение времени жизни сети в целом. При рассмотрении сети, состоящей из 30 сенсоров, разряд сети начинается после 1400 эпохи, в то время как при иных методах кластеризации сеть начинает разряд значительно раньше (на 1000 эпохе или ранее). На рисунке 8 представлен график разряда сети, демонстрирующий меньшую скорость разряда в предложенном алгоритме кластеризации, по сравнению с другими рассмотренными методами.

Эксперимент 3. Рассматривался случай регулярного ортогонального распределения сети, состоящей из трех слоев на каждом из которых задана своя вероятность доставки сообщения. Результаты зависимости полных энергетических затрат от линейного размера сети (N) и сравнения количества потерянных пакетов (PLR) от количества максимального количества перепосылок (N), согласно параметрам, из табл. 2 представлен на рис. 9.

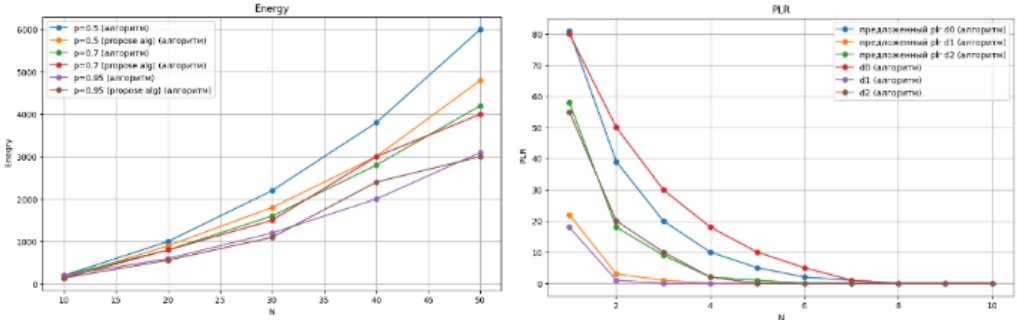


Рис. 9. Графики зависимости энергии сети от линейного размера сети и график PLR от максимального количества перепосылок

Результаты моделирования подтверждают высокую энергетическую эффективность и качество передаваемых данных при идентичных параметрах сенсорной сети

Выводы. Представленная имитационная модель позволяет решать ряд ключевых проблем, связанных с управлением ресурсами ПБСС. Во-первых, предложенный алгоритм уменьшает количество потерянных сообщений за счет оптимизации процесса передачи данных. Во-вторых, алгоритм позволяет снизить общее энергопотребление сети, за счет балансировки нагрузки между узлами и эффективного использования ретрансляторов. Используемый TDMA протокол, обеспечивает одновременную работу временных слотов, что также сокращает общее время работы сети, минимизируя энергозатраты. Предложенная методология рекластеризации повышает надежность сети и увеличивает время её автономной работы.

Следует отметить, что применение лувенского алгоритма для кластеризации в подводных беспроводных сенсорных сетях обеспечивает несколько преимуществ.

Гибкость в адаптации к динамике сети. В реальных условиях подводные сенсоры могут двигаться под воздействием течений или других факторов, изменяя свою позицию в сети. Лувенский алгоритм с его возможностью динамической рекластеризации позволяет поддерживать эффективную структуру сети даже в таких условиях.

Энергоэффективность. Благодаря использованию энергетических параметров при кластеризации, предложенный метод снижает нагрузку на узлы с низким уровнем энергии, что позволяет продлить время жизни сети.

Минимизация потерь при передаче данных. За счет кластеризации алгоритм снижает количество дальних передач между узлами, что особенно важно для подводной среды, где потери сигнала значительно выше, чем в наземных сетях.

Таким образом, использование лувенского алгоритма и метода Дейкстра в предложенной модели позволило построить устойчивую, адаптивную и энергоэффективную кластерную структуру для подводной беспроводной сенсорной сети.

Сравнение полученных результатов имитационного моделирования с результатами моделей других авторов демонстрируют увеличение времени жизни ПБСС и большую надежность доставки сообщений для рассмотренных конкретных сетей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Буров Д.В., Каменная Е.В., Щербинина И.А.* Локализация и маршрутизация в беспроводных подводных сетях, используемых для охраны мариферм // ТДР. – 2017. – № 2. – URL: https://cyberleninka.ru/article/n/lokalizatsiya-i-marshrutizatsiya-v-besprovodnyh-podvodnyh-setyah-ispolzuemyh-dlya-ohrany-mariferm (дата обращения: 26.02.2025).
2. *Громашева О.С., Каменная Е.В., Леонтьева Н.А., Щербинина И.А.* Обзор возможностей применения подводной акустической сенсорной сети и предлагаемых архитектурных решений реализации // ТДР. – 2016. – № 2. – URL: https://cyberleninka.ru/article/n/obzor-vozmozhnostey-primeneniya-podvodnoy-akusticheskoy-sensornoy-seti-i-predlagaemyh-arhitekturnyh-resheniy-realizatsii (дата обращения: 26.02.2025).
3. *Тарик А., Азам Ф., Анвар М. В., Захур Т., Музаффар А.В.* Последние тенденции в развитии подводной беспроводной сенсорной сети: систематический обзор литературы // Тр. ИСП РАН. – 2021. – № 1. – URL: https://cyberleninka.ru/article/n/poslednie-tendentsii-v-razvitii-podvodnoy-besprovodnoy-sensornoy-seti-sistematicheskiy-obzor-literatury (дата обращения: 26.02.2025).
4. *Heinzelman W.R., Chandrakasan A. and Balakrishnan H.* Energy-efficient communication protocol for wireless microsensor networks // Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 2000. – Vol. 2. – P. 10. – DOI: 10.1109/HICSS.2000.926982.
5. *Younis O. and Fahmy S.* HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks // in IEEE Transactions on Mobile Computing. – Oct.-Dec. 2004. – Vol. 3, No. 4. – P. 366-379. – DOI: 10.1109/TMC.2004.41.
6. *Sangho Yi, Junyoung Heo, Yookun Cho, Jiman Hong.* PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks // Computer Communications. – 2007. – Vol. 30, Issues 14–15. – P. 2842-2852. – ISSN 0140-3664, 10.1016/j.comcom.2007.05.034.
7. *Татарникова Т.М., Бимбетов Ф., & Горина Е.В.* Алгоритм энергоэффективного взаимодействия узлов беспроводной сенсорной сети // Научно-технический вестник информационных технологий, механики и оптики. – 2022. – 22 (2). – С. 294-301.
8. *Li Qing, Qingxin Zhu, Mingwen Wang.* Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks // Computer Communications. – 2006. – Vol. 29, Issue 12. – P. 2230-2237. – ISSN 0140-3664, doi.org/10.1016/j.comcom.2006.02.017.
9. *Khan A., & Pirzada A.* Energy-Efficient Vertical Communica-tion in Underwater Wireless Sensor Networks // International Journal of Communication Systems. – 2012. – 25 (12). – P. 1585-1601.
10. *Partan J., Kurose J., & Levine B.N.* A Survey of Practical Is-sues in Underwater Networks // ACM SIGMOBILE Mobile Computing and Communications Review. – 2006. – 11 (4). – P. 23-33.
11. *Heinzelman W.B., Chandrakasan A., & Balakrishnan H.* Energy-Efficient Communication Protocol for Wireless Microsensor Networks // Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. – 2000. – P. 1-10.
12. *Rodoplu V., & Meng T.H.* Minimum Energy Mobile Wireless Networks // IEEE Journal on Selected Areas in Communications. – 1999. – 17 (8). – P. 1333-1344.
13. *Kartik P., & Hanno T.* Probabilistic Routing in Underwater Sensor Networks: A Survey and the Way Forward // IEEE Communications Surveys & Tutorials. – 2015. – 17 (2). – P. 626-647.

14. *Евстифеева Е.А., Семейкин В.Д.* Методика выбора головного кластерного узла в беспроводной сенсорной сети на основе нечеткой логики // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2018. – № 1. – URL: https://cyberleninka.ru/article/n/metodika-vybora-golovnogo-klasternogo-uzla-v-besprovodnoy-sensornoy-seti-na-osnove-nechetkoy-logiki (дата обращения: 26.02.2025).
15. *Махров С.С.* Нейросетевая кластеризация узлов беспроводной сенсорной сети // T-Comm. – 2014. – № 6. – URL: https://cyberleninka.ru/article/n/neyrosetevaya-klasterizatsiya-uzlov-besprovodnoy-sensornoy-seti (дата обращения: 26.02.2025).
16. *Fedorova T.A., Ryzhov V.A., Safronov K.S. et al.* Energy-Efficient and Reliable Deployment Models for Hybrid Underwater Acoustic Sensor Networks with a Mobile Gateway // J. Marine. Sci. – 2024. – Appl. 23. – P. 960-983. – https://doi.org/10.1007/s11804-024-00444-z.
17. *Федорова Т.А., Рыжов В.А., & Сафронов К.С.* Использование гибридной коммуникационной архитектуры подводной беспроводной сенсорной сети для повышения ее времени жизни и эффективности // Информатика и автоматизация. – 2024. – 23 (5). – С. 1532-1570.
18. *Fedorova T.A., Ryzhov V.A., Semenov N.N. et al.* Optimization of an Underwater Wireless Sensor Network Architecture with Wave Glider as a Mobile Gateway // J. Marine. Sci. – 2022. – Appl. 21. – P. 179-196. – https://doi.org/10.1007/s11804-022-00268-9.
19. *Mar M. De er, Arthur S.C. França, Debabrata Panja, Michael X. Cohen.* Characterizing neural phase-space trajectories via Principal Louvain Clustering // Journal of Neuroscience Methods. – 2021. – Vol. 362. – 109313. – ISSN 0165-0270, https://doi.org/10.1016/j.jneumeth.2021.109313.
20. *Грошков П.В.* Автоматизация процесса передачи данных по сети. Множественный доступ // Проблемы Науки. – 2017. – № 18 (100). – URL: https://cyberleninka.ru/article/n/avtomatizatsiya-protsessa-peredachi-dannyh-po-seti-mnozhestvennyy-dostup (дата обращения: 26.02.2025).
21. *Базаров Ю.И., Исмагилов М.И., Рогов А.Н.* Новая морская цифровая связь для е-Навигации // Транспорт Российской Федерации. Журнал о науке, практике, экономике. – 2018. – № 3 (76). – URL: https://cyberleninka.ru/article/n/novaya-morskaya-tsifrovaya-svyaz-dlya-e-navigatsii (дата обращения: 26.02.2025).
22. *Yi J., Tang J., Yuan F., Qiao G., Dai D.* Non-Uniform Clustering Algorithm for UWSNs Based on Energy Equalization Non-Uniform Clustering Algorithm for UWSNs Based on Energy Equalization // Sensors. – 2023. – 23. – 5466. – https://doi.org/10.3390/s23125466.
23. *Tian K., Zhou C., Zhang J.* Improved LEACH Protocol Based on Underwater Energy Propagation Model, Parallel Transmission, and Replication Computing for Underwater Acoustic Sensor Networks // Sensors. – 2024. – 24. – 556. – https://doi.org/10.3390/s24020556.
24. *Rappaport T.* Wireless Communications: Principles and Practice. – Upper Saddle River, NJ: Prentice Hall, 1996. – 656 p.
25. *Thorp W.H.* Deep Sound Attenuation in the Sub and Low Kilocycle per-second Range // J. Acoust. Soc. Am. – 1965. – Vol. 38. – P. 648-654.
26. *Cui J.-H., Kong J., Gerla M., Zhou S.* The challenges of building scalable mobile underwater wireless sensor networks for aquatic applications // IEEE Network. – 2006. – Vol. 20, No. 3. – P. 12-18. – https://doi.org/10.1109/MNET.2006.1637927.
27. *Mosqueda-Arvizu C.-A., Romero-González J.-A., Córdova-Esparza D.-M., Terven J. Chaparro-Sánchez R., Rodríguez-Reséndiz J.* Logical Execution Time and Time-Division Multiple Access in Multicore Embedded Systems: A Case Study // Algorithms. – 2024. – 17. – 294. – https://doi.org/10.3390/a17070294.

REFERENCES

1. *Burov D.V., Kamennaya E.V., Shcherbinina I.A.* Lokalizatsiya i marshrutizatsiya v besprovodnykh podvodnykh setyakh, ispol'zuemykh dlya okhrany mariferm [Localization and routing in wireless underwater networks used to protect marine farms], *TDR* [Transport Business in Russia], 2017, No. 2. Available at: https://cyberleninka.ru/article/n/lokalizatsiya-i-marshrutizatsiya-v-besprovodnyh-podvodnyh-setyah-ispolzuemyh-dlya-ohrany-mariferm (accessed 26 February 2025).
2. *Gromasheva O.S., Kamennaya E.V., Leont'eva N.A., Shcherbinina I.A.* Obzor vozmozhnostey primeneniya podvodnoy akusticheskoy sensornoy seti i predlagaemykh arkhitekturnykh resheniy realizatsii [Review of the Possibilities of Using an Underwater Acoustic Sensor Network and the Proposed Architectural Implementation Solutions], *TDR* [Transport Business in Russia], 2016, No. 2. Available at: https://cyberleninka.ru/article/n/obzor-vozmozhnostey-primeneniya-podvodnoy-akusticheskoy-sensornoy-seti-i-predlagaemyh-arhitekturnyh-resheniy-realizatsii (accessed 26 February 2025).
3. *Tarik A., Azam F., Anvar M.V., Zakhur T., Muzaffar A.V.* Poslednie tendentsii v razvitii podvodnoy besprovodnoy sensornoy seti: sistematicheskiy obzor literatury [Recent trends in the development of underwater wireless sensor network: a systematic literature review], *Tr. ISP RAN* [Proceedings of ISP RAS], 2021, No. 1. Available at: https://cyberleninka.ru/article/n/poslednie-tendentsii-v-razvitii-podvodnoy-besprovodnoy-sensornoy-seti-sistematicheskiy-obzor-literatury (accessed 26 February 2025).

4. *Heinzelman W.R., Chandrakasan A. and Balakrishnan H.* Energy-efficient communication protocol for wireless microsensor networks, *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 2000,* Vol. 2, pp. 10. DOI: 10.1109/HICSS.2000.926982.
5. *Younis O. and Fahmy S.* HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks, *in IEEE Transactions on Mobile Computing,* Oct.-Dec. 2004, Vol. 3, No. 4, pp. 366-379. – DOI: 10.1109/TMC.2004.41.
6. *Sangho Yi, Junyoung Heo, Yookun Cho, Jiman Hong.* PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks, *Computer Communications,* 2007, Vol. 30, Issues 14–15, pp. 2842-2852. ISSN 0140-3664, 10.1016/j.comcom.2007.05.034.
7. *Tatarnikova T.M., Bimbetov F., & Gorina E.V.* Algoritm energoeffektivnogo vzaimodeystviya uzlov besprovodnoy sensornoy seti [Algorithm for energy-efficient interaction of wireless sensor network nodes], *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics], 2022, 22 (2), pp. 294-301.
8. *Li Qing, Qingxin Zhu, Mingwen Wang.* Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks, *Computer Communications,* 2006, Vol. 29, Issue 12, pp. 2230-2237. – ISSN 0140-3664, doi.org/10.1016/j.comcom.2006.02.017.
9. *Khan A., & Pirzada A.* Energy-Efficient Vertical Communica-tion in Underwater Wireless Sensor Networks, *International Journal of Communication Systems,* 2012, 25 (12), pp. 1585-1601.
10. *Partan J., Kurose J., & Levine B.N.* A Survey of Practical Is-sues in Underwater Networks, *ACM SIGMOBILE Mobile Computing and Communications Review,* 2006, 11 (4), pp. 23-33.
11. *Heinzelman W.B., Chandrakasan A., & Balakrishnan H.* Energy-Efficient Communication Protocol for Wireless Microsensor Networks, *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences,* 2000, pp. 1-10.
12. *Rodoplu V., & Meng T.H.* Minimum Energy Mobile Wireless Networks, *IEEE Journal on Selected Areas in Communications,* 1999, 17 (8), pp. 1333-1344.
13. *Kartik P., & Hanno T*. Probabilistic Routing in Underwater Sensor Networks: A Survey and the Way Forward, *IEEE Communications Surveys & Tutorials,* 2015, 17 (2), pp. 626-647.
14. *Evstifeeva E.A., Semeykin V.D.* Metodika vybora golovnogo klasternogo uzla v besprovodnoy sensornoy seti na osnove nechetkoy logiki [Methodology for selecting the head cluster node in a wireless sensor network based on fuzzy logic], *Vestnik AGTU. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika* [Bulletin of ASTU. Series: Management, computing engineering and informatics], 2018, No. 1. Available at: https://cyberleninka.ru/article/n/metodika-vybora-golovnogo-klasternogo-uzla-v-besprovodnoy-sensornoy-seti-na-osnove-nechetkoy-logiki (accessed 26 February 2025).
15. *Makhrov S.S.* Neyrosetevaya klasterizatsiya uzlov besprovodnoy sensornoy seti [Neural network clustering of wireless sensor network nodes], *T-Comm,* 2014, No. 6. Available at: https://cyberleninka.ru/article/n/neyrosetevaya-klasterizatsiya-uzlov-besprovodnoy-sensornoy-seti (accessed 26 February 2025).
16. *Fedorova T.A., Ryzhov V.A., Safronov K.S. et al.* Energy-Efficient and Reliable Deployment Models for Hybrid Underwater Acoustic Sensor Networks with a Mobile Gateway, *J. Marine. Sci*., 2024, Appl. 23, pp. 960-983. Available at: https://doi.org/10.1007/s11804-024-00444-z.
17. *Fedorova T.A., Ryzhov V.A., & Safronov K.S.* Ispol'zovanie gibridnoy kommunikatsionnoy arkhitektury podvodnoy besprovodnoy sensornoy seti dlya povysheniya ee vremeni zhizni i effektivnosti [Using a hybrid communication architecture of an underwater wireless sensor network to increase its lifetime and efficiency], *Informatika i avtomatizatsiya* [Computer Science and Automation], 2024, 23 (5), pp. 1532-1570.
18. *Fedorova T.A., Ryzhov V.A., Semenov N.N. et al.* Optimization of an Underwater Wireless Sensor Network Architecture with Wave Glider as a Mobile Gateway, *J. Marine. Sci*., 2022, Appl. 21, pp. 179-196. – https://doi.org/10.1007/s11804-022-00268-9.
19. *Mar M. De er, Arthur S.C. França, Debabrata Panja, Michael X. Cohen.* Characterizing neural phase-space trajectories via Principal Louvain Clustering, *Journal of Neuroscience Methods,* 2021, Vol. 362, 109313. ISSN 0165-0270, https://doi.org/10.1016/j.jneumeth.2021.109313.
20. Groshkov P.V. Avtomatizatsiya protsessa peredachi dannykh po seti. Mnozhestvennyy dostup [Automation of the process of data transmission over the network. Multiple access], *Problemy Nauki* [Problemy Nauki], 2017, No. 18 (100). Available at: https://cyberleninka.ru/article/n/avtomatizatsiya-protsessa-peredachi-dannyh-po-seti-mnozhestvennyy-dostup (accessed 26 February 2025).
21. *Bazarov Yu.I., Ismagilov M.I., Rogov A.N.* Novaya morskaya tsifrovaya svyaz' dlya e-Navigatsii [New maritime digital communication for e-Navigation], *Transport Rossiyskoy Federatsii. Zhurnal o nauke, praktike, ekonomike* [Transport of the Russian Federation. Journal of science, practice, economics], 2018, No. 3 (76). Available at: https://cyberleninka.ru/article/n/novaya-morskaya-tsifrovaya-svyaz-dlya-e-navigatsii (accessed 26 February 2025).

22. *Yi J., Tang J., Yuan F., Qiao G., Dai D.* Non-Uniform Clustering Algorithm for UWSNs Based on Energy Equalization Non-Uniform Clustering Algorithm for UWSNs Based on Energy Equalization, *Sensors,* 2023, 23, 5466. Available at: https://doi.org/10.3390/s23125466.
23. *Tian K., Zhou C., Zhang J.* Improved LEACH Protocol Based on Underwater Energy Propagation Model, Parallel Transmission, and Replication Computing for Underwater Acoustic Sensor Networks, *Sensors,* 2024, 24, 556. Available at: https://doi.org/10.3390/s24020556.
24. *Rappaport T.* Wireless Communications: Principles and Practice. Upper Saddle River, NJ: Prentice Hall, 1996, 656 p.
25. *Thorp W.H.* Deep Sound Attenuation in the Sub and Low Kilocycle per-second Range, *J. Acoust. Soc. Am*., 1965, Vol. 38, pp. 648-654.
26. *Cui J.-H., Kong J., Gerla M., Zhou S.* The challenges of building scalable mobile underwater wireless sensor networks for aquatic applications, *IEEE Network,* 2006, Vol. 20, No. 3, pp. 12-18. Available at: https://doi.org/10.1109/MNET.2006.1637927.
27. *Mosqueda-Arvizu C.-A., Romero-González J.-A., Córdova-Esparza D.-M., Terven J. Chaparro-Sánchez R., Rodríguez-Reséndiz J.* Logical Execution Time and Time-Division Multiple Access in Multicore Embedded Systems: A Case Study, *Algorithms,* 2024, 17, 294. Available at: https://doi.org/10.3390/a17070294.

Маевский Андрей Михайлович – АО НПП ПТ «Океанос»; e-mail: maevskiy_andrey@mail.ru; г. Санкт-Петербург, Россия; к.т.н.; н.с.; руководитель отдела морской робототехники СПбГМТУ.

Рыжов Владимир Александрович – СпбГМТУ; e-mail: ryzhov@smtu.ru; г. Санкт-Петербург, Россия; д.т.н.; профессор; зав. кафедрой ПМиММ.

Федорова Татьяна Александровна – СпбГМТУ; e-mail: fedorova.tan@gmail.com; г. Санкт-Петербург, Россия; к.ф.-м.н.; доцент кафедры ПМиММ.

Кожемякин Игорь Владиленович – СпбГМТУ; e-mail: 1861vp@mail.ru; г. Санкт-Петербург, Россия; начальник Управления оборонных исследований и разработок СпбГМТУ.

Буров Никита Михайлович – ГУАП; e-mail: burov.nm@yandex.ru; г. Санкт-Петербург, Россия; студент.

Maevsky Andrey Mikhailovich – “Oceanos” JSC; e-mail: maevskiy_andrey@mail.ru; Saint Petersburg, Russia; cand. of eng. sc.; researcher; head of marine department SMTU.

Ryzhov Vladimir Alexandrovich – SMTU; e-mail: ryzhov@smtu.ru; Saint Petersburg, Russia; dr. of eng. sc.; professor; head of AM&MM Department.

Fedorova Tatiana Aleksandrovna – SMTU; e-mail: fedorova.tan@gmail.com; Saint Petersburg, Russia; cand. of phys and math. sc.; associate professor of AM&MM Department.

Kozhemyakin Igor Vladilenovich – SMTU; e-mail: 1861vp@mail.ru; Saint Petersburg, Russia; head of Division Defense Research and Development.

Burov Nikita Michailovich – GUAP; e-mail: burov.nm@yandex.ru; Saint Petersburg, Russia; student.

УДК 681.1 DOI 10.18522/2311-3103-2025-3-81-90

В.П. Федосов, Аль-Мусави Висам Мохаммедтаки М. Джавад, С.В. Кучерявенко

АДАПТИВНЫЙ АЛГОРИТМ ОБРАБОТКИ ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ СИГНАЛОВ С КОДИРОВАНИЕМ РИДА-СОЛОМОНА ДЛЯ ТРЕХМЕРНОЙ МОДЕЛИ БЕСПРОВОДНОГО КАНАЛА РАДИОСВЯЗИ

Уменьшение вероятности возникновения ошибок при передаче сообщений имеет значение в спутниковых, беспроводных и космических системах связи. Уменьшение вероятности битовых ошибок в беспроводной системе связи возможно при применении кодирования отправляемых данных. Использование канального кодирования позволяет обнаружить и исправить ошибки при передаче сообщения в зашумленном канале. Целью работы является исследование влияния применения кодов Рида-Соломона и алгоритма пространственно-временной обработки сигналов в прием-

нике с использованием адаптивной антенной решетки на повышение помехоустойчивости в беспроводных системах радиосвязи. При наличии сложных путей распространения сигнала это позволяет выполнять пространственную фильтрацию в каналах с отражениями. Метод адаптации, рассматриваемый в этой статье, основан на теории векторов и собственных значений пространственной корреляционной матрицы. Для кодов Рида-Соломона результаты моделирования показывают значительное уменьшение показателей битовой ошибки за счет исправления ошибок передачи. Используя совместно адаптивные алгоритмы для систем «один вход – множественный выход» с мультиплексированием с ортогональным частотным разделением каналов (SIMO-OFDM) и систем «множественный вход – множественный выход» с мультиплексированием с ортогональным частотным разделением каналов MIMO-OFDM и код Рида-Соломона для передаваемого сообщения, достигнуто увеличение отношения сигнал/шум для фиксированного уровня битовой ошибки до значений 8 дБ и 5 дБ соответственно. Результаты показывают, что адаптивный алгоритм с одновременным применением кода Рида-Соломона может увеличить пропускную способность при одновременном значительном снижении вероятности ошибки. В условиях многопутного распространения сигнала можно утверждать, что использование адаптивных пространственно-временных алгоритмов улучшает помехоустойчивость приемной системы при обработке сигналов.

SIMO – Single Input Multiple Output; MIMO – Multiple Input – Multiple Output – MIMO; вероятность битовых ошибок BER – Bit Error Rate; OFDM – Orthogonal Frequency Division Multiplexing; многопутность; код Рида-Соломона.

V.P. Fedosov, AL-Musawi Wisam Mohammedtaqi M.Jawad, S.V. Kucheryavenko

ADAPTIVE ALGORITHM FOR PROCESSING SPATIAL-TEMPORAL SIGNALS WITH REED-SOLOMON CODING FOR A THREE-DIMENSIONAL MODEL OF A WIRELESS RADIO COMMUNICATION CHANNEL

Reducing the probability of errors in message transmission is important in satellite, wireless and space communication systems. Reducing the probability of bit errors in a wireless communication system is possible by using encoding of the data being sent. Using channel encoding allows detecting and correcting errors in message transmission in a noisy channel. The aim of the work is to study the effect of using Reed-Solomon codes and the algorithm of space-time signal processing in a receiver using an adaptive antenna array on increasing noise immunity in wireless radio communication systems. In the presence of complex signal propagation paths, this allows performing spatial filtering in channels with reflections. The adaptation method, considered in this paper, is based on the theory of vectors and eigenvalues of the spatial correlation matrix. For Reed-Solomon codes, the simulation results show a significant decrease in bit error rates due to the correction of transmission errors. By using adaptive algorithms for single-input multiple-output orthogonal frequency division multiplexing (SIMO-OFDM) and multiple-input multiple-output MIMO-OFDM systems together with the Reed-Solomon code for the transmitted message, the signal-to-noise ratio for a fixed bit error level was increased to 8 dB and 5 dB, respectively. The results show that the adaptive algorithm with simultaneous use of the Reed-Solomon code can increase the throughput while significantly reducing the error probability. Under conditions of multipath signal propagation, it can be argued that the use of adaptive space-time algorithms improves the noise immunity of the receiving system during signal processing.

SIMO – Single Input Multiple Output; MIMO – Multiple Input – Multiple Output – MIMO; BER – Bit Error Rate; OFDM – Orthogonal Frequency Division Multiplexing; multipath; Reed-Solomon code.

Введение. Коммуникация – это процесс установления соединения или связи между двумя точками информации или базовый процесс обмена информацией. Электронное оборудование, которое используется для целей коммуникации, называется системой связи. Основная цель этой системы – передавать информационный несущий сигнал от источника, расположенного в одной точке, к пользователю или получателю, расположенному в другой точке на некотором расстоянии [1, 2].

Для цифровой передачи и хранения данных, стандарт BER (Bit Error Rate – вероятность битовых ошибок) обычно используется при оценке производительности. Оценивается количество битов, принятых ошибочно по сравнению с общим количеством переданных битов Искажение данных происходит из-за шума в канале передачи. Отношение сигнал/шум (CNR – Signal to Noise Ratio) определяется мощностью сигнала по отношению к

шуму и обратно пропорционально BER. [3]. Это означает, что чем меньше результат BER, тем выше SNR и лучше качество связи. Из-за появления шума при прохождении сигнала через канал AWGN (Additive White Gaussian Noise – аддитивный белый гауссовский шум), принимаемое информационное сообщение искажается. Это изменяет исходные биты сообщения и может стать серьезной проблемой для точности и производительности цифровой системы. Поэтому методы обнаружения и исправления ошибок играют важную роль. Одним из способов преодоления ошибок при передаче является максимизация отношения сигнал/шум. Но на практике это отношение не может быть увеличено сверх возможного.

Кодирование Рида Соломона. Коды Рида-Соломона являются кодами исправления ошибок, которые используются в различных областях: от сбора данных из штрих-кодов и QR-кодов, которые мы используем в повседневной жизни, до отправки сообщений на космические аппараты. Ирвинг Рид и Гас Соломон открыли код Рида-Соломона (RS – Reed-Solomon) в 1959 [4]. С тех пор коды RS значительно способствовали усовершенствованию телекоммуникационных систем. Коды Рида-Соломона являются наиболее используемыми цифровыми кодами контроля ошибок для цифровой техники, такой как цифровой аудиодиск, системы дальней космической связи, системы с расширенным спектром, компьютерная память и контроль ошибок систем с обратной связью. Коды Рида-Соломона относятся к блочным линейным подмножествам [5, 6]. Код Рида-Соломона представляет собой матрицу RS (n, k) с символами размерностью s-бита каждый. Кодер создает n-символьное кодовое слово, собирая k символов данных по s бит каждый, а затем добавляя символы четности. Каждый s бит содержит n·k символов четности. Декодер Рида-Соломона может исправить пакеты данных длительностью до t символов в кодовом слове, где 2t = n·k. Код Рида-Соломона имеет максимальную длину кодового слова (n) при заданном размере символа s, которая равна n = 2s - 1. Например, код с 8-битными символами (s = 8) может иметь максимальную длину 255 байт. Можно сократить коды Рида-Соломона, сделав в кодере ряд символов сообщения нулевыми, не передавая их, а затем повторно вставив их в декодер. Число символов четности в кодовых словах коррелирует с количеством вычислительной мощности, необходимой для декодирования и кодирования кодов Рида-Соломона. Несмотря на то, что можно исправить значительное количество ошибок, большое значение длительности сообщения t требует большего количества вычислительной мощности, чем малое значение t [7].

Модель трехмерного канала 3GPP 3D. Модель трехмерного канала 3GPP используется для описания беспроводных каналов связи городов с плотной застройкой. Эта трехмерная геометрическая стохастическая модель описывает азимутальные и вертикальные (по углу места) направления рассеивающей среды между сектором мобильной пользовательской станцией (MS – mobile station) и стационарной базовой станцией (BS – base station) [8, 9]. Рассеивание представлено как статистическая характеристика с неопределенным местоположением. Модель характеризуется учетом путей распространения сигнала по прямой видимости (LoS – Line of Sight) и отсутствием прямой видимости (NLoS – No Line of Sight) [2, 10, 12]. Модель учитывает параметры для крупномасштабного замирания, мелкомасштабного замирания и средней потери маршрута распространения для каждого из этих случаев. Высота расположения базовой станции на конструкционной мачте и расстояние до точки разрыва в передаче сообщения влияют на вероятность нахождения в зоне прямой видимости. Место, где зона Френеля впервые нарушается между приемником и передатчиком, называется точкой разрыва [13, 14]. Место установки базовой станции имеет настройки, установленные в соответствии с местоположением и локальными условиями распространения. Параметры трехмерной модели распространения включают в себя: разброс задержки (дальности), разброс азимутального угла отправления и прибытия, разброс угла места отправления и прибытия, затухание тени и коэффициент Райса (только в сценарии LoS) [15]. Дополнительные параметры включают в себя мощности передатчиков, задержки, углы прибытия и отправления в направлениях угла места и азимута соответственно [13, 16–18]. В модели канала рассматриваются N передатчиков, каждый передающий сигнал может быть разбит на M путей передачи, в зависимости от отражающих объектов. На рис. 1 показана модель системы распространения в плоскости XYZ (азимут – угол места – задержка).

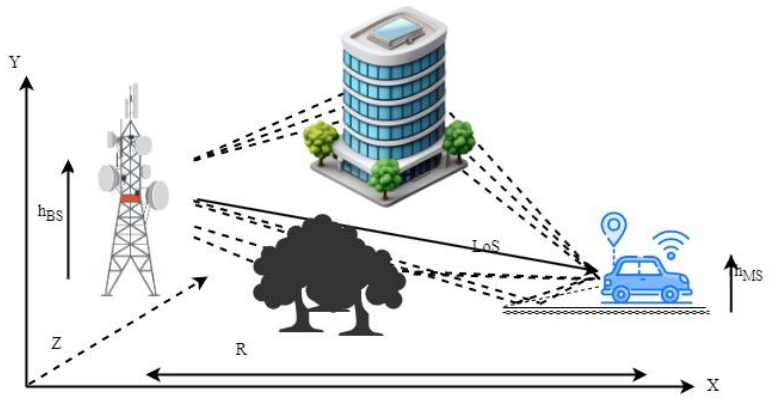


Рис. 1. Модель системы распространения в плоскости XZ

На рис. 1 расположение передающей BS (базовой станции) и приемной MS (мобильной станции) задается значениями высот h_{BS}, h_{MS} и горизонтальным расстоянием R. Показаны пути распространения в условиях прямой видимости LoS и для условий с переотражениями вне прямой видимости NLoS (на рисунке показаны штриховыми трассами).

Пространственно-временное кодирование. Пространственно-временное кодирование (STC – Spatio-temporal coding) является эффективным методом оценки пропускной способности беспроводного канала MIMO [19]. Этот метод кодирования был разработан для работы с несколькими передающими антеннами. Кодирование выполняется в пространственных и временных областях для создания корреляции между сигналами, передаваемыми различными антеннами в разное время. Не уменьшая полосу пропускания, пространственно-временное кодирование может повысить мощность передачи по сравнению с пространственно некодированными системами. Передатчик использует несколько антенн для пространственно-временного кодирования. Символы можно кодировать во времени и пространстве [19–22]. Передатчик использует несколько антенн для пространственного кодирования. Параметры N_{RX} и N_{TX} обозначают соответственно количество приемных и передающих антенн. Параметр Q определяет количество периодов, которые охватывает пространственно-временный код. Матрица C[Q x N_{TX}] используется для описания пространственно-временного кода. Каждый элемент матрицы C_k^i содержит комплексный символ основной полосы частот. Антенна посылает один сигнал или линейную комбинацию символов матрицы в течение *k*-го периода элемента *i*.

$$C = \begin{bmatrix} c_1^1 & c_2^1 & \cdots & c_{N_{TX}}^1 \\ c_1^2 & c_2^2 & & c_{N_{TX}}^2 \\ \vdots & & \ddots & \vdots \\ c_1^Q & c_2^Q & \cdots & c_{N_{TX}}^Q \end{bmatrix}. \quad (1)$$

Большинство систем пространственно-временного кодирования допускают использование нескольких приемных антенн. Дополнительные приемные антенны обеспечивают как вещательное, так и приемное разнесение за счет пространственно-временного кодирования [13, 22]. Однако преимущество приемного разнесения требует большего оборудования, поскольку приемнику требуется больше цепей обработки.

Результаты моделирования. Компьютерное моделирование было использовано для оценки эффективности предложенного метода для систем SIMO-OFDM и MIMO-OFDM и для радиоканалов с несколькими лучами. В этом разделе представлены результаты исследования производительности передачи данных WiMAX с использованием 3D-модели канала 3GPP. Принимающая и передающая антенны были настроены на текущую частоту 2,5 ГГц, чтобы обеспечить умеренное затухание сигнала для требуемого беспроводного диапазона системы WiMAX. Выбор высоты и расстояния базовой и

мобильной станций основывается на ожидаемой производительности системы связи на высоте 25 метров и расстоянии между станциями около 2 километров в городской среде с плотной застройкой. Предполагается, что базовая станция BS остается на месте, а мобильная станция MS движется с постоянной скоростью 40 км/ч. В этом исследовании будут моделироваться все узлы системы SIMO и MIMO. Моделирование можно использовать для оценки производительности отдельных узлов системы в соответствии с параметрами.

Рис. 2 и 3 показывают вероятность ошибки системы SIMO-OFDM. На рис. 2 показаны графики для случаев с адаптацией и без нее, а на рис. 3 показаны графики для случаев с кодированием и адаптацией. Методом кодирования передаваемого сообщения являются коды Рида-Соломона.

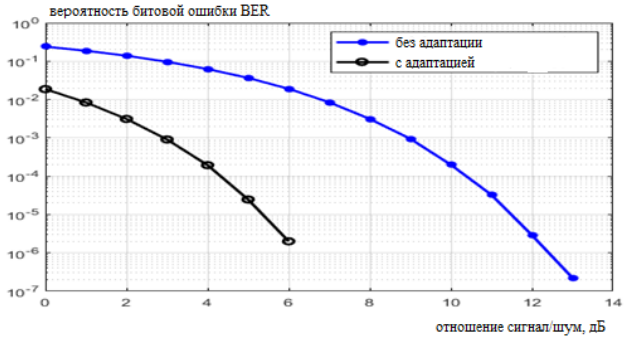


Рис. 2. Зависимость вероятности битовой ошибки для адаптивного алгоритма в системе SIMO-OFDM от отношения сигнал/шум

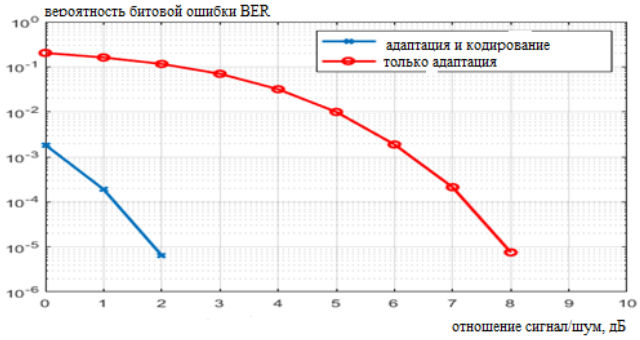


Рис. 3. Зависимость вероятности битовой ошибки для адаптивного алгоритма в системе SIMO-OFDM и кодов Рида-Соломона от отношения сигнал/шум

Анализируя графики на рис. 2, можно заметить, что при фиксированном значении битовой ошибки, например в $2 \cdot 10^{-6}$, передача сообщения для алгоритма с адаптацией возможна при отношении сигнал/шум в 6 дБ, для случая без применения данного алгоритма достичь такого показателя битовой ошибки возможно только при отношении сигнал/шум в 12 дБ.

Анализируя графики на рис. 3, можно заметить, что при фиксированном значении битовой ошибки, например в $8 \cdot 10^{-6}$, передача сообщения для алгоритма с адаптацией и кодом Рида-Соломона возможна при отношении сигнал/шум в 2 дБ, для случая без применения кодирования достичь такого показателя битовой ошибки возможно только при отношении сигнал/шум в 8 дБ.

Приведенные выше результаты показывают, что алгоритм адаптации может обеспечить помехоустойчивость до 6 дБ. Кодирование каналов может адаптивно использоваться передатчиком и приемником при изменении помеховой среды во время передачи данных по беспроводному каналу и так же улучшает помехоустойчивость передачи сообщения.

На рис. 4 показаны графики для сценария без адаптации и случая с адаптацией для системы MIMO 3x3 и частотным мультиплексированием OFDM. Для системы MIMO результаты получены при числе антенн в передатчике и приемнике, равном 3.

Анализируя графики на рис. 4, можно заметить, что при фиксированном значении битовой ошибки, например в $6 \cdot 10^{-6}$, передача сообщения для алгоритма с адаптацией возможна при отношении сигнал/шум в 24 дБ, для случая без применения данного алгоритма достичь такого показателя битовой ошибки возможно только при отношении сигнал/шум в 29 дБ.

На рис. 5 показаны графики для совместного использования системы MIMO 3x3 – OFDM и кодирования Рида-Соломона.

Анализируя графики на рис. 5, можно заметить, что при фиксированном значении битовой ошибки, например в $1 \cdot 10^{-5}$, передача сообщения для алгоритма с адаптацией и кодом Рида-Соломона возможна при отношении сигнал/шум в 20 дБ, для случая без применения кодирования достичь такого показателя битовой ошибки возможно только при отношении сигнал/шум в 25 дБ.

Таким образом, использование адаптивного метода и кодирования может привести к увеличению помехоустойчивости системы до 5 дБ.

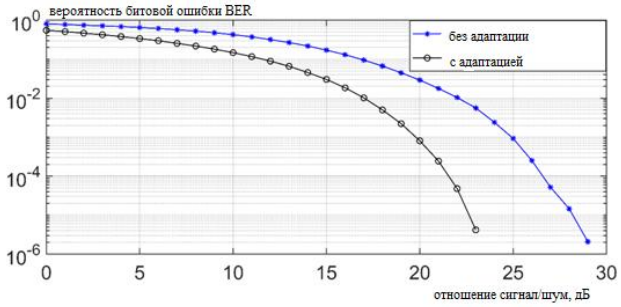


Рис. 4. Зависимость вероятности битовой ошибки для адаптивного алгоритма в системе MIMO-OFDM от отношения сигнал/шум

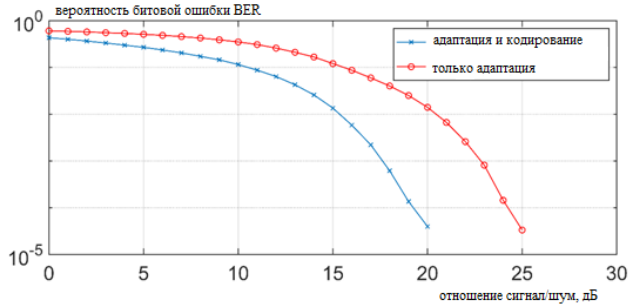


Рис. 5. Зависимость вероятности битовой ошибки для адаптивного алгоритма в системе MIMO-OFDM и кодов Рида-Соломона от отношения сигнал/шум

Применение алгоритма адаптации снижает вероятность битовой ошибки в передаваемом сообщении в системах SIMO и MIMO, как показано на рисунках 2 и 4. Можно сделать вывод, что использование адаптивных алгоритмов повышает помехоустойчивость при обработке сигналов в приемном устройстве в условиях многопутного распространения сигнала.

Заключение. Данное исследование посвящено исследованию совместного использования кодов Рида-Соломона и адаптивной системы обработки сигналов для 3D-системы, основанной на SIMO-OFDM и MIMO-OFDM. Результаты получены с использованием и без использования метода адаптации при различных уровнях отношения

сигнал/шум (SNR). Также учитываются проблемы повышения помехоустойчивости системы связи посредством использования алгоритмов адаптации в сочетании с помехоустойчивым кодированием. Использование кодирования совместно с алгоритмом адаптации делает поток информации более устойчивым к ухудшению качества передаваемой информации, вызванному шумом, помехами и затуханием сигнала. Эффективный механизм исправления ошибок включен в код Рида-Соломона. При использовании адаптивных алгоритмов для SIMO-OFDM и MIMO-OFDM код Рида-Соломона обеспечивает увеличение помехоустойчивости передачи до 6 дБ и до 5 дБ соответственно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Fedosov V., Jameel J., Kucheryavenko S.* Medical Image Transmission in 3D WiMAX Channel Using Adaptive Algorithm Based on MIMO-OFDM Principles // Conference Proceedings - 2023 Radiation and Scattering of Electromagnetic Waves, RSEMW 2023. – 2023. – P. 236-239.
2. *Fedosov V., Legin A., Lomakina A.* Adaptive algorithm for data transmission in wireless channels based on MIMO-OFDM technique // Conference Proceedings - 2017 Radiation and Scattering of Electromagnetic Waves, RSEMW 2017. – 2017. – P. 218-221.
3. *Hendrick R.E.* Signal, noise, signal-to-noise, and contrast-to-noise ratios // Breast MRI: fundamentals and technical aspects, Colorado. – 2008. – P. 93-111.
4. *Reed Irving S., Solomon G.* Polynomial Codes over Certain Finite Fields // Journal of the Society for Industrial and Applied Mathematics. Philadelphia. – 8 (2). – P. 300-304.
5. *Shrivastava P., Singh U.P.* Error detection and correction using Reed Solomon codes // International Journal of Advanced Research in Computer Science and Software Engineering. – 2013. – Vol. 3. – P. 965-969.
6. *Wicker S.B., Bhargava V.K.* An introduction to Reed-Solomon codes // Reed-Solomon codes and their applications. – 1994. – P. 1-16.
7. *Fedosov V.P., Lomakina A.V., Legin A.A., Voronin V.V.* Three-dimensional model of hydro acoustic channel for research MIMO systems // Proceedings of SPIE - The International Society for Optical Engineering. 9. Ocean Sensing and Monitoring IX. – 2017. – P. 101860W.
8. *Федосов В.П., Аль-Мусави Висам Мохаммедтаки М. Джавад.* Анализ и сравнение адаптивного алгоритма в системах SISO и MIMO для канала 3D-WiMAX в условиях функционирования беспилотных летательных средств в районе с плотной застройкой // Компьютерные и информационные технологии в науке, инженерии и управлении (КомТех-2023): Матер. Всероссийской научно-технической конференции с международным участием. Т. 1. – Таганрог, 2023. – С. 50-56.
9. *Fedosov V.P., Jameel J.S., Kucheryavenko S.V.* Analysis of an Adaptive Algorithm for Processing Space-Time Signals for Image Transmission Based on 3D Wireless Channel Model // Book Analysis of an Adaptive Algorithm for Processing Space-Time Signals for Image Transmission Based on 3D Wireless Channel Model. – IEEE, 2021. – P. 443-446.
10. *Fedosov V.P., Jameel J.S., Kucheryavenko S.V.* Theoretical Analysis of Adaptive Algorithm Modulation Scheme in 3D OFDM WiMAX System // Trends in Sciences. – 2022. – No. 19.12. – P. 4605-4605.
11. *Fedosov V., Legin A., Lomakina A.* Adaptive algorithm for wireless data transmission (including images) based on SISO system and OFDM technique // Serbian Journal of Electrical Engineering. – 2018. – Vol. 15, No. 3. – P. 353-364.
12. *Джамил Д.С.* Передача информации на основе канала MIMO-OFDM 3D WiMAX с использованием адаптивного алгоритма // Научная инициатива иностранных студентов и аспирантов. – Томск, 2021. – С. 107-112.
13. *Федосов В.П., Джамил Д.С., Кучерявенко С.В.* Передача данных в канале 3D WIMAX на основе SISO-OFDM и MIMO-OFDM // Известия ЮФУ. Технические науки. – 2020. – № 6 (216). – С. 6-18.
14. *Fedosov V., Al-Musawi W., Kucheryavenko S.* Transmission Data in 3D Channel Using Adaptive Algorithm Based on The MIMO-OFDM in a Densely Built-Up Area // in 2023 Radiation and Scattering of Electromagnetic Waves (RSEMW-2023). – 2023. – P. 240-243.
15. *Федосов В.П., Емельяненко А.В.* Сравнительная эффективность беспроводного доступа на основе пространственной адаптации на выходах антенной решетки при использовании MIMO OFDM в релеевском канале // Антенны. – 2013. – № 10 (197). – С. 045-049.
16. *Fedosov V., Jameel J., Kucheryavenko S.* Transmitting Image in 3D Wireless Channel using Adaptive Algorithm Processing with MMSE based on MIMO principles // Book Transmitting Image in 3D Wireless Channel using Adaptive Algorithm Processing with MMSE based on MIMO principles. – IOP Publishing, 2021. – P. 012131.

17. *Федосов В.П., Терновой Д.О.* Алгоритм совместной адаптации на прием и передачу в системе связи на основе антенных решеток // Радиотехника. – 2011. – № 9. – С. 52-55.
18. *Федосов В.П., Ковтун Д.Г., Легин А.А., Ломакина А.В*. Исследование модели OFDM-сигнала с малым уровнем внеполосного излучения // Известия ЮФУ. Технические науки. – 2015. – № 11 (172). – С. 6-16.
19. *Федосов В.П., Муравицкий Н.С.* Адаптивная приемная антенная решетка для обработки пространственно-временных сигналов в MIMO-системе беспроводной передачи данных // Антенны. – 2011. – № 8 (171). – С. 35-43.
20. *Федосов В.П., Джамил Д.С., Кучерявенко С.В.* Сравнение производительностей адаптивного алгоритма и метода минимума среднеквадратического отклонения для передачи изображений на основе систем связи с использованием антенных решеток // Радиотехника. – 2023. – Т. 87, № 2. – С. 69-78.
21. *Федосов В.П., Кучерявенко С.В., Муравицкий Н.С.* Повышение эффективности радиосвязи в релеевском канале на основе антенных решеток // Антенны. – 2008. – № 11 (138). – С. 98-104.
22. *Федосов В.П., Аль-Мусави Висам Мохаммедтаки М. Джавад, Кучерявенко С.В.* Пространственно-временной адаптивный алгоритм с использованием кода Хэмминга на основе модели беспроводного канала 3D-MIMO // Радиотехника. – 2024. – Т. 88, № 2. – С. 113-123.
23. *Fedosov V., Lomakina A., Legin A., Voronin V*. Modeling of systems wireless data transmission based on antenna arrays in underwater acoustic channels // Book Modeling of systems wireless data transmission based on antenna arrays in underwater acoustic channels. International Society for Optics and Photonics. – 2016. – P. 98720G.
24. *Kucheryavenko A., Fedosov V.* Model of multicomponent micro-Doppler signal in environment MATLAB // MATEC Web of Conferences. – 2017. – P. 05008.
25. *Fedosov V., Legin A*. Wireless Data Transmission in Underwater Hydroacoustic Environment Based on MIMO-OFDM System and Application Adaptive Algorithm at the Receiver Side // Serbian journal of electrical engineering. – February 2019. – Vol. 16, No. 1. – P. 71-83.

REFERENCES

1. *Fedosov V., Jameel J., Kucheryavenko S.* Medical Image Transmission in 3D WiMAX Channel Using Adaptive Algorithm Based on MIMO-OFDM Principles, *Conference Proceedings - 2023 Radiation and Scattering of Electromagnetic Waves, RSEMW 2023,* 2023, pp. 236-239.
2. *Fedosov V., Legin A., Lomakina A.* Adaptive algorithm for data transmission in wireless channels based on MIMO-OFDM technique, *Conference Proceedings - 2017 Radiation and Scattering of Electromagnetic Waves, RSEMW 2017,* 2017, pp. 218-221.
3. *Hendrick R.E.* Signal, noise, signal-to-noise, and contrast-to-noise ratios, *Breast MRI: fundamentals and technical aspects, Colorado,* 2008, pp. 93-111.
4. *Reed Irving S., Solomon G.* Polynomial Codes over Certain Finite Fields, *Journal of the Society for Industrial and Applied Mathematics. Philadelphia,* 8 (2), pp. 300-304.
5. *Shrivastava P., Singh U.P.* Error detection and correction using Reed Solomon codes, *International Journal of Advanced Research in Computer Science and Software Engineering,* 2013, Vol. 3, pp. 965-969.
6. *Wicker S.B., Bhargava V.K.* An introduction to Reed-Solomon codes, *Reed-Solomon codes and their applications,* 1994, pp. 1-16.
7. *Fedosov V.P., Lomakina A.V., Legin A.A., Voronin V.V.* Three-dimensional model of hydro acoustic channel for research MIMO systems, *Proceedings of SPIE - The International Society for Optical Engineering. 9. Ocean Sensing and Monitoring IX,* 2017, pp. 101860W.
8. *Fedosov V.P., Al'-Musavi Visam Mokhammedtaki M. Dzhavad*. Analiz i sravnenie adaptivnogo algoritma v sistemakh SISO i MIMO dlya kanala 3D-WiMAX v usloviyakh funktsionirovaniya bespilotnykh letatel'nykh sredstv v rayone s plotnoy zastroykoy [Analysis and comparison of adaptive algorithm in SISO and MIMO systems for 3D-WiMAX channel under conditions of unmanned aerial vehicles operation in densely populated areas], *Komp'yuternye i informatsionnye tekhnologii v nauke, inzhenerii i upravlenii (KomTekh-2023): Mater. Vserossiyskoy nauchno-tekhnicheskoy konferentsii s mezhdunarodnym uchastiem* [Computer and information technologies in science, engineering and management (KomTech-2023). Proceedings of the All-Russian scientific and technical conference with international participation]. Vol. 1. Taganrog, 2023, pp. 50-56.
9. *Fedosov V.P., Jameel J.S., Kucheryavenko S.V.* Analysis of an Adaptive Algorithm for Processing Space-Time Signals for Image Transmission Based on 3D Wireless Channel Model, *Book Analysis of an Adaptive Algorithm for Processing Space-Time Signals for Image Transmission Based on 3D Wireless Channel Model*. IEEE, 2021, pp. 443-446.

10. *Fedosov V.P., Jameel J.S., Kucheryavenko S.V.* Theoretical Analysis of Adaptive Algorithm Modulation Scheme in 3D OFDM WiMAX System, *Trends in Sciences,* 2022, No. 19.12, pp. 4605-4605.
11. *Fedosov V., Legin A., Lomakina A.* Adaptive algorithm for wireless data transmission (including images) based on SISO system and OFDM technique, *Serbian Journal of Electrical Engineering,* 2018, Vol. 15, No. 3, pp. 353-364.
12. *Dzhamil D.S.* Peredacha informatsii na osnove kanala MIMO-OFDM 3D WiMAX s ispol'zovaniem adaptivnogo algoritma [Information transmission based on MIMO-OFDM 3D WiMAX channel using adaptive algorithm], *Nauchnaya initsiativa inostrannykh studentov i aspirantov* [Scientific initiative of foreign students and postgraduates]. Tomsk, 2021, pp. 107-112.
13. *Fedosov V.P., Dzhamil D.S., Kucheryavenko S.V.* Peredacha dannykh v kanale 3D WIMAX na osnove SISO-OFDM i MIMO-OFDM [Data transmission in 3D WIMAX channel based on SISO-OFDM and MIMO-OFDM], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 6 (216), pp. 6-18.
14. *Fedosov V., Al-Musawi W., Kucheryavenko S.* Transmission Data in 3D Channel Using Adaptive Algorithm Based on The MIMO-OFDM in a Densely Built-Up Area, *in 2023 Radiation and Scattering of Electromagnetic Waves (RSEMW-2023),* 2023, pp. 240-243.
15. *Fedosov V.P., Emel'yanenko A.V.* Sravnitel'naya effektivnost' besprovodnogo dostupa na osnove prostranstvennoy adaptatsii na vykhodakh antennoy reshetki pri ispol'zovanii MIMO OFDM v releevskom kanale [ravnitel'naja jeffektivnost' besprovodnogo dostupa na osnove prostranstvennoj adaptacii na vyhodah antennoj reshetki pri ispol'zovanii MIMO-OFDM v releevskom kanale], *Antenny* [Antennas], 2013, No. 10 (197), pp. 045-049.
16. *Fedosov V., Jameel J., Kucheryavenko S.* Transmitting Image in 3D Wireless Channel using Adaptive Algorithm Processing with MMSE based on MIMO principles, *Book Transmitting Image in 3D Wireless Channel using Adaptive Algorithm Processing with MMSE based on MIMO principles*. IOP Publishing, 2021, pp. 012131.
17. *Fedosov V.P., Ternovoy D.O.* Algoritm sovmestnoy adaptatsii na priem i peredachu v sisteme svyazi na osnove antennykh reshetok [Algorithm for joint adaptation for reception and transmission in a communication system based on antenna arrays], *Radiotekhnika* [Journal Radioengineering], 2011, No. 9, pp. 52-55.
18. *Fedosov V.P., Kovtun D.G., Legin A.A., Lomakina A.V.* Issledovanie modeli OFDM-signala s malym urovnem vnepolosnogo izlucheniya [Study of an OFDM signal model with a low level of out-of-band radiation], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 11 (172), pp. 6-16.
19. *Fedosov V.P., Muravitskiy N.S.* Adaptivnaya priemnaya antennaya reshetka dlya obrabotki prostranstvenno-vremennykh signalov v MIMO-sisteme besprovodnoy peredachi dannykh [Adaptive receiving antenna array for processing spatio-temporal signals in a MIMO wireless data transmission system], *Antenny* [Antennas], 2011, No. 8 (171), pp. 35-43.
20. *Fedosov V.P., Dzhamil D.S., Kucheryavenko S.V.* Sravnenie proizvoditel'nostey adaptivnogo algoritma i metoda minimuma srednekvadraticheskogo otkloneniya dlya peredachi izobrazheniy na osnove sistem svyazi s ispol'zovaniem antennykh reshetok [Comparison of the performance of an adaptive algorithm and a minimum mean square deviation method for image transmission based on communication systems using antenna arrays], *Radiotekhnika* [Journal Radioengineering], 2023, Vol. 87, No. 2, pp. 69-78.
21. *Fedosov V.P., Kucheryavenko S.V., Muravitskiy N.S.* Povyshenie effektivnosti radiosvyazi v releevskom kanale na osnove antennykh reshetok [Increasing the efficiency of radio communication in the Rayleigh channel based on antenna arrays], *Antenny* [Antennas], 2008, No. 11 (138), pp. 98-104.
22. *Fedosov V.P., Al'-Musavi Visam Mokhammedtaki M. Dzhavad, Kucheryavenko S.V.* Prostranstvenno-vremennoy adaptivnyy algoritm s ispol'zovaniem koda Khemminga na osnove modeli bes-provodnogo kanala 3D-MIMO [Spatio-temporal adaptive algorithm using the Hamming code based on the 3D-MIMO wireless channel model], *Radiotekhnika* [Journal Radioengineering], 2024, Vol. 88, No. 2, pp. 113-123.
23. *Fedosov V., Lomakina A., Legin A., Voronin V*. Modeling of systems wireless data transmission based on antenna arrays in underwater acoustic channels, *Book Modeling of systems wireless data transmission based on antenna arrays in underwater acoustic channels. International Society for Optics and Photonics,* 2016, pp. 98720G.
24. *Kucheryavenko A., Fedosov V.* Model of multicomponent micro-Doppler signal in environment MATLAB, *MATEC Web of Conferences,* 2017, pp. 05008.
25. *Fedosov V., Legin A*. Wireless Data Transmission in Underwater Hydroacoustic Environment Based on MIMO-OFDM System and Application Adaptive Algorithm at the Receiver Side, *Serbian journal of electrical engineering,* February 2019, Vol. 16, No. 1, pp. 71-83.

Федосов Валентин Петрович – Южный федеральный университет; e-mail: vpfedosov@sfedu.ru; г. Таганрог, Россия; кафедра теоретических основ радиотехники; профессор.

Аль-Мусави Висам Мохаммедтаки М. Джавад – Южный федеральный университет; e-mail: almusavi@sfedu.ru; г. Таганрог, Россия; тел.: +78634371632; кафедра теоретических основ радиотехники; аспирант.

Кучерявенко Светлана Валентиновна – Южный федеральный университет; e-mail: svkucheryavenko@sfedu.ru; г. Таганрог, Россия; кафедра теоретических основ радиотехники; доцент.

Fedosov Valentin Petrovich – Southern Federal University; e-mail: vpfedosov@sfedu.ru; Taganrog, Russia; the Department of Theoretical Foundations of Radio Engineering; professor.

Al-Musawi Wisam Mohammedtaqi M. Jawad – Southern Federal University; almusavi@sfedu.ru; Taganrog, Russia; phone: +78634371632; the Department of Theoretical Foundations of Radio Engineering; postgraduate student.

Kucheryavenko Svetlana Valentinovna – Southern Federal University; e-mail: svkucheryavenko@sfedu.ru; Taganrog, Russia; the Department of Theoretical Foundations of Radio Engineering; associate professor.

Раздел III. Криптографические системы и шифрование

УДК 519.72+004 DOI 10.18522/2311-3103-2025-3-91-99

В.О. Осипян, Е.С. Фурсина, Э.Т. Альгариб

РАЗРАБОТКА АЛФАВИТНОЙ ДИСИММЕТРИЧНОЙ ТРИГРАММНОЙ КРИПТОСИСТЕМЫ НА ОСНОВЕ РЕШЕНИЯ НОРМАЛЬНОЙ СИСТЕМЫ ДИОФАНТОВЫХ УРАВНЕНИЙ 5-Й СТЕПЕНИ РАЗМЕРНОСТИ ШЕСТЬ НАД КОЛЬЦОМ ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ

Целью работы являются разработка математической модели алфавитной криптосистемы на основе общего двухпараметрического решения нормальной системы диофантовых уравнений пятой степени размерности шесть над кольцом целых гауссовых числах и написание программы, демонстрирующей возможности такой криптосистемы. В работе реализована идея К. Шеннона по разработке математической модели криптосистемы, содержащие диофантовы трудности, возникающие при решении нормальных и других многостепенных систем диофантовых уравнений (МСДУ) типа Тарри-Эскотта. К. Шенноном отмечалось, что наибольшей неопределённостью при подборе ключей обладают криптосистемы, содержащие диофантовы трудности. Особенность таких МСДУ заключается в том, что неизвестны общие непереборные методы их решения на основе отрицательного решения 10-й проблемы Гильберта об алгоритмической неразрешимости произвольного диофантова уравнения в целых числах. Отметим также, что диофантовы уравнения представляют собой мощный инструмент в криптографии благодаря своей сложности, однако их использование требует глубокого понимания математического аппарата диофантова анализа при возможных методах решений для предотвращения уязвимостей в таких криптосистемах. Решения являются ключевыми факторами для обеспечения безопасности и надежности криптографических систем, основанных на этих уравнениях. Нами предусмотрено использовать стратегии и подходы в зависимости от значений размерности и степени таких МСДУ для повышения долю стойкости алфавитных систем защиты информации, включая количество параметров, входящих в её общее параметрическое решение, с учётом либо сложности алгоритма решения системы уравнений, либо самого решения, либо и того, и другого одновременно. В работе представлена математическая модель алфавитной дисимметричной триграммной криптосистемы на основе общего двухпараметрического решения нормальной системы диофантовых уравнений пятой степени размерности шесть над кольцом целых гауссовых числах, среди числовых значений параметров которых входят и числовые эквиваленты элементарных сообщений, и ключи, для нахождения которых нелегальному пользователю потребуется поискать общее двухпараметрическое решение нормальной системы диофантовых уравнений. Математическая модель алфавитной дисимметричной триграммной криптосистемы, представленная в работе, содержит диофантовы трудности, поэтому она обладает хорошей криптостойкостью: нелегальный пользователь не сможет сократить множество перебираемых ключей, ему необходимо решить систему диофантовых уравнений в гауссовых числах, что является трудно вычислимой задачей без обладания соответствующих секретных ключей. Также использование вместо посимвольного шифрования открытого текста – трехсимвольное (триграммы) ещё больше повышает криптостойкость системы. Приводится программная реализация указанной криптосистемы средствами языка Python.

Дисимметричная криптосистема; диофантовы трудности; многостепенная система диофантовых уравнений; гауссовы числа; криптосистема на основе решения системы диофантовых уравнений; триграммные криптосистемы.

V.O. Osipyan, E.S. Fursina, E.T. Algarib

DEVELOPMENT OF ALPHABETICAL DISSYMMETRIC TRIGRAM CRYPTOSYSTEM BASED ON SOLVING A NORMAL SYSTEM OF DIOPHANTINE EQUATIONS OF THE 5TH DEGREE OF DIMENSION SIX OVER THE RING OF GAUSSIAN INTEGERS

The aim of the work is to develop a mathematical model of an alphabetic cryptosystem based on a general two-parameter solution of a normal system of Diophantine equations of the fifth degree of dimension six over the ring of Gaussian integers and to write a program demonstrating the capabilities of such a cryptosystem. The paper implements the idea of K. Shannon to develop a mathematical model of a cryptosystem containing Diophantine difficulties encountered in solving normal and other multistep systems of Diophantine equations (MSDE) of the Tarry-Escott type. K. Shannon noted that cryptosystems containing Diophantine difficulties have the greatest uncertainty in selecting keys. The peculiarity of such MSDEs is that general non-exhaustive methods for solving them based on a negative solution to Hilbert's 10th problem on the algorithmic undecidability of an arbitrary Diophantine equation in integers are unknown. It should also be noted that Diophantine equations are a powerful tool in cryptography due to their complexity, but their use requires a deep understanding of the mathematical apparatus of Diophantine analysis with possible methods of solutions to prevent vulnerabilities in such cryptosystems. Solutions are key factors for ensuring the security and reliability of cryptographic systems based on these equations. We provide for the use of strategies and approaches depending on the values of the dimension and degree of such MSDE to increase the share of resistance of alphabetic information security systems (ISS), including the number of parameters included in its general parametric solution, taking into account either the complexity of the algorithm for solving the system of equations, or the solution itself, or both at the same time. The paper presents a mathematical model of an alphabetic dissymmetric trigram cryptosystem based on a general two-parameter solution of a normal system of Diophantine equations of the fifth degree of dimension six over a ring of integer Gaussian numbers, among the numerical values of the parameters of which are both numerical equivalents of elementary messages and keys, for finding which an illegal user will need to look for a general two-parameter solution of a normal system of Diophantine equations. The mathematical model of the alphabetic dissymmetric trigram cryptosystem presented in the paper contains Diophantine difficulties, so it has good cryptographic resistance: an illegal user will not be able to reduce the set of keys being tried, he needs to solve a system of Diophantine equations in Gaussian numbers, which is a difficult-to-calculate problem without having the corresponding secret keys. Also, the use of three-symbol (trigram) encryption of plaintext instead of symbolic encryption of plaintext further increases the cryptographic resistance of the system. A software implementation of the specified cryptosystem using the Python language is provided.

Dissymmetric cryptosystem; Diophantine difficulties; multi-degree system of Diophantine equations; Gaussian numbers; cryptosystem based on solving a system of Diophantine equations; trigram cryptosystems.

Введение. С учетом развития информационных технологий стоит острая необходимость усовершенствовать алгоритмы шифрования и методы защиты конфиденциальных данных для предотвращения возможных кибератак и утечек информации. Одним из важных направлений научных исследований в этой области является поиск новых криптографических решений для повышения безопасности передачи и хранения конфиденциальной информации. Для этого необходимо повышать криптостойкость существующих криптосистем или разрабатывать новые. Как известно, задачи, содержащие диофантовы трудности, являются сложными математическими задачами. Системы защиты информации, в которых используются такие задачи, не дают возможности сократить множество перебираемых ключей [1] Такие криптосистемы обладают наибольшей неопределенностью при подборе ключей [1, 14–21].

В работе рассматривается математическая модель алфавитной дисимметричной криптосистемы (АДК). Дисимметричные криптосистемы обобщают принцип построения криптосистем с открытым ключом: в них часть одного тождества используется в качестве функции прямого преобразования исходного текста в криптотекст, а вторая часть того же тождества используется в качестве функции обратного преобразования криптотекста в исходный текст [2]. Рассматриваемая математическая модель системы защиты инфор-

мации строится на основе двухпараметрического решения нормальной системы диофантовых уравнений 5-й степени размерности шесть в гауссовых числах, взятого из монографии В.О. Осипяна «Разработка методов построения систем передачи и защиты информации» [4]. Комплексные числа, у которых целая действительная часть и целый коэффициент при мнимой части, называются гауссовыми числами [4, 5, 7, 8]. Множество комплексных чисел

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

образует кольцо: это множество замкнуто относительно сложения, вычитания и умножения. Кольцо $\mathbb{Z}[i]$ называют кольцом целых гауссовых чисел.

Математическая модель алфавитной дисимметричной криптосистемы. Нормальная система диофантовых уравнений 5-й степени размерности шесть имеет вид [3–8]:

$$X_1^k + \ ... + \ X_6^k = \ Y_1^k + \ ... \ + \ Y_6^k, \text{ k = 1. .5} \tag{1}$$

или в компактной записи:

$$X_1, \dots, X_6 \overset{5}{=} Y_1, \dots, Y_6,$$

где $X_1, \dots, X_6, Y_1, \dots, Y_6$ – целочисленные неотрицательные переменные.

Её частные решения имеют вид:

$$a_1, \dots, a_6 \overset{5}{=} b_1, , \dots, b_6, \tag{2}$$

где $a_1, \dots, a_6, b_1, \dots, b_6 \in \mathbb{Z}$.

Для некоторых нормальных систем допускается параметризация по одному или нескольким параметрам. Если (2) – частное решение (1), удовлетворяющее следующим 4-м условиям [4]:

$$\sum_{k=1}^{6} a_k b_k (a_k - b_k) = 0, \sum_{k=1}^{6} a_k b_k \left(a_k^2 - b_k^2\right) = 0,$$
$$\sum_{k=1}^{6} a_k b_k \left(a_k^3 - b_k^3\right) = 0, \sum_{k=1}^{6} a_k^2 b_k^2 (a_k - b_k) = 0,$$

то по теореме Осипяна [4] из частного решения нормальной системы диофантовых уравнений можно получить двухпараметрическое (a, b – параметры) решение этой системы в гауссовых числах:

$$\begin{gathered}(aa_1 + bb_1 i)^5 + (aa_2 + bb_2 i)^5 + (aa_3 + bb_3 i)^5 + \\ + (aa_4 + bb_4 i)^5 + (aa_5 + bb_5 i)^5 + (aa_6 + bb_6 i)^5 = \\ = (ab_1 + ba_1 i)^5 + (ab_2 + ba_2 i)^5 + (ab_3 + ba_3 i)^5 + \\ + (ab_4 + ba_4 i)^5 + (ab_5 + ba_5 i)^5 + (ab_6 + ba_6 i)^5.\end{gathered} \tag{3}$$

Таким образом, для разработки АДК мы будем использовать двухпараметрическое решение (3) нормальной системы диофантовых уравнений 5-й степени размерности шесть и наборы частных решений (2) этой системы, которые удовлетворяют вышеприведенным 4-м условиям.

Определим модель произвольной алфавитной криптосистемы в виде следующего кортежа [9–13], предложенного автором [14]:

$$\sum_0 = \langle M^*, \ Q, \ C^*, \ E(m), D(c) | \ V(E(m), D(c)) \rangle,$$

где M^*– множество всех сообщений $m = m_1 m_2 \dots m_k$ (открытых текстов) над буквенным или числовым алфавитом M, $m_1, m_2, \dots, m_k$ – это элементарные сообщения (в частности, буквы или конкатенация букв из алфавита М), на которые разбивается открытый текст m;

Q – множество всех числовых эквивалентов элементарных сообщений m_i;

C^*– множество всех криптотекстов $c = c_1 c_2 \dots c_r$ над алфавитом C;

$E(m)$ – алгоритм прямого преобразования открытого текста m;

$D(c)$ – алгоритм обратного преобразования шифртекста c;

$V(E(m), D(c))$ – связь однозначности между алгоритмами $E(m)$ и $D(c)$: это означает, что каждому элементарному сообщению m соответствует единственный криптотекст c, и наоборот.

Протокол разработки математической модели АДК.

- Выбор алфавита сообщений открытого текста.
- Установление числовых эквивалентов элементарных сообщений и триграмм.
- Выбор частного решения нормальной системы диофантовых уравнений 5-й степени размерности шесть.
- Построение двухпараметрического решения этой системы в гауссовых числах.
- Выбор функций прямого и обратного преобразования и секретного ключа.

Для разработки АДК мы используем алфавит *M*, состоящий из 26 заглавных букв английского языка, а также пробела (в общем случае *M* – алфавит мощности *u,* где *u,* в частности, может являться основанием числовой системы, например, 27-м):

$$M = \{A, B, \dots, Z, \_\}.$$

Далее, определим множество числовых эквивалентов как $Q = \{0,1, \dots 26\}$, где каждой букве алфавита *M* сопоставляется числовой эквивалент от 0 до 25 соответственно, пробелу – 26.

Разбиваем открытый текст $m = m_1 m_2 \dots m_k$ на группы из r букв (так называемые - граммы, обозначаемыми через s_i): в нашем случае $r = 3$. Если последняя группа состоит из одной или двух букв, то к ней добавляется один или два пробела соответственно.

Числовой эквивалент нового элементарного сообщения s_i – триграммы рассчитываем по следующий формуле:

$$q_i(s_i) = q_1 u^2 + q_2 u + q_3 = (q_1 q_2 q_3)_{27}, \quad (4)$$

т.е. как число в 27-м системе счисления, где q_1, q_2, q_3 – соответствующие числовые эквиваленты букв из множества Q, u – основание числовой системы, равное 27 – мощности алфавита *M*.

Используя (3), определим функцию прямого преобразования $E(m)$ для числового эквивалента элементарного сообщения s_i, равное a, в криптотекст c путем переноса слагаемых левой части в правую, кроме одного любого.

Например, так:

$$\begin{gathered} E(s_i) = (aa_1 + bb_1 i)^5 + (aa_2 + bb_2 i)^5 + (aa_3 + bb_3 i)^5 + \\ + (aa_4 + bb_4 i)^5 + (aa_5 + bb_5 i)^5 + (aa_6 + bb_6 i)^5 - \\ -(ab_2 + ba_2 i)^5 - (ab_3 + ba_3 i)^5 - (ab_4 + ba_4 i)^5 - \\ -(ab_5 + ba_5 i)^5 - (ab_6 + ba_6 i)^5 = c. \end{gathered} \quad (5)$$

Тогда функция обратного преобразования $D(c)$ криптотекста c в a соответственно будет иметь вид:

$$D(c) = (ab_1 + ba_1 i)^5 = m \quad (6)$$

$$\Rightarrow a = (\sqrt[5]{m} - a_1 bi)/b_1.$$

Теперь выберём одно частное решение нормальной системы диофантовых уравнений 5-й степени размерности шесть и соответствующее двухпараметрическое решение этой системы в гауссовых числах. Особо отметим, что это частное решение (2) является частью закрытого ключа, т.к. при различных $a_1, \dots, a_6, b_1, \dots, b_6$ получаются разные функции шифрования и дешифрования. Значения b и u также являются частью закрытого ключа K: b и u следуют выбирать достаточно большими числами и некоторым особом способом.

Таким образом, имеем функции криптографических преобразований (5) и (6) и закрытый ключ $K = (u, b, a_1, \dots a_6, b_1, \dots b_6)$.

Для получения криптотекста c вычисляем численный эквивалент a триграммы s_i по формуле (4) – к полученному численному эквиваленту триграммы a применяем (5) с секретным ключом K. В итоге получаем криптотекст c. Применяя к шифртексту c функцию (6) с секретным ключом K получаем численный эквивалент a триграммы s_i. Для получения элементарных сообщений, т.е. букв, необходимо из a получить численные эквиваленты букв q_1, q_2, q_3 по следующему алгоритму [5]:

1) $p = 3$;
2) пока $p > 1$;
3) $a \; mod \; u = q_p$;
4) $a = (a - q_p)/u, p = p - 1$, переходим к шагу 1;
5) $q_p = a$.

Полученные числовые эквиваленты букв $q_1, q_2, q_3 \in Q$ необходимо сопоставить с буквами алфавита M и находить зашифрованную триграмму s_i. Описанные действия проделываются для всех триграмм s_i открытого текста m.

Пример разработки АДК. Рассмотрим пример разработки дисимметричной криптосистемы на основе двухпараметрического решения заданной МСДУ.

Пусть для шифрования и дешифрования открытого текста мы выбрали открытый текст m = DIOPHANT, и следующее частное решение нормальной МСДУ пятой степени:

$$2, 3, 4, 6, 7, 8 \overset{5}{=} 3, 6, 2, 8, 4, 7.$$

Можно убедиться, что данное частное решение удовлетворяет всем четырём условиям, приведенным в начале работы. Следовательно, этот набор можем использовать при параметризации решения нормальный системы диофантовых уравнений пятой степени в гауссовых числах:

$$2a + 3bi, 3a + 6bi, 4a + 2bi, 6a + 8bi, 7a + 4bi, 8a + 7bi \overset{5}{=}$$
$$\overset{5}{=} 3a + 2bi, 6a + 3bi, 2a + 4bi, 8a + 6bi, 4a + 7bi, 7a + 8bi.$$

Пусть $u = 27$, а $b = 7$. На практике значения u и b необходимо выбирать, как уже было сказано выше, достаточно большими числами и некоторым особом способом.

Открытый текст m = DIOPHANT предварительно разбиваем на триграммы: DIO, PHA, NT_. Последнее элементарное сообщение состоит из двух букв, поэтому к нему добавляем пробел. Далее, вычислим числовой эквивалент для первой триграммы s_1 = DIO. Так как числовые эквиваленты букв D, I, O равны $q_1 = 3$, $q_2 = 8$ и $q_3 = 14$ соответственно, то получим значение числового эквивалента первой триграммы s_1 = DIO:

$$a = 3 * 27^2 + 8 * 27 + 14 = 2417.$$

Используя функцию прямого преобразования открытого текста (5) и секретный ключ $K = (27, 7, 2, 3, 4, 6, 7, 8, 3, 6, 2, 8, 4, 7)$ мы получим шифртекст числового эквивалента первой триграммы s_1 = *DIO*:

$$(2 * 2417 + 3 * 7 * i)^5 + (3 * 2417 + 6 * 7 * i)^5 +$$
$$+(4 * 2417 + 2 * 7 * i)^5 + (6 * 2417 + 8 * 7 * i)^5 +$$
$$+(7 * 2417 + 4 * 7 * i)^5 + (8 * 2417 + 7 * 7 * i)^5 -$$
$$-(6 * 2417 + 3 * 7 * i)^5 - (2 * 2417 + 4 * 7 * i)^5 -$$
$$-(8 * 2417 + 6 * 7 * i)^5 - (4 * 2417 + 7 * 7 * i)^5 -$$
$$-(7 * 2417 + 8 * 7 * i)^5 =$$
$$= 20043489617808458000 + 193502429678415870i = c_1$$

Полученное целое комплексное число c_1 представляет собой шифртекст первой триграммы s_1 = *DIO*.

Аналогичным образом вычисляются числовые эквиваленты для остальных триграмм: s_2 = PHA, и s_3 = NT_.

Теперь перейдём к процедуре восстановления открытого текста по полученным криптограммам триграмм. Как и выше, рассмотрим эту процедуру только для первой криптограммы. Чтобы из неё получить числовой эквивалент первой триграммы, необходимо к c_1 применить функцию обратного преобразования (6) с секретным ключом K.

Имеем:

$$(3 * a + 2 * 7 * i)^5 = 20043489617808458000 + 193502429678415870i$$

или

$$(20043489617808458000 + 193502429678415870i)^{1/5} = 7251 + 14i.$$

Решаем простое линейное диофантово уравнение в гауссовых числах, и находим a – числовой эквивалент триграммы s_1 = *DIO*. Имеем:

$$3a + 14i = 7251 + 14i, a = 2417.$$

Таким образом, получили числовой эквивалент первой триграммы $a = 2417$. Далее применяем алгоритм извлечения числовых эквивалентов букв q_1, q_2, q_3 из числового эквивалента первой триграммы:

1) $p = 3$;
2) $3 > 1 => 2417\ mod\ 27 = 14 = q_3$;
3) $a = (2417 - 14)/27 = 89, p = 3 - 1 = 2$;
4) $2 > 1 => 89\ mod\ 27 = 8 = q_2$;
5) $a = (89 - 8)/27 = 3, p = 2 - 1 = 1$;
6) $1 \not> 1 => q_1 = 3$.

Получили $q_1 = 3$, $q_2 = 8$ и $q_3 = 14$, что соответствуют буквам D, I и O первой триграммы s_1.

Таким образом, реализация протокола разработки математической модели алфавитно-дисимметричной триграммной криптосистемы позволит повысить криптостойкость существующих криптосистем при безопасной передаче и хранении конфиденциальной информации.

Программная реализация. В рамках данной программной реализации была написана программа на языке Python, которая выполняет следующие задачи.

Генерация секретного ключа K. Включает следующие подзадачи: определение значения u; выбор значения p; определение наборов $A = (a_1, \dots a_6)$ и $B = (b_1, \dots b_6)$).

Подготовка отрытого текста m. Включает следующие подзадачи: разбиение открытого текста на триграммы; сопоставление буквам открытого текста численных эквивалентов из Q; вычисление числового эквивалента каждой триграммы по формуле вычисления числового эквивалента триграммы (4).

Формирование криптотекста c. Включает следующую подзадачу: формирование криптотекста c при помощи функции прямого преобразования (5) для каждой триграммы s_i.

Извлечение открытого текста m *из криптотекста* c. Включает следующие подзадачи: вычисление из c численные эквиваленты триграмм s_i; получение из s_i численные эквиваленты букв q_1, q_2, q_3, содержащихся в триграмме; сопоставление полученных числовых эквивалентов $q_1, q_2, q_3 \in Q$ буквам алфавита M для нахождения m.

Сохранение всех полученных результатов в файлы формата txt. Включает следующие подзадачи: сохранение K в файл; сохранение c в файл; сохранение m в файл.

Главное окно программы представлено на рис. 1:

Рис. 1. Главное окно программы

Ввод и вывод отрытого текста, криптотекста и секретного ключа осуществляется с помощью файлов формата txt. Для генерации K используется кнопка 1. Для получения c загружается m (кнопка 3) и по кнопке 5 происходит преобразование m в c. Полученный c сохраняется в файл. Для извлечения m из c устанавливается соответствующий K (кнопка 2), выбирается c (кнопка 4) и по кнопке 6 происходит дешифрование c, в итоге получаем m. Полученный m сохраняется в файл. Окна 7-10 служат для вывода служебной информации (расположение файлов, подсказки, ошибки и т. д.).

Файл с полученным криптотекстом представлен на рис. 2.

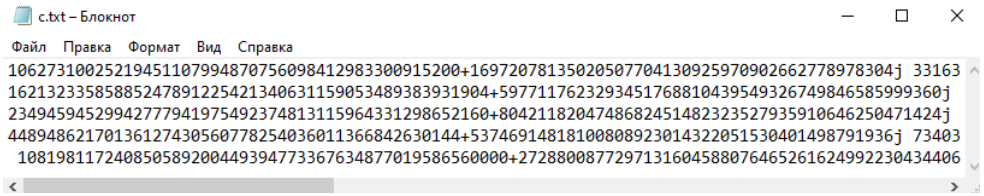


Рис. 2. Криптотекст

Логично использовать данную программную реализацию в качестве криптографического блока других программных продуктов, в которых стоит необходимость обеспечения защиты конфиденциальных данных. Данная программная реализация является учебной версией, которая демонстрирует работу описываемой криптосистемы на простых числовых данных. Соответственно функционал и интерфейс программы организован с целью продемонстрировать возможности алфавитной дисимметричной триграммной криптосистемы на основе двухпараметрического решения нормальной системы диофантовых уравнений 5-й степени размерности шесть в целых гауссовых числах.

Заключение. Сложность диофантовых уравнений, заключающаяся в поиске целочисленных решений, делает их привлекательными для шифрования данных и создания криптографических протоколов. Ключевым моментом является то, что даже зная структуру уравнения, найти конкретное решение может быть крайне затруднительно, особенно при увеличении числа переменных и степени полиномов.

Таким образом, в работе были представлены математическая модель алфавитной дисимметричной триграммной криптосистемы, на основе двухпараметрического решения нормальной системы диофантовых уравнений 5- й степени размерности шесть в гауссовых числах, и программа для шифрования данных на основе этой криптосистемы. Программа, разработанная средствами языка Python, позволяет пользователям генерировать секретный ключ, загружать файлы для шифрования или дешифрования, производить само шифрование или дешифрование и сохранять результат применения криптоалгоритмов в файл.

Данную программную реализацию криптосистемы можно использовать во многих областях, например, ее можно встроить в платежную систему для обеспечения безопасности конфиденциальных финансовых данных пользователей, онлайн-платежей, интернет-банкинга и так далее. Или, например, для защиты конфиденциальных данных непосредственно на компьютерах или серверах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. – 1949. – Vol. 28, No. 4. – P. 656-715.
2. *Осипян В.О., Литвинов К.И., Жук А.С.* Разработка математических моделей систем защиты информации на основе многостепенных систем диофантовых уравнений // Экологический вестник научных центров ЧЭС. – 2019. – Т. 16, № 3. – С. 6-15.
3. *Gloden A.* Mehrgradige Gleichungen. – P. Noordhoff: Groningen, 1944.
4. *Осипян В.О.* Разработка методов построения систем передачи и защиты информации: монография. – Краснодар: Кубан. гос. ун-т, 2004. – 180 с.
5. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел: пер. с англ. – М.: Мир, 1987. – 416 с.

6. *Фурсина Е.С., Осипян В.О.* Математическая модель дисимметричной триграммной криптосистемы на основе параметрического решения системы диофантовых уравнений 5-й степени // Матер. VI Всероссийской научно-практической конференции, молодых ученых. – 2024. – Т. 2. – С. 295-299.
7. *Яглом И.М.* Комплексные числа и их применение в геометрии. – М.: Физматгиз, 1963. – 192 с.
8. *Кузьмин Р.О., Фаддеев Д.К.* Алгебра и арифметика комплексных чисел: пособие для учителей. – М.: Учпедгиз, 1939. – 187 с.
9. *Диксон Л.Е.* История теории чисел. Т. 1. – М.: Челси, Нью-Йорк, 1952. – 486 с.
10. *Матиясевич Ю.В.* Диофантовы множества. – М.: УМН, 1972. – 222 с.
11. *Шестопал М.Г., Дорофеева А.В.* Проблемы Гильберта. – М.: Наука, 1969. – 240 с.
12. *Осипян В.О., Григорян Э.С.* Метод параметризации диофантовых уравнений и математическое моделирование систем защиты данных на их основе // Прикаспийский журнал: управление и высокие технологии. – 2019. – Н. 1. – 218 с.
13. *Левина А.Б.* Моделирование криптосистем. – СПб.: Интермедия, 2016. – 144 с.
14. *Осипян В.О.* Разработка математической модели дисимметричной биграммной криптосистемы на основе параметрического решения многостепенной системы диофантовых уравнений // Инженерный вестник Дона. – 2020. – Н. 6. – URL: ivdon.ru/ru/magazine/archive/n6y2020/6534.
15. *Болибрух А.А.* Проблемы Гильберта (100 лет спустя). – М.: МЦНМОБ, 1999. – 24 с.
16. *Болелов Э.А.* Криптографические методы защиты информации. – М.: МГТУ ГА, 2011. – 80 с.
17. *Саломаа А.* Криптография с открытым ключом. – М.: Мир, 1995. – 318 с.
18. *Смарт Н.* Криптография. – М.: Техносфера, 2005. – 528 с.
19. *Матиясевич Ю.В.* Десятая проблема Гильберта. – М.: Наука, 1993. – 12 с.
20. *Осипян В.О., Осипян К.В.* Криптография в задачах и упражнениях. – М.: Гелиос АРВ, 2004. – 144 с.
21. *Катц Д., Линдел Й.* Введение в современную криптографию. – Чэпмэн энд Холл: CRC, 2014. – 336 с.

REFERENCES

1. *Shannon C*. Communication theory of secrecy systems, *Bell System Techn. J.*, 1949, Vol. 28, No. 4, pp. 656-715.
2. *Osipyan V.O., Litvinov K.I., Zhuk A.S.* Razrabotka matematicheskikh modeley sistem zashchity informatsii na osnove mnogostepennykh sistem diofantovykh uravneniy [Development of mathematical models of information security systems based on multi-degree systems of Diophantine equations], *Ekologicheskiy vestnik nauchnykh tsentrov ChES* [Ecological Bulletin of Scientific Centers of the Black Sea Economic Cooperation], 2019, Vol. 16, No. 3, pp. 6-15.
3. *Gloden A.* Mehrgradige Gleichungen. P. Noordhoff: Groningen, 1944.
4. *Osipyan V.O.* Razrabotka metodov postroeniya sistem peredachi i zashchity informatsii: monografiya [Development of methods for constructing information transmission and protection systems: monograph]. Krasnodar: Kuban. gos. un-t, 2004, 180 p.
5. *Ayerlend K., Rouzen M.* Klassicheskoe vvedenie v sovremennuyu teoriyu chisel [Classical introduction to modern number theory]: transl. from engl. M.: Mir, 1987, 416 p.
6. *Fursina E.S., Osipyan V.O.* Matematicheskaya model' disimmetrichnoy trigrammnoy kriptosistemy na osnove parametricheskogo resheniya sistemy diofantovykh uravneniy 5-y stepeni [Mathematical model of a dissymmetric trigram cryptosystem based on a parametric solution of a system of Diophantine equations of the 5th degree], *Mater. VI Vserossiyskoy nauchno-prakticheskoy konferentsii, molodykh uchenykh* [Proceedings of the VI All-Russian scientific and practical conference of young scientists], 2024, Vol. 2, pp. 295-299.
7. *Yaglom I.M.* Kompleksnye chisla i ikh primenenie v geometrii [Complex numbers and their application in geometry]. Moscow: Fizmatgiz, 1963, 192 p.
8. *Kuz'min R.O., Faddeev D.K.* Algebra i arifmetika kompleksnykh chisel: posobie dlya uchiteley [Algebra and arithmetic of complex numbers: manual for teachers]. Moscow: Uchpedgiz, 1939, 187 p.
9. *Dikson L.E.* Istoriya teorii chisel [History of number theory]. Vol. 1. Moscow: Chelsi, N'yu-York, 1952, 486 p.
10. *Matiyasevich Yu.V.* Diofantovy mnozhestva [Diophantine sets]. Moscow: UMN, 1972, 222 p.
11. *Shestopal M.G., Dorofeeva A.V.* Problemy Gil'berta [Hilbert's Problems]. Moscow: Nauka, 1969, 240 p.
12. *Osipyan V.O., Grigoryan E.S.* Metod parametrizatsii diofantovykh uravneniy i matematicheskoe modelirovanie sistem zashchity dannykh na ikh osnove [Method of parameterization of Diophantine equations and mathematical modeling of data protection systems based on them], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2019, N. 1, 218 p.

13. *Levina A.B.* Modelirovanie kriptosistem [Modeling of cryptosystems]. Saint Petersburg: Intermediya, 2016, 144 p.
14. *Osipyan V.O.* Razrabotka matematicheskoy modeli disimmetrichnoy bigrammnoy kriptosistemy na osnove parametricheskogo resheniya mnogostepennoy sistemy diofantovykh uravneniy [Development of a mathematical model of a dissymmetric bigram cryptosystem based on a parametric solution of a multi-degree system of Diophantine equations], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2020, N. 6. Available at: ivdon.ru/ru/magazine/archive/n6y2020/6534.
15. *Bolibrukh A.A.* Problemy Gil'berta (100 let spustya) [Hilbert's problems (100 years later)]. Moscow: MTsNMOB, 1999, 24 p.
16. *Bolelov E.A.* Kriptograficheskie metody zashchity informatsii [Cryptographic methods of information protection]. Moscow: MGTU GA, 2011, 80 p.
17. *Salomaa A.* Kriptografiya s otkrytym klyuchom [Public-key cryptography]. Moscow: Mir, 1995, 318 p.
18. *Smart N.* Kriptografiya [Cryptography]. Moscow: Tekhnosfera, 2005, 528 p.
19. *Matiyasevich Yu.V.* Desyataya problema Gil'berta [Hilbert's tenth problem]. Moscow: Nauka, 1993, 12 p.
20. *Osipyan V.O., Osipyan K.V.* Kriptografiya v zadachakh i uprazhneniyakh [Cryptography in tasks and exercises]. Moscow: Gelios ARV, 2004, 144 p.
21. *Katts D., Lindel Y.* Vvedenie v sovremennuyu kriptografiyu [Introduction to modern cryptography]. Chepmen end Kholl: CRC, 2014, 336 p.

Осипян Валерий Осипович – Кубанский государственный университет; e-mail: v.osippyan@gmail.com; г. Краснодар, Россия; кафедра анализа данных и искусственного интеллекта; д.ф.-м.н.; доцент.

Фурсина Елизавета Сергеевна – ООО "БСР"; e-mail: lizafursina@gmail.com; г. Краснодар, Россия; программист 1С.

Альгариб Эман Талиб – Кубанский государственный университет; e-mail: emanalghareeb38@gmail.com; г. Краснодар, Россия; кафедра анализа данных и искусственного интеллекта; аспирант.

Osipyan Valeriy Osipovich – Kuban State University; e-mail: v.osippyan@gmail.com; Krasnodar, Russia; the Department of Data Analysis and Artificial Intelligence; dr. of phys. and math. sc.; associate professor.

Fursina Elizaveta Sergeevna – Limited Liability Partnerships "BSR"; e-mail: lizafursina@gmail.com; Krasnodar, Russia; 1C programmer.

Alghareeb Eman Talib – Kuban State University; e-mail: emanalghareeb38@gmail.com; Krasnodar, Russia; the Department of Data Analysis and Artificial Intelligence; graduate student.

УДК 004.056.55 DOI 10.18522/2311-3103-2025-3-99-110

К.С. Романенко, Е.А. Ищукова, Н.Б. Ельчанинова

ШИФРОВАНИЕ ДАННЫХ В СЭД НА ОСНОВЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ

Рассмотрены вопросы хранения конфиденциальных и персональных данных в системах электронного документооборота. Рассмотрена возможность хранения конфиденциальных и персональных данных в системах электронного документооборота на основе блокчейн технологий. Одной из ключевых характеристик блокчейна является открытость данных. Все транзакции, внесенные в блокчейн, видны всем участникам сети. Это может стать серьезной проблемой при хранении чувствительных данных, таких как личная информация, банковские реквизиты или медицинская история. В связи с этим возникает неизбежный вопрос о безопасном хранении личных данных, поскольку блокчейн-платформа является открытой. Для скрытия информации применяются различные методы, включая гомоморфное шифрование, ZK-SNARK (доказательства с нулевым разглашением), специализированные аппаратные дополнения и другие способы. Ранее авторами был представлен протокол для хранения конфиденциальных данных в блокчейн системах с использованием гибридного шифрования. В работе уделено внимание применению алгоритмов симметричной криптографии в связке с криптографией на эллиптических кривых, поскольку она широко используется в современных блокчейн-платформах, таких как Bitcoin и Ethereum. Причиной выбора эллиптических кривых являются их высокая криптографическая стойкость при относительно малой длине ключа, эффективность вычислений и низкие требования к ресурсам, что особенно важно для децентрализованных сетей с ограниченными вычислительными возможностями узлов. В статье представлены резуль-

таты по моделированию процесса формирования зашифрованных конфиденциальных данных с использованием различных алгоритмов шифрования – ECC ElGamal, ECDH-AES, ECDH-Магма (в режимах CTR и CBC). Эксперименты показали, что наиболее эффективным решением является использование гибридного алгоритма ECDH-AES с поддержкой AES-NI, обеспечивающего высокую скорость обработки данных при сохранении высокого уровня безопасности. Проведённый анализ позволяет утверждать, что применение гибридного шифрования в блокчейн-системах обеспечивает баланс между необходимостью обеспечения конфиденциальности и сохранения ключевых преимуществ технологии – децентрализации, неизменности и прозрачности для авторизованных участников. Рассмотрены возможные форматы представления данных, проведено экспериментальное сравнение различных алгоритмов шифрования, которые могут быть использованы в системах электронного документооборота на основе блокчейн технологий.

Система электронного документооборота (СЭД); конфиденциальные данные; блокчейн; шифрование; формат данных; ключ; эллиптические кривые.

K.S. Romanenko, E.A. Ishchukova, N.B. Elchaninova

DATA ENCRYPTION IN EDMS BASED ON BLOCKCHAIN TECHNOLOGIES

The article discusses the issues of storing confidential and personal data in electronic document management systems. The possibility of storing confidential and personal data in electronic document management systems based on blockchain technologies is considered. One of the key characteristics of blockchain is the openness of data. All transactions entered into the blockchain are visible to all network participants. This can become a serious problem when storing sensitive data, such as personal information, bank details or medical history. storage of personal data, since the blockchain platform is open. Various methods are used to hide information, including homomorphic encryption, ZK-SNARKs (zero-knowledge proofs), specialized hardware add-ons, and other methods. Previously, the authors presented a protocol for storing confidential data in blockchain systems using hybrid encryption. The paper focuses on the use of symmetric cryptography algorithms in conjunction with elliptic curve cryptography, as it is widely used in modern blockchain platforms such as Bitcoin and Ethereum. The reason for choosing elliptic curves is their high cryptographic strength with a relatively short key length, computational efficiency, and low resource requirements, which is especially important for decentralized networks with limited node computing capabilities. The article presents the results of modeling the process of generating encrypted confidential data using various encryption algorithms: ECC ElGamal, ECDH-AES, ECDH-Magma (in CTR and CBC modes). Experiments have shown that the most effective solution is to use the hybrid ECDH-AES algorithm with AES-NI support, which provides high data processing speed while maintaining a high level of security. The analysis suggests that the use of hybrid encryption in blockchain systems strikes a balance between the need to ensure privacy and preserve the key benefits of the technology – decentralization, immutability, and transparency for authorized participants. Possible formats of data presentation are considered, an experimental comparison of various encryption algorithms that can be used in electronic document management systems based on blockchain technologies is carried out.

Electronic document management system (EDMS); confidential data; blockchain; encryption; data format; key; elliptical curves.

Введение. Хранение личной информации в системах блокчейна сопряжено с рядом технических проблем. Системы блокчейна, особенно публичные, сталкиваются с ограничениями масштабируемости. Хранение большого количества личных данных в реестре может привести к перегрузке сети и замедлению транзакций. Решение этой проблемы требует улучшения протоколов консенсуса и архитектурных изменений.

Блокчейн изначально спроектирован для обеспечения прозрачности и целостности данных. Это может привести к проблемам с сохранением конфиденциальности личной информации. Решения по обеспечению конфиденциальности, такие как zk -SNARKs [1] и кольцевые подписи [2], могут быть сложными в реализации и требовать вычислительных ресурсов.

Известно, что данные в блокчейне неизменяемы. Это означает, что, если персональные данные были размещены в блокчейне по ошибке или с нарушением законодательства, то они не могут быть удалены или изменены без ущерба для целостности всего блокчейна. Это создает серьезные проблемы с правом на забвение и другими законными требованиями.

Управление доступом к личным данным в блокчейне может оказаться сложной задачей. Должны быть обеспечены безопасность и контроль данных для предотвращения несанкционированного доступа. В зависимости от платформы блокчейна скорость обработки транзакций может быть ограничена. Хранение больших объемов персональных данных может увеличить время и затраты на обработку транзакций [3]. Блокчейны могут подвергаться атакам, а потеря приватных ключей или атака в сети могут привести к утечке персональных данных [4].

В статье [5] обсуждается проблема хранения персональных данных на платформе блокчейна и предлагается хранить данные в форме ключ-значение, но этот подход применяется только в публичной платформе Ethereum и не рассматриваются приватные платформы, которые могут применятся в СЭД. Авторы отмечают, что предлагаемый ими подход имеет ряд ограничений, связанных с ограничением сложной обработки данных в целях экономии средств и обеспечения информационной безопасности.

В работах [5, 6] обсуждаются проблемы хранения персональных данных на платформе Ethereum. Авторы предлагают управляемую пользователем и проверяемую структуру контроля доступа для Decentralized Online Social Network (DOSN) с использованием технологии блокчейн. В предложенном авторами подходе блокчейн используется для определения политики конфиденциальности. Владелец ресурса использует открытый ключ для определения гибких политик контроля доступа на основе ролей, в то время как закрытый ключ, связанный с учетной записью Ethereum субъекта, используется для расшифровки личных данных после проверки разрешения доступа в блокчейне.

В работе [7] рассматривается проблема хранения данных и предлагается хранить данные в базе данных, развернутой на клиенте. Используемые персональные данные хранятся в автономной базе данных и при необходимости извлекаются безопасным способом и передаются пользователю или веб-сервису, имеющему право доступа к этим файлам.

На сегодняшний день одной из острых проблем в области блокчейн-технологий является обеспечение конфиденциальности данных. Поскольку большинство существующих блокчейн-систем по своей природе предполагают прозрачность и доступность информации для всех участников сети, хранение конфиденциальных данных в открытом виде в таких системах является неприемлемым. Это ограничивает возможность использования блокчейна для реализации надежных и безопасных систем электронного документооборота, где защита персональных и коммерческих данных играет ключевую роль.

В этой связи возникает необходимость разработки механизмов, которые бы позволили эффективно шифровать данные перед их записью в блокчейн, обеспечивая тем самым их конфиденциальность. При этом важно сохранить основные преимущества блокчейн-технологий – децентрализацию, неизменность и прозрачность операций для авторизованных участников. Такой механизм может стать основой для создания защищённых систем электронного документооборота, сочетающих высокий уровень безопасности с функциональностью распределённого реестра.

Ранее авторами был представлен протокол хранения персональных данных на основе использования гибридного шифрования [8]. Хранение и обмен такими данными предполагается осуществлять в зашифрованном виде. Известно, что в основе любой блокчейн-платформы лежит асимметричная криптография. Как правило, это криптография, основанная на использовании эллиптических кривых [9]. Так, например, платформы Bitcoin и Ethereum используют алгоритм ECDSA, основанный на кривой secp256k1. При этом сами блокчейн-системы никаким образом не регулируют процесс пользовательского обмена ключами или другими данными для совершения транзакций. Для оптимизации работы ранее разработанного протокола и выбора правильных параметров шифрования требуется провести эксперимент по эффективности применения различных подходов шифрования.

Авторы видят два возможных пути применения шифрования для разработанного протокола. Первый вариант заключается в использовании асимметричной криптографии на эллиптической кривой (например, алгоритма Эль-Гамаля ECC ElGamal) для шифрова-

ния небольшой порции информации, которую требуется сохранить в блокчейне. Известно, что асимметричные шифры работают медленнее симметричных и не предназначены для шифрования больших объемов данных. Но в случае, если сохраняемый в блокчейне объем данных небольшой и занимает всего 1-2 блока, такой вариант облегчает работу протокола, так как не требуется производить дополнительную выработку ключа между разными абонентами блокчейн-системы. Вторым вариантом сохранения данных в блокчейне является использование симметричного шифрования в связке с протоколом Elliptic Curve Diffie-Hellman (ECDH), т.к. данный протокол может использовать кривую secp256k1, уже используемую в блокчейн-системах. В этом случае абоненты блокчейн-сети могут использовать свои открытые и закрытые ключи для выработки общего секрета, которые впоследствии будет использоваться как ключ симметричного шифрования. Для того, чтобы сделать правильный выбор, необходимо определить потенциальный объем хранения конфиденциальных данных, а также экспериментально оценить скорость обработки этих данных с использованием различных алгоритмов.

Объем персональных данных в популярных системах электронного документооборота. Объем персональных данных, которые хранятся в системах электронного документооборота (СЭД) для одного человека, может существенно различаться в зависимости от ряда факторов. К ним относятся тип информации, которая сохраняется, структура данных, используемая в системе, а также внутренние требования и политики организации, которая управляет этими данными. В среднем, объем персональных данных на одного человека может составлять от нескольких килобайт до нескольких мегабайт.

Для более глубокого понимания того, как формируется объем персональных данных, важно детально разобрать его основные составляющие. Прежде всего, ключевым фактором является тип хранимой информации. Это могут быть как простые данные, например, фамилия, имя, отчество, дата рождения, номера телефонов или адреса электронной почты, так и более сложные материалы, такие как отсканированные копии документов, фотографии, электронные подписи, история переписки, письма и другие файлы.

Персональные данные могут включать различные типы информации, каждый из которых занимает определенный объем. Идентификационные данные, такие как ФИО, дата рождения, паспортные данные, ИНН, СНИЛС и другие, обычно хранятся в текстовых полях (VARCHAR или STRING) и занимают от 100 до 500 байт. Контактная информация, включая адрес, телефон и email, также хранится в текстовых полях и требует от 100 до 300 байт. Рабочая информация, такая как должность, отдел и история работы, занимает больше места – от 1 до 5 КБ в текстовом формате.

Биометрические данные, например фотографии или сканы документов, могут занимать от 100 КБ до 5 МБ в зависимости от качества изображения. Электронные документы, такие как трудовой договор, приказы или сканы паспорта, сохраняются в форматах PDF или других форматах и могут занимать от 100 КБ до 10 МБ, в зависимости от количества страниц и разрешения сканирования. История действий, включая логи изменений, подписей и согласований, обычно хранится в текстовом или JSON-формате и занимает от 1 до 10 КБ.

Примерный расчет объема данных для одного человека может варьироваться в зависимости от типа и количества хранимой информации. Если в системе сохраняются только основные данные, такие как ФИО, контактная информация и должность, то объем составит от 1 до 10 КБ. Это минимальный объем, который требуется для хранения базовых сведений.

Если к этим данным добавляются сканированные копии документов, например, паспорта, СНИЛС или трудового договора, то объем увеличивается до 1–10 МБ. Это средний уровень, который учитывает хранение как текстовой информации, так и файлов.

В случае, когда система хранит подробные данные, включая историю изменений, множество сканов документов и биометрические данные (например, фотографии или отпечатки пальцев), объем может достигать 10–50 МБ и более. Это максимальный объем, который требуется для хранения полного набора персональных данных с учетом всех возможных файлов и метаданных.

Системы электронного документооборота (СЭД) используют различные подходы к хранению данных, что влияет на объем информации и структуру хранения. Рассмотрим подробнее, как организовано хранение данных в популярных СЭД, включая размеры полей и особенности каждой системы.

1С:Документооборот использует реляционные базы данных, такие как PostgreSQL или Microsoft SQL Server, для хранения информации. Данные в системе делятся на текстовые поля и прикрепленные файлы. Основные поля, такие как ФИО, дата рождения, контактная информация, занимают от 100 до 500 байт каждое. Например, поле для ФИО (VARCHAR) обычно имеет ограничение в 255 символов, что соответствует 255 байтам. Дополнительные данные, такие как должность или история работы, могут занимать от 1 до 5 КБ в зависимости от объема текста. Сканы документов, фотографии и другие файлы хранятся отдельно. Размер таких файлов варьируется от 100 КБ до 10 МБ в зависимости от качества сканирования и количества страниц. Например, скан паспорта в высоком разрешении может занимать 2–3 МБ. Для одного пользователя с минимальным набором данных (текстовые поля и несколько файлов) объем может составлять 1–10 МБ. Если добавляются дополнительные документы и история изменений, объем может увеличиться до 50 МБ и более [10].

Система «ДЕЛО» от компании ЭОС (Электронные Офисные Системы) поддерживает хранение больших объемов данных, включая сканы документов и метаданные. Для оптимизации хранения система использует комбинацию реляционной базы данных и файлового хранилища. Основные поля, такие как ФИО, контактная информация и должность, занимают от 100 до 500 байт. Поля для хранения описаний документов или комментариев могут занимать до 5 КБ. Сканы документов хранятся в файловом хранилище, что позволяет экономить место в основной базе данных. Размер файлов зависит от качества сканирования: низкое разрешение занимает 100–500 КБ, а высокое разрешение – 1–5 МБ. Например, скан трудового договора в высоком разрешении может занимать 3–4 МБ. Для одного пользователя с минимальным набором данных объем составляет 1–10 МБ. Если добавляются сканы документов и история изменений, объем может достигать 10–50 МБ [11].

Диалог от компании СКБ Контур ориентирован на хранение электронных документов и их метаданных. Система активно используется для обмена юридически значимыми документами, что требует надежного хранения и быстрого доступа к информации. Основные поля, такие как ФИО, ИНН, контактная информация, занимают от 100 до 500 байт. Поля для хранения метаданных (например, дата создания документа или подпись) могут занимать до 1 КБ. Электронные документы, такие как счета-фактуры, договоры или акты, хранятся в формате PDF. Размер файлов зависит от количества страниц и разрешения: документ на 1–2 страницы занимает 100–500 КБ, а документ на 10 и более страниц – 1–5 МБ. Для одного пользователя с минимальным набором данных объем составляет 1–5 МБ. Если добавляются дополнительные документы и история изменений, объем может увеличиться до 10–20 МБ [12].

Docsvision – это гибкая система, которая поддерживает хранение данных как в реляционных базах данных, так и в файловых хранилищах. Это позволяет адаптировать систему под нужды конкретной организации. Основные поля, такие как ФИО, контактная информация и должность, занимают от 100 до 500 байт. Поля для хранения описаний документов или истории изменений могут занимать до 10 КБ. Сканы документов и другие файлы хранятся в файловом хранилище. Размер файлов зависит от их типа: сканы документов занимают 100 КБ – 5 МБ, а электронные документы (PDF) – 100 КБ – 10 МБ. Для одного пользователя с минимальным набором данных объем составляет 1–10 МБ. Если добавляются сканы документов, биометрические данные и история изменений, объем может достигать 10–50 МБ и более [13].

Формат персональных данных для использования в блокчейн. Анализ существующих систем электронного документооборота показывает, что в среднем хранение основной информации о пользователе занимает от 100 до 500 байт. В связи с тем, что мы рассматриваем хранение данных не просто в базе данных, а именно в блокчейн системе, то в рамках данного исследования мы не будем останавливаться на вопросах хранения

«тяжелых» документов, таких как сканы в виде изображений или пдф-файлов, также не будем рассматривать хранение каких-либо других форматов файлов. Остановимся только на хранении основной информации о пользователе.

На первом шаге рассмотрим какие данные мы можем собирать в блоки с учетом предполагаемого к использованию алгоритма шифрования. Особенно это важно для первого исследуемого алгоритма ECC ElGamal, для которого в рамках протокола мы хотим ограничить шифрование одним блоком данных. Для шифров AES и Магма такое распределение не является критичным, так как используемые режимы обеспечивают шифрование любых объемов данных. В отведенную размерность 512 бит или 64 байта мы можем упаковать, например, ФИО пользователя. Согласно данным переписи населения в России самая длинная фамилия содержит 20 букв, самое длинное мужское имя содержит 15 букв (Абдурахмангаджи), женское – 12 букв (Вильгельмина), а самое длинное отчество содержит 19 букв (Абдурахмангаджиевич или Абдурахмангаджиевна). Отведем под эти поля символы с запасом так, как показано на рис. 1.

Также в один блок размерности 512 бит или 64 байта можно упаковать такую информацию как СНИЛС, ИНН, паспортные данные, дату рождения и телефон. Останется еще 4 байта для хранения служебной информации. Например, для связи данной записи с другими записями пользователя.

Таким образом мы определили минимальный объем персональных данных. Который в зашифрованном виде может быть помещен в блокчейн-систему.

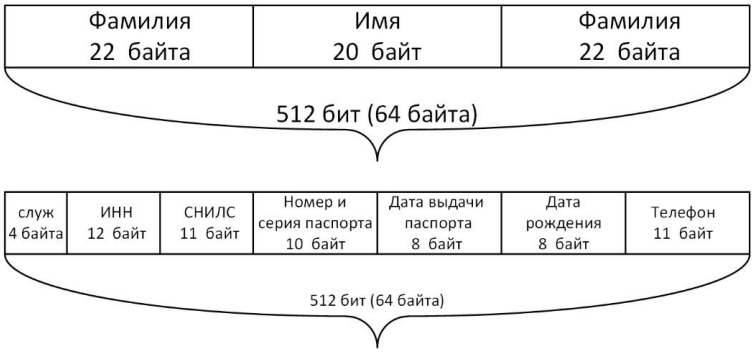


Рис. 1. Формат представления блока данных для алгоритма ECC ElGamal

Шифрование данных в блокчейн. Эллиптические кривые и асимметричная криптография на их основе играют важную роль в современных блокчейн-системах. Они обеспечивают безопасность и целостность данных, а также используются для создания цифровых подписей, аутентификации и защиты транзакций.

Эллиптическая кривая – это математический объект, который задается уравнением специального вида. В криптографии используются кривые над конечными полями, например, где значения координат точек кривой ограничены простым числом. Основное свойство эллиптических кривых, которое делает их полезными для криптографии, – это сложность задачи дискретного логарифмирования. Нахождение числа, которое связывает две точки на кривой, является вычислительно сложной задачей, что обеспечивает высокий уровень безопасности.

В блокчейн-системах, таких как Bitcoin и Ethereum, для подписи транзакций используется алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm). Этот алгоритм позволяет подтвердить, что транзакция была отправлена владельцем приватного ключа, не раскрывая сам ключ. Приватный ключ – это случайное число, выбранное из определенного диапазона, а публичный ключ – это точка на эллиптической кривой, которая вычисляется с использованием приватного ключа и базовой точки кривой. Подпись создается с использованием приватного ключа и хэша транзакции, а затем проверяется с помощью публичного ключа.

Важно отметить, что так как алгоритм ECDSA является основой публичных блокчейн систем, таких как Bitcoin и Ethereum, то все пользователи системы уже имеют пару назначенных им ключей вида открытый – закрытый ключ. Размерность ключа определяется параметрами используемой эллиптической кривой. В данном случае используется кривая вида secp256k1 и открытый ключ содержит две координаты эллиптической кривой общим объемом 512 бит. Ассиметричная криптография не предназначена для шифрования больших объемов данных. Однако мы можем попробовать рассмотреть вариант использования ассиметричных ключей алгоритма ECDSA для шифрования одного блока данных, если хранимые данные умещаются в 512 бит. Для этих целей подойдет использование алгоритма Эль-Гамаля на эллиптических кривых (ECC ElGamal). Алгоритм ECC ElGamal – это асимметричный алгоритм шифрования, адаптированный для работы с эллиптическими кривыми. В отличие от гибридных схем, он шифрует данные напрямую, используя математические операции на кривой. Для шифрования сообщение преобразуется в точку на кривой, что требует дополнительных вычислительных ресурсов.

Во всех остальных случаях, когда объем данных, предназначенных для хранения, превышает размерность ключа алгоритма ECDSA, целесообразнее использовать симметричное шифрование. При этом у пользователей должна быть возможность сформировать общий секретный ключ. Например, с использованием протокола Диффи-Хеллмана, адаптированного под использование на эллиптических кривых (ECDH, Elliptic Curve Diffie-Hellman).

Рассмотрим в качестве шифрования два основных стандарта: стандарт AES (Advanced Encryption Standard) и стандарт ГОСТ Р 34.12-2015 (Магма).

Стандарт AES представляет собой симметричный блочный шифр, основанный на алгоритме Rijndael. Будем рассматривать вариант стандарта, в котором блок данных и секретный ключ шифрования имеют длину 128 бит. Будем рассматривать применение стандарта AES в режиме CBC (Cipher Block Chaining).

Шифр Магма представляет собой симметричный блочный шифр с длиной ключа 256 бит и объемом одного шифруемого блока 64 бита. Для шифра ГОСТ Р 34.12-2015 (Магма) есть два режима, предназначенных для шифрования файлов: режим CTR (Counter) и режим CBC. Режим CTR (Counter) превращает блочный шифр в потоковый, позволяя выполнять параллельную обработку данных. Режим CBC требует, чтобы каждый блок данных зависел от предыдущего, что исключает параллельную обработку. Рассмотрим в эксперименте оба режима.

Таким образом, в настоящей работе будет проведен эксперимент для определения эффективности использования того или иного метода шифрования с использованием четырех разных подходов: ECC ElGamal, ECDH-AES, ECDH-Магма- CTR и ECDH-Магма- CBC.

Результаты экспериментов. При проведении сравнительного анализа алгоритмов шифрования для систем электронного документооборота (СЭД) на основе блокчейна важно учитывать не только криптографическую стойкость, но и скорость обработки данных различных размеров. Рассмотрим четыре алгоритма: Эль-Гамаль на эллиптических кривых ECC ElGamal, ECDH-AES, ECDH-Магма-CTR и ECDH-Магма-CBC. Три последних из них сочетают в себе асимметричные и симметричные методы, но с разными подходами к шифрованию, что влияет на производительность.

Экспериментальное сравнение алгоритмов проводилось с использованием библиотеки OpenSSL и с использованием компилятора g++ для языка программирования C++ в операционной системе Ubuntu 24.04.2 LTS (WSL). Процессор QuadCore Intel Core i5-4460, 3233 MHz (34 x 95). Оперативная память 16 ГБ (DDR3-1600 DDR3 SDRAM).

OpenSSL – это одна из наиболее известных и широко используемых библиотек с открытым исходным кодом, предназначенная для реализации криптографических функций, протоколов безопасности и работы с SSL/TLS. Она предоставляет разработчикам инструменты для защиты данных, аутентификации, шифрования и создания защищенных сетевых соединений. Библиотека написана на языках C и ассемблере, что обеспечивает высокую производительность и кроссплатформенность. OpenSSL активно применяется в веб-серверах (например, Apache, Nginx), блокчейн-системах, мобильных приложениях и IoT-устройствах [14-16].

OpenSSL включает реализацию симметричных шифров (AES, DES), асимметричных алгоритмов (RSA, ECDSA, EdDSA), хэш-функций (SHA-256, SHA-3, MD5) и алгоритмов обмена ключами (Diffie-Hellman, ECDH). Это позволяет выбирать оптимальные методы для конкретных задач, будь то шифрование данных, цифровые подписи или аутентификация [17, 18].

Распространенной практикой оценки скорости шифрования одного блока данных является многократное повторение действий по шифрованию (например, шифрование 1000 блоков) и потом получение усредненного значения. Так как разные шифры шифруют разные объемы данных, то итоговое сравнение будем делать не по скорости обработки одного блока, а по скорости обработки 64 байт информации. Для алгоритма ECC ElGamal такое преобразование займет всего один блок данных, для алгоритма ECDH-AES – 4 блока данных, а для алгоритмов ECDH-Магма-CTR и ECDH-Магма-CBC – по 8 блоков данных соответственно. Для алгоритмов, использующих протокол ECDH, выработка ключа производится однократно. После чего весь объем данных шифруется на одном и том же ключе.

В результате проведенного эксперимента, были получены временные замеры обработки информации, которые сведены в табл. 1

Таблица 1

Скорость шифрования данных

Алгоритм / Время обработки, сек	ECC+ Эль-Гамаля	ECDH-AES	ECDH-AES (AES-NI)	ECDH-Магма (CTR)	ECDH-Магма (CBC)
1024 байт	0,0370294 секунд	0,00002684 секунд	0.000002651 секунд	0,001 секунд	0,001 секунд
10240 байт	0,340882 секунд	0,000277854 секунд	0,000021231 секунд	0,001 секунд	0,001 секунд
Среднее время для обработки 1 блока	0,00116406 секунд	0,000001631 секунд	0,000000715 секунд	0,001 секунд	0,001 секунд
Среднее время для 64 байт	0,00225913 секунд	0,000003103 секунд	0,000000919 секунд	0,001 секунд	0,001 секунд

При шифровании небольших объемов данных (до 1 КБ) ECC ElGamal демонстрирует приемлемую скорость, так как операции на кривой выполняются быстро. Однако преобразование данных в точки может добавлять задержки. Для файлов размером от 1 МБ и выше производительность резко падает. Асимметричное шифрование требует значительных вычислений для каждого блока данных, что делает алгоритм непрактичным для больших объемов данных, как и предполагалось изначально. Таким образом, как и ожидалось, экспериментально подтверждено, что применение алгоритма ECC ElGamal для шифрования одного блока данных может быть использовано в блокчейн-системах без использования дополнительных надстроек криптографии.

Настройка ECDH добавляет задержку (генерация ключей и обмен), но сам AES крайне эффективен. Для документов до 1 КБ общее время шифрования сопоставимо с ECC ElGamal. AES оптимизирован для быстрой обработки крупных объемов, особенно при использовании аппаратного ускорения (например, инструкций AES-NI). Для файлов от 1 МБ ECDH-AES значительно превосходит ECC ElGamal.

Магма в режиме CTR работает быстро даже на небольших файлах, но уступает AES из-за менее оптимизированных реализаций. Для документов до 1 МБ разница между CBC и CTR не критична, но CBC всё же медленнее из-за последовательной природы.

В результате проведенного анализа можно сделать вывод, что гибридный алгоритм ECDH-AES оказался быстрее. Современные процессоры Intel (и AMD) имеют встроенные инструкции для ускорения AES, известные как AES-NI (Advanced Encryption Standard New Instructions) [19–22]. Эти инструкции позволяют выполнять операции шифрования и расшифрования AES на аппаратном уровне, что значительно ускоряет процесс по сравнению с программной реализацией.

OpenSSL активно использует аппаратные возможности процессоров, включая AES-NI. Если процессор поддерживает AES-NI, OpenSSL автоматически задействует эти инструкции для выполнения операций шифрования и дешифрования.

Заключение. В данной работе был проведен анализ возможного объема хранимой информации в системах электронного документооборота, а также проведен сравнительный анализ алгоритмов шифрования, которые могут использоваться для шифрования данных в системах электронного документооборота на основе блокчейн технологий. Следующим шагом станет детальная проработка протоколов для хранения персональных данных в системе электронного документооборота на основе блокчейн-технологий. Эта работа будет учитывать выбранную блокчейн-платформу, специфику решаемой задачи, а также предполагает использование оптимального алгоритма шифрования – в данном случае ECDH-AES-NI с поддержкой аппаратного ускорения, реализованного в библиотеке OpenSSL.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кондырев Дмитрий*. Метод обеспечения конфиденциальности данных на основе ЗК-СНАРК // Прикладная дискретная математика. Приложение. – 2021. – 14. – С. 132-134.
2. *Бендер А., Кац Дж., Морселли Р.* Кольцевые сигнатуры: более строгие опреде-ления и конструкции без случайных оракулов / Халеви С., Рабин Т. (ред.) // Теория криптографии. TCC 2006. Конспекты лекций по информатике. Т. 3876. – Springer, Берлин, Гейдельберг, 2006. – https://doi.org/10.1007/11681878_4.
3. *Зискинд Г., Натан О. и Пентланд А.* Децентрализация конфиденциальности: ис-пользование блокчейна для защиты персональных данных // Семинары IEEE по безопасности и конфиденциальности, 2015 г. Сан-Хосе, Калифорния, США, 2015 г. – С. 180-184. Номер документа: 10.1109/ SPW.2015.27.
4. *Гуггенбергер Тобиас, Шлатт Винсент, Шмид Джонатан, Нильс Урбах.* Структурированный обзор атак на системы блокчейн. – 2021. – URL: https://www.researchgate.net/publication/352960457_A_Structured_Overview_of_Attacks_on_Blockchain_Systems (дата обращения: 22.03.2025).
5. *Алдиафла И. и др.* Проектирование и реализация безопасного хранилища данных на основе смарт-контракта Ethereum // Applied Sciences. – 2023. – Vol. 13, No. 9.
6. *Рахман М., Баярди Ф., Гуиди Б., Риччи Л.* Защита персональных данных с помощью смарт-контрактов // Матер. IEEE Int. Conf. Blockchain. – 2019. – URL: https://ieeexplore.ieee.org/document/8971241 (дата обращения: 22.03.2025).
7. *Киран А., Дхараникота С. и Басава А*. Контроль доступа к данным на основе блокчейна с использованием смарт-контрактов // TENCON, конференция IEEE Region 10 (TENCON), 2019–2019 гг., Кочи, Индия, 2019 г. – С. 2335-2339. – DOI: 10.1109/TENCON.2019.8929451.
8. *Романенко К.С., Ищукова Е.А.* Алгоритм хранения приватных данных в блокчейн системах // Современные методы, средства и технологии защиты информации: Сб. трудов XV Международной научно-практической конференции имени Олега Борисовича Макаревича (Таганрог, 11–15 сентября 2024 г.). – Ростов-на-Дону; Таганрог: Изд-во ЮФУ, 2024.
9. *Ищукова Е.А., Панасенко С.П., Романенко К.С., Салманов В.Д.* Криптографические основы блокчейн-технологий. – М.: ООО "ДМК Пресс. Электронные книги", 2022. – 301 с. – ISBN 978-5-9706-0865-4.
10. 1С:Документооборот 8. – URL: https://v8.1c.ru/doc8/ (дата обращения: 22.03.2025).
11. СЭД «Дело». – URL: https://eos.ru/eos_products/eos_delo/sed-delo/ (дата обращения: 22.03.2025).
12. Контур Диадок. – URL: https://www.diadoc.ru/ (дата обращения: 22.03.2025).
13. Платформа Docsvision. – URL: https://docsvision.com/ (дата обращения: 22.03.2025).
14. *Ситников Д.С., Гайрбеков С.М.К.* Анализ возможного использования библиотеки криптографических процедур OpenSSL // Информационные технологии в науке, бизнесе и образовании. Проблемы обеспечения цифрового суверенитета государства: Матер. XIII Международной на-

учно-практической конференции студентов, аспирантов и молодых ученых, Москва, 26 ноября 2021 г. / под общ. ред. А.М. Прохорова, А.В. Царегородцева. – М.: Московский государственный лингвистический университет, 2022. – С. 85-91.
15. *Белявский Д.* Российская криптография в свободном ПО // Пятнадцатая конференция разработчиков свободных программ: Тезисы докладов. Калуга, 28–30 сентября 2018 г. / отв. ред. В.Л. Черный. – Калуга: ООО "МАКС Пресс", 2018. – С. 38-39.
16. *Никифоров А.Н., Матвеева Н.Н.* Исследование методов защиты информации с помощью криптографии // Современные информационные технологии, инновации и молодежь - «СИТИМ-2024»: Матер. Всероссийской студенческой научно-практической конференции с международным участием, Якутск, 22-23 марта 2024 г. – Ульяновск: ИП Кеньшенская Виктория Валерьевна (Изд-во "Зебра"), 2024. – С. 151-155.
17. OpenSSL. – URL: https://openssl-library.org/ (дата обращения: 22.03.2025).
18. *Гафуров И.Р.* Методы оптимизации программной реализации блочного шифра "Магма" // Ученые записки УлГУ. Серия: Математика и информационные технологии. – 2022. – № 1. – С. 8-16.
19. *Tezcan C.* Optimization of Advanced Encryption Standard on Graphics Processing Units // IEEE Access. – 2021. – Vol. 9. – P. 67315-67326. – DOI: 10.1109/ACCESS.2021.3077551.
20. *Valamehr J., Tiwari M., Sherwood T. [et al.].* Hardware assistance for trustworthy systems through 3-D integration // Proceedings - Annual Computer Security Applications Conference, ACSAC: 26th Annual Computer Security Applications Conference, ACSAC 2010, December 6–10, 2010 / sponsors: Applied Computer Security Associates (ACSA). – Austin, TX: [s.n.], 2010. – P. 199-210. – DOI: 10.1145/1920261.1920292.
21. *Лебедев Р.К.* Применение расширений процессорной архитектуры x86 для затруднения анализа программного кода // МНСК-2021: Матер. 59-й Международной научной студенческой конференции. Новосибирск, 12–23 апреля 2021 г. Новосиб. нац. исслед. гос. ун-т. – Новосибирск: Изд-во НГУ, 2021. – С. 12.
22. *Пристанскоов Е.И., Кудрявцев О.А., Андреев Д.Е. [и др.].* Анализ аппаратной поддержки криптографии при построении информационной безопасности вуза // Управление образованием: теория и практика. – 2022. – № 6 (52). – С. 126-132. – DOI: 10.25726/h2048-6130-4735-p.

REFERENCES

1. *Kondyrev Dmitriy.* Metod obespecheniya konfidentsial'nosti dannykh na osnove ZK-SNARK [A method for ensuring data confidentiality based on the ZK-SNARK], *Prikladnaya diskretnaya matematika. Prilozhenie* [Applied discrete mathematics. Appendix], 2021, 14, pp. 132-134.
2. *Bender A., Kats Dzh., Morselli R.* Kol'tsevye signatury: bolee strogie opredeleniya i konstruktsii bez sluchaynykh orakulov [Ring signatures: stricter definitions and constructions without random oracles], Khalevi S., Rabin T. (ed.), *Teoriya kriptografii. TCC 2006. Konspekty lektsiy po informatike* [Theory of cryptography. TCC 2006. Lecture Notes on Computer Science]. Vol. 3876. Springer, Berlin, Geydel'berg, 2006. Available at: https://doi.org/10.1007/11681878_4.
3. *Ziskind G., Natan O. and Pentland A.* Detsentralizatsiya konfidentsial'nosti: ispol'zovanie blokcheyna dlya zashchity personal'nykh dannykh [Decentralizing Privacy: Using Blockchain to Protect Personal Data], *Seminary IEEE po bezopasnosti i konfidentsial'nosti, 2015 g. San-Khose, Kaliforniya, SShA, 2015 g.* [IEEE Seminars on Security and Privacy, 2015, San Jose, California, USA, 2015], pp. 180-184. Document number: 10.1109/ SPW.2015.27.
4. *Guggenberger Tobias, Shlatt Vinsent, Shmid Dzhonatan, Nil's Urbakh*. Strukturirovannyy obzor atak na sistemy blokcheyn [Structured overview of attacks on blockchain systems], 2021. Available at: https://www.researchgate.net/publication/352960457_A_Structured_Overview_of_Attacks_on_Blockchain_Systems (accessed 22 March 2025).
5. *Aldiafla I., et al.* Proektirovanie i realizatsiya bezopasnogo khranilishcha dannykh na osnove smart-kontrakta Ethereum [Designing and implementing a secure data warehouse based on the Ethereum smart contract], *Applied Sciences,* 2023, Vol. 13, No. 9.
6. *Rakhman M., Bayardi F., Guidi B., Richchi L.* Zashchita personal'nykh dannykh s pomoshch'yu smart-kontraktov [Protection of personal data using smart contracts], *Mater. IEEE Int. Conf. Blockchain* [Proceedings of the IEEE Int. Conf. Blockchain], 2019. Available at: https://ieeexplore.ieee.org/document/8971241 (accessed 22 March 2025).
7. *Kiran A., Dkharanikota S. and Basava A*. Kontrol' dostupa k dannym na osnove blokcheyna s ispol'zovaniem smart-kontraktov [Blockchain-based data access control using smart contracts], *TENCON, konferentsiya IEEE Region 10 (TENCON), 2019–2019 gg., Kochi, Indiya, 2019 g*. [TENCON, IEEE Region 10 Conference (TENCON), 2019-2019, Kochi, India, 2019], pp. 2335-2339. DOI: 10.1109/TENKON.2019.8929451.

8. *Romanenko K.S., Ishchukova E.A.* Algoritm khraneniya privatnykh dannykh v blokcheyn sistemakh [Algorithm for storing private data in blockchain systems], *Sovremennye metody, sredstva i tekhnologii zashchity informatsii: Sb. trudov XV Mezhdunarodnoy nauchno-prakticheskoy konferentsii imeni Olega Borisovicha Makarevicha (Taganrog, 11–15 sentyabrya 2024 g.)* [Proceedings of the XV International Scientific and Practical Conference Named After Oleg Borisovich Makarevich (Taganrog, September 11–15, 2024)]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2024.
9. *Ishchukova E.A., Panasenko S.P., Romanenko K.S., Salmanov V.D.* Kriptograficheskie osnovy blokcheyn-tekhnologiy [Cryptographic foundations of blockchain technologies]. Moscow: OOO "DMK Press. Elektronnye knigi", 2022, 301 p. ISBN 978-5-9706-0865-4.
10. 1S:Dokumentooborot 8 [1C:Document management 8]. Available at: https://v8.1c.ru/doc8/ (accessed 22 March 2025).
11. SED «Delo» [SED "Delo"]. Available at: https://eos.ru/eos_products/eos_delo/sed-delo/ (accessed 22 March 2025).
12. Kontur Diadok [Contour of Diadems]. Available at: https://www.diadoc.ru/ (accessed 22 March 2025).
13. Platforma Docsvision [Docsvision platform]. Available at: https://docsvision.com/ (accessed 22 March 2025).
14. *Sitnikov D.S., Gayrbekov S.M.K.* Analiz vozmozhnogo ispol'zovaniya biblioteki kriptograficheskikh protsedur OpenSSL [Analysis of the possible use of the OpenSSL cryptographic procedure library], *Informatsionnye tekhnologii v nauke, biznese i obrazovanii. Problemy obespecheniya tsifrovogo suvereniteta gosudarstva: Mater. XIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh, Moskva, 26 noyabrya 2021 g.* [Information technologies in science, business and education. Problems of ensuring the digital sovereignty of the state: Proceedings of the XIII International Scientific and Practical Conference of Students, Postgraduates and Young Scientists, Moscow, November 26, 2021], under the general ed. A.M. Prokhorova, A.V. Tsaregorodtseva. Moscow: Moskovskiy gosudarstvennyy lingvisticheskiy universitet, 2022, pp. 85-91.
15. *Belyavskiy D.* Rossiyskaya kriptografiya v svobodnom PO [Russian cryptography in free software], *Pyatnadtsataya konferentsiya razrabotchikov svobodnykh programm: Tezisy dokladov. Kaluga, 28–30 sentyabrya 2018 g*. [The Fifteenth Conference of Free Software Developers : abstracts. Kaluga, September 28-30, 2018], ed. by V.L. Chernyy. Kaluga: OOO "MAKS Press", 2018. – S. 38-39.
16. *Nikiforov A.N., Matveeva N.N.* Issledovanie metodov zashchity informatsii s pomoshch'yu kriptografii [Investigation of information security methods using cryptography], *Sovremennye informatsionnye tekhnologii, innovatsii i molodezh' - «SITIM-2024»: Mater. Vserossiyskoy studencheskoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem, Yakutsk, 22-23 marta 2024 g.* [Modern information technologies, innovations and youth - SITIM-2024 : proceedings of the All-Russian Student Scientific and Practical Conference with international participation, Yakutsk, March 22-23, 2024]. Ul'yanovsk: IP Ken'shenskaya Viktoriya Valer'evna (Izd-vo "Zebra"), 2024, pp. 151-155.
17. OpenSSL. Available at: https://openssl-library.org/ (accessed 22 March 2025).
18. *Gafurov I.R.* Metody optimizatsii programmnoy realizatsii blochnogo shifra "Magma" [Methods of optimizing the software implementation of the block cipher "Magma"], *Uchenye zapiski UlGU. Seriya: Matematika i informatsionnye tekhnologii* [Scientific notes of the USU. Series: Mathematics and Information Technology], 2022, No. 1, pp. 8-16.
19. *Tezcan C.* Optimization of Advanced Encryption Standard on Graphics Processing Units, *IEEE Access,* 2021, Vol. 9, pp. 67315-67326. DOI: 10.1109/ACCESS.2021.3077551.
20. *Valamehr J., Tiwari M., Sherwood T. [et al.].* Hardware assistance for trustworthy systems through 3-D integration, *Proceedings - Annual Computer Security Applications Conference, ACSAC: 26th Annual Computer Security Applications Conference, ACSAC 2010, December 6–10, 2010 / sponsors: Applied Computer Security Associates (ACSA)*. Austin, TX: [s.n.], 2010, pp. 199-210. DOI: 10.1145/1920261.1920292.
21. *Lebedev R.K.* Primenenie rasshireniy protsessornoy arkhitektury x86 dlya zatrudneniya analiza programmnogo koda [The use of extensions of the x86 processor architecture to complicate the analysis of program code], *MNSK-2021: Mater. 59-y Mezhdunarodnoy nauchnoy studencheskoy konferentsii. Novosibirsk, 12–23 aprelya 2021 g.* [MNSK-2021: Proceedings of the 59th International Scientific Student Conference. Novosibirsk, April 12-23, 2021]. *Novosib. nats. issled. gos. un-t*. Novosibirsk: Izd-vo NGU, 2021, pp. 12.
22. *Pristanskov E.I., Kudryavtsev O.A., Andreev D.E. [et al.].* Analiz apparatnoy podderzhki kriptografii pri postroenii informatsionnoy bezopasnosti vuza [Analysis of hardware support for cryptography in building information security of a university], *Upravlenie obrazovaniem: teoriya i praktika* [Education Management: Theory and Practice], 2022, No. 6 (52), pp. 126-132. DOI: 10.25726/h2048-6130-4735-p.

Романенко Кирилл Сергеевич – Южный федеральный университет; e-mail: kirromanenko@sfedu.ru; г. Таганрог, Россия; тел.: +79885190125; кафедра безопасности информационных технологий им. Макаревича О.Б.; ассистент.

Ищукова Евгения Александровна – Южный федеральный университет; e-mail: uaishukova@sfedu.ru; г. Таганрог, Россия; тел.: +79281435898; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Ельчанинова Наталья Борисовна – Южный федеральный университет; e-mail: inf_2012@mail.ru; г. Таганрог, Россия; тел.: +79185000495; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Romanenko Kirill Sergeevich – Southern Federal University; e-mail: kirromanenko@sfedu.ru; phone: +79885190125; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; assistant.

Ishchukova Evgeniya Aleksandrovna – Southern Federal University; e-mail: uaishukova@sfedu.ru; phone: +79281435898; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

Elchaninova Nataliya Borisovna – Southern Federal University; e-mail: inf_2012@mail.ru; phone: +79185000495; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

УДК 004.056.55 DOI 10.18522/2311-3103-2025-3-110-118

В.С. Стародубцев, Л.К. Бабенко, Н.Б. Ельчанинова

ОЦЕНКА ВРЕМЕНИ ВЫПОЛНЕНИЯ ПОИСКА СОСТАВЛЯЮЩИХ КЛЮЧА В АТАКЕ С ИЗВЕСТНЫМ ОТКРЫТЫМ ТЕКСТОМ НА КРИПТОСИСТЕМУ ДОМИНГО-ФЕРРЕРА

Представлено краткое описание полностью гомоморфной криптографической системы Доминго-Феррера, приводится характеристика этапов атаки с известным открытым текстом на данную криптосистему. Анализируется этап поиска составляющих ключа рассматриваемой атаки, для которого описываются существующие методы реализации, среди которых определяется метод, обладающий минимальной вычислительной сложностью. Обоснование вычислительной сложности и временных затрат рассматриваемого метода реализации этапа поиска составляющих ключа формируется на основе теоретических расчётов, а также экспериментальных исследований. Целью исследования является оценка сложности реализации этапа поиска составляющих ключа в атаке с известным открытым текстом на полностью гомоморфную криптографическую систему Доминго-Феррера с помощью метода Гаусса, разработанного для решения систем линейных алгебраических уравнений по модулю простого числа. Основным результатом настоящей работы является оценка вычислительной сложности этапа поиска составляющих ключа в атаке с известным открытым текстом на криптографическую систему Доминго-Феррера, реализованного с использованием метода Гаусса. Оценка сложности выражена в количестве базовых математических операций и подтверждена рядом экспериментальных исследований, что позволяет сделать обоснованные выводы о вычислительной сложности рассматриваемого метода. Проведенное исследование представляет собой значимый вклад в развитие полностью гомоморфной криптосистемы Доминго-Феррера, основанной на задаче факторизации целых чисел. Оно обладает практической значимостью, так как позволяет оценить критичность атаки с известным открытым текстом на данную криптосистему. Полученные результаты могут служить основой для исследователей и криптографов при разработке рекомендаций по выбору параметров криптосистемы Доминго-Феррера для обеспечения необходимого уровня безопасности в различных приложениях.

Информационная безопасность; гомоморфное шифрование; гомоморфная схема шифрования; полностью гомоморфное шифрование; криптосистема Доминго-Феррера; криптоанализ.

V.S. Starodubcev, L.K. Babenko, N.B. Yelchaninova

ESTIMATION OF THE SEARCH TIME FOR KEY COMPONENTS IN A KNOWN PLAINTEXT ATTACK ON THE DOMINGO-FERRER CRYPTOSYSTEM

This paper provides a brief description of the fully homomorphic Domingo-Ferrer cryptographic system and describes the stages of an attack with a known plaintext on this cryptosystem. The stage of searching for the key components of the attack in question is analyzed, for which existing implementation methods are described, among which the method with minimal computational complexity is determined. The rationale for the computational complexity and time costs of the considered method for implementing the key component search stage is based on theoretical calculations, as well as experimental studies. The aim of the study is to evaluate the complexity of implementing the stage of searching for key components in an attack with a known plaintext on a fully homomorphic Domingo-Ferrer cryptographic system using the Gauss method, developed for solving systems of linear algebraic equations modulo a prime number. The main result of this work is an assessment of the computational complexity of the key component search stage in a known plaintext attack on the Domingo-Ferrer cryptographic system, implemented using the Gauss method. The complexity estimate is expressed in the number of basic mathematical operations and is confirmed by a number of experimental studies, which allows us to draw reasonable conclusions about the computational complexity of the method under consideration. The conducted research represents a significant contribution to the development of a fully homomorphic Domingo-Ferrer cryptosystem based on the integer factorization problem. It has practical significance, as it allows us to assess the criticality of an attack with a known plaintext on a given cryptosystem. The results obtained can serve as a basis for researchers and cryptographers to develop recommendations for choosing the parameters of the Domingo-Ferrer cryptosystem to ensure the necessary level of security in various applications.

Information security; homomorphic encryption; homomorphic encryption scheme; fully homomorphic encryption; Domingo-Ferrer cryptosystem; cryptanalysis.

Введение. В настоящее время облачные вычисления получили широкое распространение, что обусловлено их преимуществами в области обработки и хранения данных [1]. Однако, несмотря на указанные достоинства, существует критический недостаток данной технологии: данные, подлежащие обработке, должны быть представлены в открытом виде. Это создает серьезные проблемы в тех областях, где конфиденциальность информации имеет первостепенное значение и где публикация данных в недоверенной среде является неприемлемой.

Традиционным решением данной проблемы является использование гомоморфного шифрования, которое позволяет выполнять операции над зашифрованными данными без необходимости их предварительной расшифровки [2]. Первая стойкая полностью гомоморфная криптографическая система была представлена в 2009 году Крейгом Джентри [3]. Эта система основана на идеальных решетках и использует добавление небольшого значения шума в шифртексты [4].

В дальнейшем было предложено множество гомоморфных криптосистем, основанных на концепциях, выдвинутых Джентри, которые получили название «криптосистемы типа Джентри» [5]. Эти схемы имеют доказанную высокую криптографическую стойкость, но обладают высокой вычислительной сложностью выполнения гомоморфных операций [6], что значительно ограничивает их практическое применение.

В качестве альтернативы криптосистемам типа Джентри были разработаны различные схемы, обладающие значительно меньшей вычислительной сложностью [7–10]. Однако, эти криптосистемы не получили широкого распространения, их криптографическая стойкость и вычислительная сложность операций недостаточно оценены. В данной работе рассматривается основанная на задаче факторизации чисел криптосистема Доминго-Феррера [8]. Задача факторизации чисел всегда считалась эталоном вычислительной сложности в криптографических задачах [11, 12], что позволяет предполагать, что исследование стойкости криптосистемы Доминго-Феррера может быть перспективным для оценки возможностей её практического применения.

В статье [13] приводится описание атаки с известным открытым текстом на криптосистему Доминго-Феррера, требующей наличия пар (открытый текст – шифртекст) на 1 больше, чем степень полиномов представления шифртекста (d). В работе [14] предложе-

на модификация атаки с известным открытым текстом (known-plaintext attack), позволяющая сократить количество необходимых пар (открытый текст – шифртекст) до 2. Поскольку для криптосистемы Доминго-Феррера актуальна атака с известным открытым текстом, необходимо рассмотреть вычислительную сложность практической реализации данной атаки.

Описание криптосистемы Доминго-Феррера. Данная криптосистема поддерживает гомоморфные операции, включая сложение, вычитание и умножение [8]. Шифр Доминго-Феррера относится к классу симметричных криптосистем, поскольку для процессов шифрования и расшифрования используется один и тот же ключ [15]. Важно отметить, что данная криптосистема не имеет ограничений на количество последовательных гомоморфных операций, что, несомненно, является её значительным преимуществом перед криптосистемами типа Джентри. Но необходимо учитывать, что размер итоговых шифртекстов при выполнении этих операций увеличивается: в частности, при проведении операций умножения наблюдается экспоненциальный рост объёма шифртекстов. Для инициализации криптосистемы Доминго-Феррера используется следующий набор параметров:

- p и q – большие простые числа;
- $n = p \times q$ – труднофакторизуемое число;
- d – степень полиномов представления шифртекстов.

Алгоритмы, выполняющие генерацию ключа, а также процессы шифрования и расшифрования в криптосистеме Доминго-Феррера, представлены на рис. 1.

Рис. 1. Описание алгоритмов операций шифра Доминго-Феррера

Атака с известным открытым текстом на криптосистему Доминго-Феррера. В работе [14] представлена атака с известным открытым текстом на криптографическую систему Доминго-Феррера. Для успешной реализации данной атаки противнику необходимо обладать по крайней мере d парами (открытый текст – шифртекст), созданными на одном ключе, где d – степень полинома представления шифртекста.

Атака с известным открытым текстом является двухэтапной. На первом этапе происходит факторизация числа n, на втором – выполняется поиск составных частей ключа (r_p, r_q).

Раскрытие факторизации числа n осуществляется путём вычисления наибольшего общего делителя (НОД) этого числа и результанта A двух полиномов, составленных из значений открытых текстов (m_1, m_2) и первой части шифртекстов $(\pi(x)_1, \pi(x)_2)$, как показано в формуле (1).

$$A = Res(\pi(x)_1 - m_1, \pi(x)_2 - m_2), \quad (1)$$

где Res – функция поиска результанта полиномов.

Число n известно, поэтому первая его составляющая (p) вычисляется по формуле (2), а значение q определяется, как частное от деления n на p.

$$p = \text{НОД}(A, n). \tag{2}$$

На втором этапе атаки происходит поиск частей ключа (r_p, r_q) путём решения двух систем линейных алгебраических уравнений (СЛАУ) по соответствующим модулям (p, q). Из значений открытых текстов $m_1 \ldots m_d$ и первой части шифртекстов $\pi(x)_1 \ldots \pi(x)_d$ формируется матрица B по формуле (3).

$$B \equiv \begin{pmatrix} -m_1 & y_{11} & y_{12} & \cdots & y_{1d} \\ -m_2 & y_{21} & y_{22} & \cdots & y_{2d} \\ & & & \vdots & \\ -m_d & y_{d1} & y_{d2} & \cdots & y_{dd} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} mod\ p, \tag{3}$$

где $m_1 \ldots m_d$ – открытые тексты, y – коэффициент многочлена соответствующей степени первой части шифртекстов $\pi(x)_1 \ldots \pi(x)_d$.

Важно отметить, что полученная матрица B является СЛАУ по модулю p. Переменные, входящие в матрицы не являются независимыми друг от друга, представляют собой мультипликативные обратные значения первой части ключа ${r_p}^{-1}$ по модулю p, возведённые в степени, соответствующие их позициям в уравнениях. Рассмотрим решение СЛАУ методом Гаусса.

Значение первой части ключа r_p вычисляется по формуле (4), как мультипликативное обратное по модулю p решения системы линейных уравнений t, представленных матрицей B.

$$r_p = t^{-1} mod\ p. \tag{4}$$

Значение второй части ключа r_q вычисляется аналогичным образом по формулам (3) и (4), за исключением того, что значения коэффициентов y в матрице B выбираются, как коэффициенты соответствующей степени второй части шифртекста $\rho(x)$.

Решение СЛАУ по модулю простого числа. При реализации атаки с известным открытым текстом возникает необходимость поиска решения СЛАУ по модулю. Итерационные методы [16] неприменимы для поиска решения подобных СЛАУ, по причине отсутствия у таких СЛАУ свойства диагонального преобладания [17], поэтому при выполнении атаки с известным открытым текстом для поиска решения рассматриваемой СЛАУ необходимо применять прямые (численные) методы. Одним из простых прямых методов поиска решения СЛАУ, обладающим низкой вычислительной сложностью, является метод Гаусса [18].

При поиске решения СЛАУ по модулю классический метод Гаусса имеет следующие особенности. В силу свойств СЛАУ, составляющие её переменные не являются независимыми друг от друга, а по сути являются одной переменной, возведенной по модулю в степень, соответствующую её позиции в уравнении. Иными словами, СЛАУ состоит из набора уравнений от одной переменной. Следовательно, единственным решением подобной СЛАУ является значение только одной переменной со степенью 1. Тогда в процессе решения СЛАУ методом Гаусса достаточно получить только одну строку с ненулевым коэффициентом переменной со степенью 1. Это означает, что на этапе обратного хода метода Гаусса нужно выполнить всего 1 шаг, что существенно сокращает время выполнения алгоритма.

Однако, наряду с описанным упрощением обратного хода метода Гаусса, вытекающим из свойств решаемых им СЛАУ, также требуются и некоторые изменения, увеличивающие количество выполняемых операций. Исходя из того, что поиск решения СЛАУ выполняется по модулю, после всех математических операций требуется дополнительная операция получения остатка от деления. Кроме того, на этапе прямого хода метода Гаусса необходимо выполнить обнуление некоторых элементов для приведения матрицы к верхнему треугольному виду. В классическом виде обнуление элемента матрицы a_{ij} происходит путём вычитания элементов строки матрицы a_k из элементов строки a_i, ум-

ноженных на коэффициент, вычисляемый как частное от деления a_{ij} на a_{kj}, где i – номер строки, j – номер столбца, k – номер выбранной строки, используемой для обнуления элемента a_{ij}. В случае, когда все операции выполняются в кольце по модулю p, операция деления (a_{ij}/a_{kj}) заменяется умножением $a_{ij} \times (a_{kj})^{-1} mod\ p$, где $(a_{kj})^{-1}$ – мультипликативное обратное a_{kj} по модулю p. Следовательно, для каждого обнуляемого элемента матрицы a_{ij} требуется одна операция поиска мультипликативного обратного с помощью расширенного алгоритма Евклида [19].

Оценка временной сложности метода Гаусса для поиска решения СЛАУ по модулю. На этапе прямого хода матрица приводится к верхнему треугольному виду, при этом первая строка матрицы остается без изменений, во второй обнуляется первый элемент, и в каждой последующей обнуляется на один элемент больше, чем в предыдущей. Следовательно, число шагов $StepCount$ прямого хода метода Гаусса определяется формулой (5).

$$StepCount = \sum_{i=1}^{d-1} i = \frac{d^2-d}{2}, \quad (5)$$

где d – размер системы линейных алгебраических уравнений.

Далее рассматривается сложность одного шага прямого хода метода Гаусса для поиска для решения СЛАУ по модулю. В первую очередь определяется подходящая строка a_k для обнуления элемента a_{ij}. После того, как подходящая строка a_k для обнуления элемента a_{ij} определена, необходимо найти коэффициент M, на который её элементы будут умножены, чтобы после вычитания строк получить $a_{ij} = 0$. Коэффициент M определяется по формуле (6).

$$M = a_{ij} \times (a_{kj})^{-1} mod\ p, \quad (6)$$

где i – номер строки, j – номер столбца, k – номер найденной строки для обнуления элемента a_{ij}, p – значение первой составляющей модуля, определенное в параметрах криптосистемы.

Из формулы (6) видно, что при поиске коэффициента M выполняется 1 операция умножения, 1 операция получения остатка от деления и 1 получение мультипликативного обратного с помощью расширенного алгоритма Евклида.

Количество шагов расширенного алгоритма Евклида зависит от чисел, которые поступают на вход. В контексте выполняемой задачи данные числа – случайные, поэтому заранее точно определить требуемое число шагов расширенного алгоритма Евклида невозможно. Однако, зная значение модуля p, согласно теореме Ламе, формулируемую как «число делений с остатком в процессе применения алгоритма Евклида не превосходит упятеренного количества цифр меньшего числа, записанного в десятичной системе» [20], возможно вычислить число шагов $MaxEuclidSteps$ для наихудшего случая расширенного алгоритма Евклида по формуле (7).

$$MaxExEuclidSteps = \log_{10}(p-1) \times 5, \quad (7)$$

где p – значение первой составляющей модуля, определенное в параметрах криптосистемы.

В работе [21] приводится оценка количества элементарных операций, выполняемых на каждом шаге расширенного алгоритма Евклида, следовательно в наихудшем случае для поиска мультипликативного обратного необходимо выполнить $MaxExEuclidSteps$ делений, $MaxExEuclidSteps \times 3$ вычитаний и $MaxExEuclidSteps \times 3$ умножения.

Завершающей операцией по обнулению коэффициента a_{ij} является вычитание строки a_k из строки a_i по формуле (8).

$$a_i = a_i - M \times a_k\ mod\ p, \quad (8)$$

где i – номер строки, M – коэффициент, найденный по формуле (6), k – номер найденной строки для обнуления элемента a_{ij}, p – значение первой составляющей модуля, определенное в параметрах криптосистемы.

Из формулы (8) следует, что для вычисления нового элемента строки a_i нужно умножить соответствующий ему элемент из строки a_k на коэффициент M, вычесть найденное значение из текущего элемента строки a_i, а затем получить остаток от деления на p. Так как в методе Гаусса используется расширенная матрица, то количество операций умножения, сложения и получения остатка от деления на p при вычитании строки a_k из строки a_i на 1 больше числа переменных.

После завершения прямого хода формируется матрица верхнего треугольного вида, из которой необходимо найти значение переменной со степенью 1 с помощью обратного хода метода Гаусса. Из особенностей рассматриваемых СЛАУ, решаемых методом Гаусса, следует, что обратный ход такого метода всегда выполняется в один шаг и состоит из одной операции поиска мультипликативного обратного элемента по модулю, одного умножения и одной операции получения остатка от деления.

Таким образом, с учётом количества шагов $StepCount$ прямого хода метода Гаусса, определяемого по формуле (5) и количества всех операций, выполняемых на каждом шаге прямого хода, а также, принимая во внимание те операции, которые необходимо выполнить на этапе обратного хода, можно определить общее количество операций метода Гаусса для поиска решения двух СЛАУ размера d, которое составляет:

- $2(\sum_{i=1}^{d-1} i + 1) = d^2 - d + 2$ операций поиска мультипликативного обратного элемента по модулю;
- $2(\sum_{i=1}^{d-1} i \times (d+1)) = d^3 - d$ операций вычитания;
- $2(\sum_{i=1}^{d-1} i \times (d+2) + 1) = d^3 + d^2 - 2d + 2$ операций умножения;
- $2(\sum_{i=1}^{d-1} i \times (d+2) + 1) = d^3 + d^2 - 2d + 2$ операций получения остатка от деления.

Практическая оценка вычислительной сложности метода Гаусса для поиска решения СЛАУ по модулю. Выше сложность расширенного алгоритма Евклида была оценена теоретически как наихудший случай. Однако в контексте оценки критичности реализации атаки важно понимать не только наихудший случай, но и средний, поэтому рассматриваемая атака была реализована на языке C# в рамках описанной в работах [22, 23] системы для анализа гомоморфных шифров. Исходными данными для запуска атаки выбраны значения модулей $p = 193$, $q = 197$, а степень полинома представления шифртекста d варьировалась от 1000 до 2000 включительно с шагом 100.

Зависимость количества шагов расширенного алгоритма Евклида от степени полинома представления шифртекста d приводится на рис. 2.

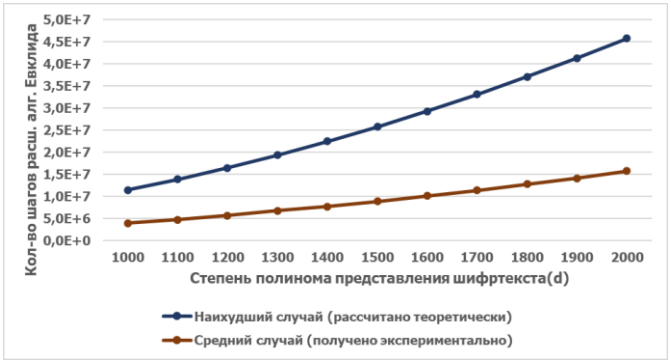


Рис. 2. Количество шагов расширенного алгоритма Евклида, выполняемых при атаке с известным открытым текстом в зависимости от степени полинома представления шифртекста (d)

Заключение. В данной работе рассмотрена атака с известным открытым текстом на криптографическую систему Доминго-Феррера. В данной атаке на этапе поиска составных частей ключа (r_p, r_q) требуется решение систем линейных алгебраических уравнений по модулю, что влечет за собой значительные вычислительные затраты. Для поиска ре-

шения подобных СЛАУ применен метод Гаусса. Данный метод обладает кубической вычислительной сложностью $O(d^3)$ и реализован в однопоточном режиме. Полученные оценки вычислительной сложности подтверждены экспериментальными исследованиями соответствующей реализации на языке программирования C#. В качестве исходных данных криптосистемы выбраны параметры модулей $p = 193$, $q = 197$ и степень полинома представления шифртекста $d = 2000$. Время реализации в рассмотренной атаке этапа поиска составляющих ключа на процессоре AMD Ryzen 5 3500U (2.1 ГГц) в однопоточном режиме составило 290,25 с.

Для метода Гаусса существуют способы параллельной реализации, применимые и для рассмотренной задачи. Следовательно, одним из направлений дальнейшей работы является оценка времени выполнения атаки с известным открытым текстом на криптографическую систему Доминго-Феррера с использованием параллельной реализации метода Гаусса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Прудникова А.А., Садовникова Т.М.* Анализ облачных сервисов с точки зрения информационной безопасности // T-Comm-Телекоммуникации и Транспорт. – 2012. – № 7. – С. 153-156.
2. *Бабенко Л.К., Русаловский И.Д.* Метод реализации гомоморфного деления // Известия ЮФУ. Технические науки. – 2020. – № 4 (214). – С. 212-221. – DOI: 10.18522/2311-3103-2020-4-212-221.
3. *Gentry C.* A fully homomorphic encryption scheme. – Stanford university, 2009.
4. *Lyubashevsky V., Peikert C., Regev O.* On ideal lattices and learning with errors over rings // Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29. – Springer Berlin Heidelberg, 2010. – P. 1-23.
5. *Бабенко Л.К. и др.* Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. – 2015. – № 3. – С. 3-26.
6. *Acar A. et al.* A survey on homomorphic encryption schemes: Theory and implementation // ACM Computing Surveys (Csur). – 2018. – Vol. 51, No. 4. – P. 1-35.
7. *Armknecht F. et al.* On constructing homomorphic encryption schemes from coding theory // IMA International Conference on Cryptography and Coding. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. – P. 23-40.
8. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism // International Conference on Information Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2002. – P. 471-483.
9. *Zhirov A., Zhirova O., Krendelev S.F.* Practical fully homomorphic encryption over polynomial quotient rings // World Congress on Internet Security (WorldCIS-2013). – IEEE, 2013. – P. 70-75.
10. *Kipnis A., Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification // Cryptology ePrint Archive. – 2012.
11. *Merkel W. et al.* Factorization of numbers with physical systems // Fortschritte der Physik: Progress of Physics. – 2006. – Vol. 54, No. 8-10. – P. 856-865.
12. *Lenstra A. K. et al.* The factorization of the ninth Fermat number // Mathematics of Computation. – 1993. – Vol. 61, No. 203. – P. 319-349.
13. *Cheon J.H., Nam H.S.* A cryptanalysis of the original domingo-ferrer's algebraic privacy homomophism // Cryptology EPrint Archive. – 2003.
14. *Trepacheva A. V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem // Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). – 2014. – Vol. 26, No. 5. – P. 83-98.
15. *Чернявский А.Ф., Козлова Е.И., Чернявский Ю.А.* Особенности структурно-аппаратного обеспечения преобразования информации в криптосистемах // Доклады Белорусского государственного университета информатики и радиоэлектроники. – 2024. – Т. 22, № 5. – С. 80-88. – DOI: 10.35596/1729-7648-2024-22-5-80-88.
16. *Соколова Е.В.* Обобщение прямых и итерационных методов решения систем линейных алгебраических уравнений // Математика и ИТ - вместе в цифровое будущее: Сб. трудов Молодежной школы, Нижний Новгород, 25–29 апреля 2022 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2022. – С. 111-120.

17. *Ефанов В.В., Закота А.А., Гунькина А.С.* Методика оценки точности определения параметров движения воздушной цели в условиях скрытного наблюдения за ней на основе применения метода итерации // Тр. МАИ. – 2021. – № 117. – DOI: 10.34759/trd-2021-117-18.
18. *Сеченов П.А.* Сравнение быстродействия численных методов Гаусса и LUP-разложения в задаче нахождения равновесного химического состава // Вестник Воронежского государственного технического университета. – 2023. – Т. 19, №. 2. – С. 79-85. – DOI: 10.36622/VSTU.2023.19.2.012.
19. *Iliev A., Kyurkchiev N.* The faster extended Euclidean algorithm // Collection of scientific works from conference. – 2018. – P. 21-26.
20. *Абрамов С.А.* Математические построения и программирование. – 1978.
21. *Бабенко Л.К., Стародубцев В.С.* Оценка времени выполнения операций шифрования, расшифрования, гомоморфных вычислений с использованием криптосистемы Доминго-Феррера // Известия ЮФУ. Технические науки. – 2024. – № 5 (241). – С. 6-15. – DOI: 10.18522/2311-3103-2024-5-6-15.
22. *Бабенко Л.К., Стародубцев В.С.* Особенности реализации системы криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел // Известия ЮФУ. Технические науки. – 2024. – № 3 (239). – С. 55-64. – DOI: 10.18522/2311-3103-2024-3-55-64.
23. *Бабенко Л.К., Стародубцев В.С.* Особенности реализации систем криптоанализа гомоморфных шифров, основанных на задаче факторизации чисел, на примере криптосистемы MORE // Вопросы кибербезопасности. – 2024. – № 3 (61). – С. 141-145. – DOI: 10.21681/2311-3456-2024-3-141-145.

REFERENCES

1. *Prudnikova A.A., Sadovnikova T.M.* Analiz oblachnykh servisov s tochki zreniya informatsionnoy bezopasnosti [Analysis of cloud services from the point of view of information security], *T-Comm-Telekommunikatsii i Transport* [T-Comm-Telecommunications and Transport], 2012, No. 7, pp. 153-156.
2. *Babenko L.K., Rusalovskiy I.D.* Metod realizatsii gomomorfnogo deleniya [Method for implementing homomorphic division], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 4 (214), pp. 212-221. DOI: 10.18522/2311-3103-2020-4-212-221.
3. *Gentry C.* A fully homomorphic encryption scheme. Stanford university, 2009.
4. *Lyubashevsky V., Peikert C., Regev O.* On ideal lattices and learning with errors over rings, *Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30–June 3, 2010. Proceedings 29*. Springer Berlin Heidelberg, 2010, pp. 1-23.
5. *Babenko L.K. i dr.* Polnost'yu gomomorfnoe shifrovanie (obzor) [Fully homomorphic encryption (review)], *Voprosy zashchity informatsii* [Information Security Issues], 2015, No. 3, pp. 3-26.
6. *Acar A. et al.* A survey on homomorphic encryption schemes: Theory and implementation, *ACM Computing Surveys (Csur),* 2018, Vol. 51, No. 4, pp. 1-35.
7. *Armknecht F. et al.* On constructing homomorphic encryption schemes from coding theory, *IMA International Conference on Cryptography and Coding*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 23-40.
8. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism, *International Conference on Information Security*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2002, pp. 471-483.
9. *Zhirov A., Zhirova O., Krendelev S.F.* Practical fully homomorphic encryption over polynomial quotient rings, *World Congress on Internet Security (WorldCIS-2013)*. IEEE, 2013, pp. 70-75.
10. *Kipnis A., Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification, *Cryptology ePrint Archive,* 2012.
11. *Merkel W. et al.* Factorization of numbers with physical systems, *Fortschritte der Physik: Progress of Physics,* 2006, Vol. 54, No. 8-10, pp. 856-865.
12. *Lenstra A. K. et al.* The factorization of the ninth Fermat number, *Mathematics of Computation,* 1993, Vol. 61, No. 203, pp. 319-349.
13. *Cheon J.H., Nam H.S.* A cryptanalysis of the original domingo-ferrer's algebraic privacy homomophism, *Cryptology EPrint Archive,* 2003.
14. *Trepacheva A. V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem, *Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS),* 2014, Vol. 26, No. 5, pp. 83-98.
15. *Chernyavskiy A.F., Kozlova E.I., Chernyavskiy Yu.A.* Osobennosti strukturno-apparatnogo obespecheniya preobrazovaniya informatsii v kriptosistemakh [Features of structural and hardware support for information transformation in cryptosystems], *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioelektroniki* [Reports of the Belarusian State University of Informatics and Radioelectronics], 2024, Vol. 22, No. 5, pp. 80-88. DOI: 10.35596/1729-7648-2024-22-5-80-88.

16. *Sokolova E.V.* Obobshchenie pryamykh i iteratsionnykh metodov resheniya sistem lineynykh algebraicheskikh uravneniy [Generalization of direct and iterative methods for solving systems of linear algebraic equations], *Matematika i IT - vmeste v tsifrovoe budushchee: Sb. trudov Molodezhnoy shkoly, Nizhniy Novgorod, 25–29 aprelya 2022 goda* [Mathematics and IT - together into the digital future: Collection of works of the Youth School, Nizhny Novgorod, April 25-29, 2022]. Nizhniy Novgorod: Natsional'nyy issledovatel'skiy Nizhegorodskiy gosudarstvennyy universitet im. N.I. Lobachevskogo, 2022, pp. 111-120.
17. *Efanov V.V., Zakota A.A., Gun'kina A.S.* Metodika otsenki tochnosti opredeleniya parametrov dvizheniya vozdushnoy tseli v usloviyakh skrytnogo nablyudeniya za ney na osnove primeneniya metoda iteratsii [Methodology for assessing the accuracy of determining the motion parameters of an air target under covert surveillance based on the iteration method], *Tr. MAI* [Proceedings of MAI], 2021, No. 117. DOI: 10.34759/trd-2021-117-18.
18. *Sechenov P.A.* Sravnenie bystrodeystviya chislennykh metodov Gaussa i LUP-razlozheniya v zadache nakhozhdeniya ravnovesnogo khimicheskogo sostava [Comparison of the performance of numerical Gaussian methods and LUP decomposition in the problem of finding the equilibrium chemical composition], *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University], 2023, Vol. 19, No. 2, pp. 79-85. DOI: 10.36622/VSTU.2023.19.2.012.
19. *Iliev A., Kyurkchiev N.* The faster extended Euclidean algorithm, *Collection of scientific works from conference,* 2018, pp. 21-26.
20. *Abramov S.A.* Matematicheskie postroeniya i programmirovanie [Mathematical constructions and programming], 1978.
21. *Babenko L.K., Starodubtsev V.S.* Otsenka vremeni vypolneniya operatsiy shifrovaniya, rasshifrovaniya, gomomorfnykh vychisleniy s ispol'zovaniem kriptosistemy Domingo-Ferrera [Estimation of execution time of encryption, decryption, homomorphic computations using the Domingo-Ferrer cryptosystem], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 5 (241), pp. 6-15. – DOI: 10.18522/2311-3103-2024-5-6-15.
22. *Babenko L.K., Starodubtsev V.S.* Osobennosti realizatsii sistemy kriptoanaliza gomomorfnykh shifrov, osnovannykh na zadache faktorizatsii chisel [Features of the implementation of the cryptanalysis system of homomorphic ciphers based on the problem of number factorization], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 3 (239), pp. 55-64. DOI: 10.18522/2311-3103-2024-3-55-64.
23. *Babenko L.K., Starodubtsev V.S.* Osobennosti realizatsii sistem kriptoanaliza gomomorfnykh shifrov, osnovannykh na zadache faktorizatsii chisel, na primere kriptosistemy MORE [Features of the implementation of cryptanalysis systems of homomorphic ciphers based on the problem of number factorization, using the example of the MORE cryptosystem], *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2024, No. 3 (61), pp. 141-145. DOI: 10.21681/2311-3456-2024-3-141-145.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; тел.: +79054530191; г. Таганрог, Россия; кафедра безопасности информационных технологий им. Макаревича О.Б.; д.т.н.; профессор.

Стародубцев Виталий Сергеевич – Южный федеральный университет; e-mail: vstarodubcev@sfedu.ru; тел.: +79996928150; г. Таганрог, Россия; кафедра безопасности информационных технологий им. Макаревича О.Б.; аспирант.

Ельчанинова Наталья Борисовна – Южный федеральный университет; e-mail: nbelchaninova@sfedu.ru; г. Таганрог, Россия; тел.: +79185000495; кафедра безопасности информационных технологий им. Макаревича О.Б.; к.т.н.; доцент.

Babenko Lyudmila Kliment'evna – Southern Federal University; e-mail: lkbabenko@sfedu.ru; phone: +79054530191; Taganrog, Russia; the Department of Information Technology Security named after Makarevich O.B.; dr of eng. sc.; professor.

Starodubcev Vitalij Sergeevich – Southern Federal University; e-mail: vstarodubcev@sfedu.ru; Taganrog, Russia; phone: +79996928150; the Department of Information Technology Security named after Makarevich O.B.; post graduate student.

Yelchaninova Natalia Borisovna – Southern Federal University; e-mail: nbelchaninova@sfedu.ru; Taganrog, Russia; phone: +79185000495; the Department of Information Technology Security named after Makarevich O.B.; cand. of eng. sc.; associate professor.

Раздел IV. Машинное обучение и обработка данных

УДК 004.272.2 DOI 10.18522/2311-3103-2025-3-119-134

И.И. Левин, Д.С. Буряков

РЕАЛИЗАЦИЯ МЕТОДОВ СИНХРОНИЗАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ В СИСТЕМАХ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

В задачах цифровой обработки сигналов, предполагающих когерентную обработку данных от фазированной антенной решетки, важно обеспечить согласованное поступление оцифрованных данных от антенных элементов в узлы обработки. С ростом числа каналов передачи данных в комплексах ЦОС существенно возрастает вероятность возникновения ошибок в каналах передачи данных, что выдвигает повышенные требования к обеспечению гарантоспособности программного комплекса изохронной передачи данных. В статье представлены результаты разработки и реализации методов, повышающих гарантоспособность изохронной передачи данных. Предложен комбинированный метод изохронной передачи данных, отличающийся применением служебных промежутков при передаче массивов операндов и динамической компенсацией задержек в каналах данных. Выделены наиболее вероятные ошибки, возникающие при передаче данных и предложены способы их парирования. Описан программный комплекс, реализующий комбинированный метод. Используя атрибутивную модель гарантоспособности, проведен анализ гарантоспособности программного комплекса. Анализ показал, что использование комбинированного метода позволит в четыре раза увеличить количество каналов передачи данных в комплексе ЦОС при заданном уровне гарантоспособности и фиксированном времени доверительной работы по сравнению с базовым методом. При значительном увеличении количества каналов передачи данных возникает необходимость сохранения заданного уровня гарантоспособности. В этой связи предложен модернизированный метод изохронной передачи данных, в котором были усовершенствованы алгоритмы проверки целостности данных, проверки допустимого диапазона рассогласования задержек в каналах данных и добавлен алгоритм переключения опорных каналов. Оценка гарантоспособности реализации модернизированного метода показала его способность обеспечить двукратное увеличение числа каналов данных по сравнению с комбинированным методом.

Программируемая логическая интегральная схема; цифровая обработка сигналов; гарантоспособность; фазированная антенная решетка; когерентная обработка данных.

I.I. Levin, D.S. Buryakov

REALIZATION OF METHODS FOR SYNCHRONIZATION OF DATA FLOWS IN DIGITAL SIGNAL PROCESSING SYSTEMS

In digital signal processing applications involving coherent processing of data from a phased antenna array, it is important to ensure the coordinated arrival of digitized data from antenna elements to processing units. As the number of data transmission channels in DSP complexes grows, the probability of errors in the data transmission channels increases significantly, which puts forward increased requirements to the assurance of the program complex of isochronous data transmission. The paper presents the results of the development and realization of methods that increase the assurance of isochronous data transmission. A combined method of isochronous data transmission is proposed, characterized by the use of service gaps in the transmission of operand arrays and dynamic compensation of delays in data channels. The most probable errors occurring during data transmission are singled out and methods of their parrying are proposed. A program complex realizing the combined method is described. Using the attributive model of dependability, the dependability of the program complex is analyzed. The analysis has shown that the use of the combined method will quadruple the number of data transmission channels in the DSP complex at a given level of dependability and fixed time of reliable operation in comparison with the basic method. With a significant increase in the number of data channels, there is a need to maintain a given

level of dependability. In this regard, a modernized method of isochronous data transmission is proposed, in which the algorithms for checking data integrity, checking the acceptable range of delay mismatch in the data channels and the algorithm for switching the reference channels were improved. An evaluation of the implementation dependability of the modernized method showed its ability to provide twice the number of data channels compared to the combined method.

Field programmable gate array; digital signal processing; dependability; phased array antenna; coherent data processing.

Введение. Ряд задач цифровой обработки сигналов (ЦОС) требует когерентной обработки, предполагающей согласование данных от множества каналов, полученных в один момент времени. Известным примером когерентной обработки является формирование диаграммы направленности ФАР [1], требующей согласованно обработать информацию, полученную от всех без исключения антенных элементов ФАР и соответствующую одному моменту физического времени [2]. Передачу данных, гарантирующую поступление операндов, соответствующих одному моменту физического времени, от множества передающих блоков (узлов) в узел цифровой обработки сигналов в дальнейшем, будем называть изохронной.

Синхронизация функционирования узлов изохронной передачи данных – сложная задача, требующая согласованной работы всех источников и приемников информации. Один из эффективных способов синхронизации данных – использование системы единого времени [3], которая включает в себя первичные (ведущие) часы и вторичные (ведомые) часы в блоках, что позволяет установить единое и точное время во всех блоках.

Наиболее важным параметром систем единого времени является точность установки времени в различных узлах. Наиболее перспективным среди существующих технологий единого времени считается протокол PTP (Precision Time Protocol) [4], который может обеспечить установку времени в различных узлах с точностью 100 нс. Однако типовая частота оцифровки данных от элементов ФАР в системах когерентной обработки сигналов составляет около 100 МГц. Для точной привязки времени к данным требуется, чтобы точность привязки времени соответствовала одному такту оцифровки, следовательно, дискрета шкалы времени должна быть не более 10 нс, что обеспечит необходимую точность установки времени в различных узлах. В этой связи точность PTP для систем когерентной обработки информации от ФАР является недостаточной.

Различные блоки, как правило, имеют свои собственные тактовые генераторы, которые не могут быть идентичными, поэтому временные метки, полученные от ведущих часов, могут быть захвачены различными фазами тактового сигнала в разных устройствах. Кроме того, существует дрейф частоты тактовых генераторов в различных устройствах, который также влияет на точность установки времени. Указанные процессы могут привести к расхождению времени в различных блоках в интервалах между обновлениями времени от ведущего устройства. Это требует разработки новых методов синхронизации времени в разных узлах комплекса ЦОС.

Для обеспечения требуемой точности установки времени предлагается применить локальную систему единого времени, распространяющую сигналы единого машинного времени и опорную тактовую частоту из единого центра во все узлы по множеству каналов с одинаковой задержкой [5]. Каждый узел комплекса когерентной обработки сигналов имеет собственную систему машинного времени. В узле имеется свой счетчик текущего времени, который работает от опорной тактовой частоты и периодически обновляется значениями времени от источника единого машинного времени.

Для передачи сигналов единого машинного времени, как правило, используется линейный самосинхронизирующийся код Манчестер-II [6]. Этот код является улучшенной версией классического кода Манчестера и обеспечивает дополнительную стабильность при передаче данных.

Предлагаемые решения обеспечат синхронизацию времени в различных блоках с точностью до нескольких наносекунд.

Средства когерентной обработки данных. Для выполнения задач когерентной обработки информации от антенных элементов ФАР используются высокопроизводительные вычислительные устройства, построенные на различной элементной базе: на интегральных схемах специального назначения (ASIC), универсальных процессорах или программируемых логических интегральных схемах (ПЛИС).

Универсальные процессоры удобны для программирования, но имеют существенные ограничения при их применении для обработки информации в реальном масштабе времени. Основная проблема – недостаточная вычислительная мощность процессоров, что критично, учитывая сложность математических операций и большие объемы обрабатываемых данных [7]. Ограниченная параллельная обработка и сложность интеграции с аппаратными компонентами систем с ФАР также являются существенными минусами.

Специализированные микросхемы ASIC обеспечивают наиболее высокую производительность, но требуют значительных затрат на разработку и производство [8]. Использование ASIC оправдано для устройств, выпускаемых серийно, но они неэффективны для устройств обработки данных от ФАР, т.к. каждая система с ФАР может потребовать реализовать особые алгоритмы обработки.

В этом случае ПЛИС представляют собой разумный компромисс. Их главное преимущество – гибкость конфигурации, позволяющая адаптировать структуру под меняющиеся требования без изменения аппаратной части [9]. Богатый набор ресурсов для цифровой обработки сигналов и разнообразные интерфейсы обеспечивают эффективную многопоточную обработку данных [10]. Важное достоинство ПЛИС – минимальная задержка при обработке, благодаря прямой работе с аппаратными ресурсами, что крайне важно для многоканальных систем реального времени [11]. Большой объем вычислительных ресурсов и развитая периферия ПЛИС упрощают их интеграцию в системы ЦОС с ФАР.

Комбинированный метод изохронной передачи данных. Для передачи данных от узлов приёма к узлам обработки предлагается использовать оптические каналы [12] из-за их стабильности и минимального дрейфа характеристик. В разных каналах данных порой возникают задержки из-за преобразования сигнала, и эти задержки могут значительно различаться, поэтому для изохронной передачи данных важно обеспечить выравнивание потоков операндов. Для передачи привязанных ко времени данных обычно используют различные протоколы сетевых технологий [13], так как классическая пакетная передача не подходит для обеспечения потока данных в режиме реального времени – она допускает высокие, порой недопустимые задержки и может даже нарушить порядок следования пакетов данных, что недопустимо для когерентной обработки.

Тривиальным решением для передачи данных, привязанных ко времени, является сопровождение каждого операнда временной меткой. Временная диаграмма показана на рис. 1.

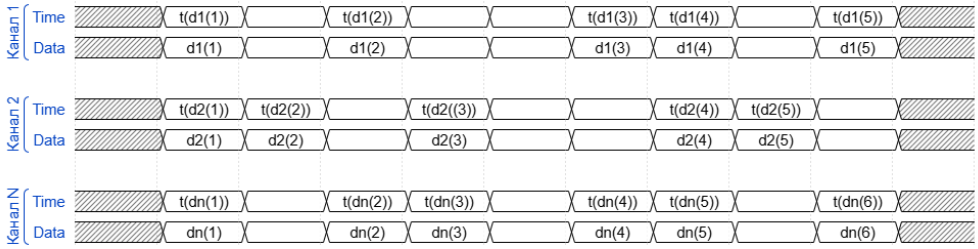


Рис. 1. Временная диаграмма привязки каждого операнда ко времени

Операнд в данном контексте – это отдельное данное, привязанное ко времени и используемое для обработки в узлах когерентной цифровой обработки сигналов. Данный метод обеспечивает передачу привязанных ко времени операндов, но имеет ряд существенных недостатков: значительное снижение пропускной способности канала из-за выделения части канала под временную метку и усложнение процедуры выравнивания операндов, требующее сложных алгоритмов анализа и буферизации на стороне приёмника.

Можно усовершенствовать протокол, сформировав непрерывный синхронный поток операндов, как показано на рис. 2. В этом случае метка времени t(d1(1)) будет передана только для первого операнда в массиве. Поскольку операнды массива передаются синхронно, временную метку можно определить для любого операнда в потоке, добавив к временной метке порядковый номер элемента массива, уменьшенный на единицу.

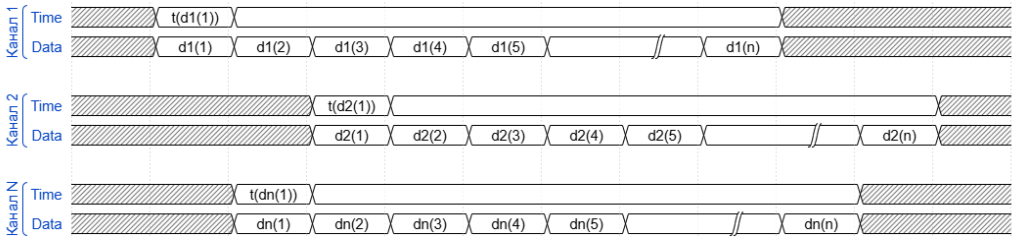


Рис. 2. Временная диаграмма привязки массива операндов ко времени

Такой протокол передачи данных избавляет от сложных алгоритмов выравнивания потоков данных в различных каналах, но сокращение пропускной способности из-за выделения отдельных каналов для передачи временной метки по-прежнему сохраняется.

Существует актуальный протокол, применяемый в современных устройства когерентной цифровой обработки сигналов, который для удобства дальнейшего изложения обозначим как базовый. Он отличается размещением временной метки непосредственно в потоке операндов, что позволяет значительно повысить пропускную способность. Временная диаграмма показана на рис. 3

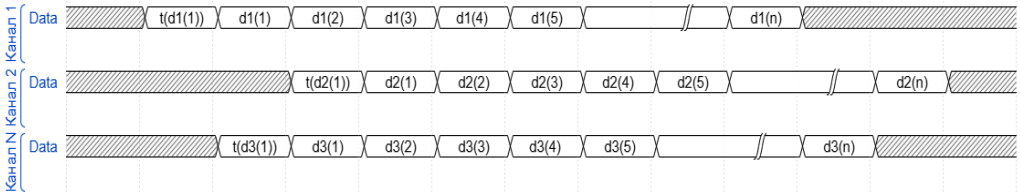


Рис. 3. Временная диаграмма размещения метки времени в потоке операндов

Для того чтобы устранить различия в задержках между каналами, используется следующий прием: во время инициализации подсистемы передачи данных производится измерение задержек для каждого канала. Полученные данные поступают в буферные элементы, которые настраиваются таким образом, чтобы на выходе задержки между каналами были устранены.

Недостатком этого метода является вычисление задержек только на этапе инициализации. Вычисленные значения задержек фиксируются и не изменяются в процессе работы системы. Метод не учитывает динамическое изменение задержек в различных каналах, однако на практике возможно изменение задержек между каналами в процессе работы. Например, при потере соединения и его последующего восстановления задержка может отличатся от той, что была рассчитана ранее, тем самым изохронная передача данных будет нарушена. В этом случае потребуется повторить процедуру вычисления новых значений задержек.

Для устранения описанных выше недостатков предлагается использовать новый метод обеспечения изохронной передачи данных, отличающийся от предыдущего применением служебных промежутков при передаче массивов операндов. Временная диаграмма показана на рис. 4.

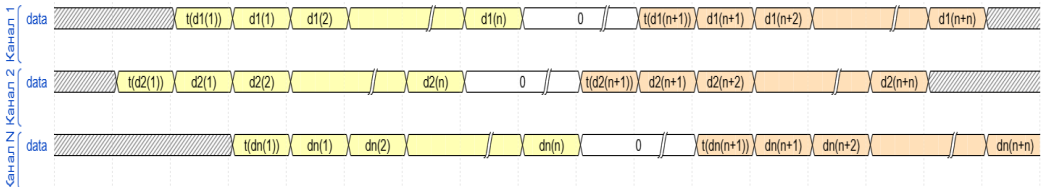


Рис. 4. Временная диаграмма передачи массивов операндов со служебными промежутками

Из передающего устройства оцифрованные данные подаются массивом операндов. Суть метода заключается в том, чтобы разделить входной массив операндов на группы одинаковой длины, которые дополняются сервисной информацией и передаются на более высокой частоте со служебными промежутками. В служебном промежутке перед началом массива операндов необходимо поместить заголовок с временной меткой, соответствующей времени получения первого операнда массива, тем самым осуществив его привязку ко времени. Кроме того, необходимо выполнить подсчет контрольной суммы заголовка и массива и разместить ее в служебном промежутке после массива операндов.

Временная диаграмма примера преобразования в формат массивов данных, разделенных служебными промежутками, представлена на рис. 5.

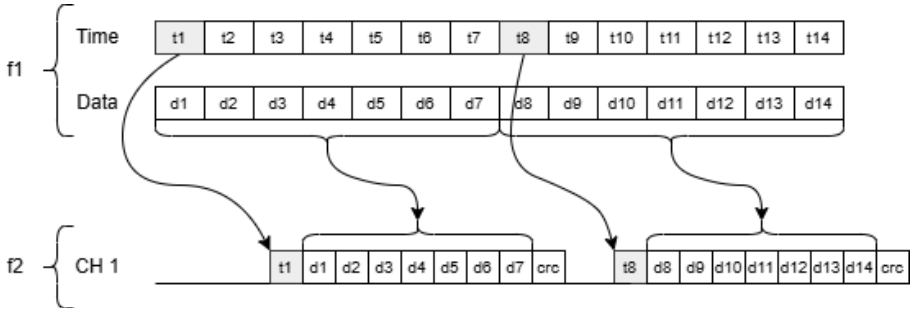


Рис. 5. Временная диаграмма преобразования непрерывного потока операндов

В процессе передачи данных в узел приема между различными каналами неизбежно возникнут рассогласования, выравнивание которых и будет произведено в узле приема. В каждом из входных каналов задействована буферная память. Запись в память массивов операндов происходит независимо по каждому каналу при их поступлении, а команда чтения подается на все блоки буферной памяти одновременно, обеспечивая выравнивание задержек между каналами, таким образом обеспечивается динамическое выравнивание задержек, возникающих при передаче массивов операндов, и происходит восстановление первоначального непрерывного изохронного потока данных, необходимого для алгоритмов когерентной цифровой обработки сигналов.

Реализация комбинированного метода изохронной передачи данных. Комбинированный метод изохронной передачи данных был применен для создания программного комплекса обеспечения изохронной передачи данных в комплексе когерентной обработки информации от антенных элементов ФАР. Комплекс когерентной обработки построен на основе группы ПЛИС Xilinx Virtex-7 XC7VX485T. На вход каждой ПЛИС поступает 24 канала разрядностью 33 бита (32 бита данных и 1 бит строб) на частоте $F_1 = 255$ МГц. Данные поступают массивами операндов, разделенными служебными промежутками. Длина массива операндов составляет 64 слова, длина служебного промежутка – четыре слова. В служебный промежуток перед началом массива операндов вставлено два слова, соответствующих метке времени первого данного массива операндов. В конце массива размещено одно слово контрольной суммы, посчитанной для всех операндов массива и для метки времени. Структура входных данных для одного канала представлена на рис. 6.

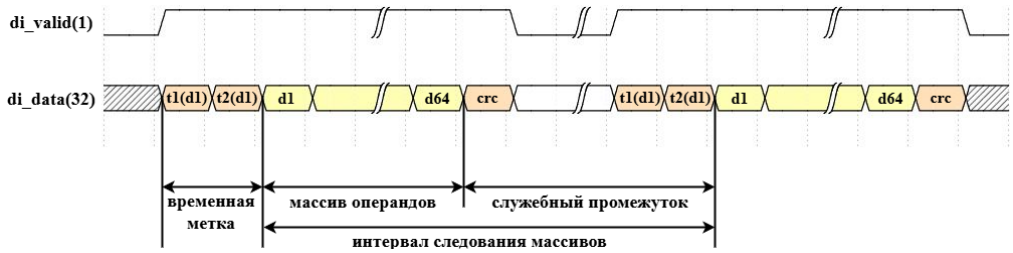


Рис. 6. Структура входных данных

Программа, реализованная в ПЛИС, выдает 24 непрерывных потока операндов разрядностью 32 бита на частоте 240 МГц. Все потоки операндов сопровождаются одним стробом и меткой времени первого операнда массива.

Программа, реализующая комбинированный метод изохронной передачи данных, состоит из программных блоков, реализованных независимо для каждого канала (B1 – B24), и общего блока (A), управляющего работой всех каналов. Общий блок для всех каналов A включает в себя: блок управления (БУПР) и блок синхронизации времени (БСВ).

Блок управления (БУПР) – выполняет несколько функций, которые определяют работу всех остальных программных блоков, среди которых: поиск и задание опорного канала, установка допустимого диапазона рассогласования, запуск процесса одновременного считывания данных из памяти.

При передаче информации в каналах данных неизбежно возникают задержки, которые в каждом канале могут быть разными. Программа выравнивает задержки во всех каналах в пределах одной ПЛИС. Однако предельные значения допустимых задержек целесообразно ограничить, поскольку большие задержки приведут к увеличению латентности данных на выходе программы и необходимости использовать больший объем памяти. Слишком большие задержки могут свидетельствовать о неполадках канала данных, таких как нарушение синхронизации узла, передающего данные с системой единого машинного времени или с генератором опорной частоты, в результате чего данные в передающих узлах формируются в неправильный момент времени.

Использование таких данных недопустимо, так как это нарушает принципы изохронной передачи. Необходимо обнаруживать подобные ситуации и не пропускать данные такого канала на выход программы. Для того чтобы обнаружить недопустимые задержки в каналах данных, необходимо установить допустимый диапазон отклонений относительно одного из каналов, который будем называть опорным. Для выбора опорного канала в блоке управления разработан алгоритм, определяющий величину задержек в каждом канале и вычисляющий их среднее арифметическое значение. Опорным выбирается канал, задержка которого наиболее близка к среднему арифметическому значению.

После выбора опорного канала нужно сформировать диапазон допустимого рассогласования относительно первого данного этого канала. Допустимое рассогласование задается параметром PS_{max}. Диапазон измеряется в тактах частоты поступления данных и должен быть установлен за PS_{max} тактов до первого данного опорного канала и закончиться через $PS_{max} - 1$ тактов после. При поступлении массивов операндов в каждом канале проверяется, попадают ли их задержки в допустимый диапазон. Если задержка выходит за пределы диапазона, данные в массивах заменяются на массивы с нулевой информацией для минимизации негативного влияния на результат обработки.

В состав блока обработки потока данных (Bn) одного канала входят блоки: интерфейс трансивера (ИТ), блок приема данных (БПД), блок расчета контрольных сумм (БРКС), блок обработки ошибок целостности данных (БОЦД), буферная память FIFO, блок управления записью (БУЗ), блок управления чтением (БУЧ).

Структура программного блока, обеспечивающего работу одного канала, представлена на рис. 7

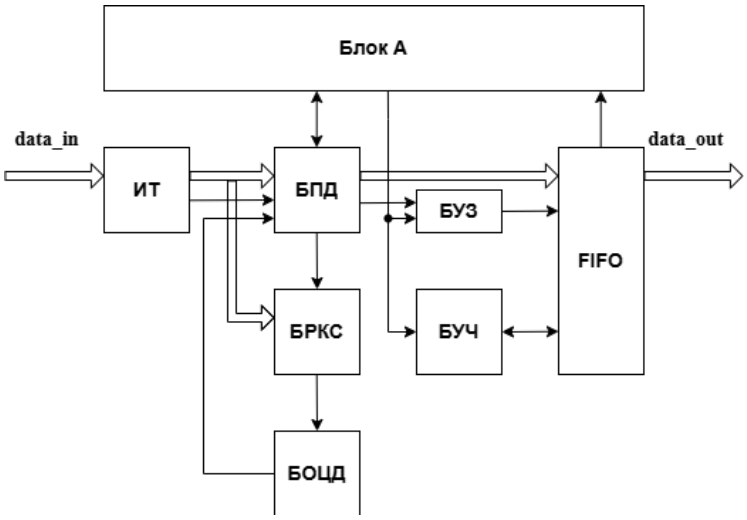


Рис. 7. Структура программного блока одного канала

Интерфейс трансивера (ИТ) – программный блок, управляющий работой аппаратного MGT трансивера (Multigigabit Transceiver), обеспечивает настройку параметров трансивера и проведение тренировки канала. На выходе блока интерфейса выставляются данные на шину di_data разрядностью 32 бита, в сопровождении строба di_valid. До приема данных после успешного завершения тренировки выставляется флаг готовности канала к работе rx_on, свидетельствующий о том, что канал активен и готов к работе.

Блок приема данных (БПД) – получает данные di_data со стробом di_valid от интерфейса трансивера, выделяет из заголовка временную метку time_mark и формирует следящие флаги: ch_data_sop – флаг начала массива данных; ch_data_eop – флаг конца массива данных; pkg_reach, pkg_reach_ltch – флаг устанавливаемый, если задержка канала входит в допустимый диапазон рассогласования; pkg_miss – флаг, устанавливаемый, если задержка канала больше допустимого диапазона рассогласования.

Блок расчета контрольных сумм (БРКС) – подсчитывает контрольную сумму для принятых данных. Блок получает данные di_data со стробом di_valid от блока интерфейса трансивера. При поступлении строба di_valid запускается счетчик принятых данных data_counter и производится расчет контрольной суммы принимаемых данных. Для расчета контрольных сумм был применен известный алгоритм CRC-16 Modbus [14]. После достижения счетчиком значения, заданного параметром длины массива, расчет контрольной суммы прекращается и производится сравнение принятой и рассчитанной контрольных сумм. При совпадении устанавливается флаг crc_pass, длительностью один такт, иначе выставляется флаг crc_fail.

Блок обработки ошибок целостности данных (БОЦД) – отслеживает количество ошибок в канале. Если число ошибок (err_cntr) превышает заданное значение (err_to_offline), то канал отключается (флаг ch_offline взводится). Для восстановления работы канала необходимо определённое количество безошибочно принятых массивов подряд. Их количество отслеживает счётчик good_cntr. Когда good_cntr достигает заданного значения (good_to_online), флаг ch_offline сбрасывается, и канал снова включается. Этот алгоритм позволяет ограничить количество ошибок за период времени и определить интервал, в течение которого отсутствие ошибок восстановит работу канала.

Буферная память FIFO – это двухпортовая блочная память (Dual-port Block RAM) [15], сконфигурированная в режиме FIFO (first in, first out). Блочная память является аппаратным ресурсом ПЛИС, она позволяет одновременно проводить операции чтения и записи, а также обеспечивает безопасную передачу данных между разными тактовыми доменами.

Блок управления записью (БУЗ) - управляет записью данных в память FIFO. Он получает флаги начала (ch_data_sop) и конца массива данных (ch_data_eop), а также флаг разрешения записи (allow_window_flag) от блока управления. Если флаг начала массива поступает при активном флаге разрешения записи, формируется флаг записи в FIFO. Запись прекращается при поступлении флага конца массива. Блок записывает в память только те массивы, начало которых попадает в допустимый интервал рассогласования.

Блок управления чтением (БУЧ) - осуществляет управление чтением данных из памяти FIFO. Алгоритм позволяет начать считывание данных в каждом канале из всех FIFO одновременно, если массивы данных прошли проверку на попадание в допустимый интервал рассогласования в блоке приёма данных. Если канал по каким-либо причинам отключится, данные из FIFO отключённого канала будут считываться до полного опустошения. При восстановлении работы канала данные из FIFO начнут считываться в момент времени, соответствующий интервалу следования массивов (длинна массива и размер служебного промежутка), чтобы сохранить согласованный поток данных.

Ресурс, занимаемый конфигурационным файлом ПЛИС, составил не более 5%. Программа была протестирована в составе устройства когерентной цифровой обработки информации от антенных элементов ФАР. В контрольных проверках было передано $3{,}38*10^{16}$ байт информации в течение 48 часов. В процессе тестирования постоянно фиксировались рассогласования каналов. Программа корректно выравнивала возникающие задержки в каналах. В процессе работы были сымитированы различные аварийные ситуации, включая недопустимые задержки рассогласования и нарушение целостности данных. На все воздействия программа реагировала корректно, парируя аварийные ситуации.

Анализ гарантоспособности программного комплекса изохронной передачи данных. Под гарантоспособностью понимается комплексное свойство системы (программного комплекса) предоставлять требуемые услуги, которым можно оправданно доверять [16].

Для количественной оценки гарантоспособности обычно используют атрибутивную модель [17]. Она описывает общие характеристики системы с помощью атрибутов и метрик. Атрибут объединяет различные свойства программного комплекса, а метрика представляет численное значение определённого параметра атрибута, характеризуя лишь одно из его свойств.

Рассматриваемый программный комплекс входит в состав программно-аппаратных средств, осуществляющих когерентную обработку данных. Поскольку программный комплекс предназначен исключительно для обеспечения изохронной передачи данных от множества каналов данных и не рассматривает функциональное преобразование данных, будем оценивать только те атрибуты, которые непосредственно влияют на его работу.

Наиболее важными атрибутами для программного комплекса изохронной передачи данных от множества каналов являются:

- целостность, которая для рассматриваемого программного комплекса понимается как целостность передаваемых данных;
- готовность, которая подразумевает доступность каналов передачи данных;
- живучесть, которая понимается как способность сохранять работоспособность в приемлемых пределах при превышении допустимых значений ошибок.

В соответствии с атрибутивной моделью оценки гарантоспособности определены метрики для каждого атрибута, причём каждый показатель должен характеризовать только одно свойство атрибута. Учитывая, что процессы имеют вероятностно-недетерминированный характер, в качестве метрик использованы вероятности возникновения возможных причин.

Целостность данных может нарушиться из-за битовых ошибок или нарушения формата передаваемых данных, поэтому для оценки этого атрибута использованы вероятность возникновения битовых ошибок в канале и вероятность нарушения формата данных.

Готовность каналов может быть нарушена из-за отключения канала вследствие неисправности или из-за ошибок в коммутации, вызванных действиями оператора или обслуживающего персонала. Для оценки готовности будем использовать вероятность отключения канала и вероятность ошибки оператора.

Живучесть программного комплекса отражает его способность сохранять работоспособность при превышении допустимого уровня ошибок. Программный комплекс изохронной передачи данных может парировать ошибки рассогласования задержек между каналами в определённых пределах. Однако могут возникнуть ситуации, когда значение рассогласования превышает допустимый уровень. Кроме того, существует вероятность того, что ошибка рассогласования будет замаскирована, если её значение совпадет с периодом следования массивов. Для оценки живучести будем использовать вероятность превышения допустимого значения рассогласования задержки канала и вероятность совпадения задержки с периодом следования массивов данных.

Атрибуты и метрики, применяемые для оценки гарантоспособности программного комплекса изохронной передачи данных, представлены в табл. 1.

Таблица 1

Атрибуты и метрики

№	Атрибут	Вес атрибута	Метрика	Вес метрики	Границы
1	Целостность	0,98	Коэффициент битовых ошибок	0,98	0..1
			Вероятность нарушения целостности формата данных	0,96	0..1
2	Готовность	0,96	Вероятность отключения канала	0,97	0..1
			Вероятность ошибки оператора	0,94	0..1
3	Живучесть	0,99	Вероятность превышения допустимого значения рассогласования задержки канала	0,99	0..1
			Вероятность совпадения задержки с периодом следования массивов данных	0,9	0..1

Весовые коэффициенты атрибутов и метрик установлены по результатам экспертных оценок, которые в свою очередь опирались на экспериментальные данные.

Очевидно, что гарантоспособность программного комплекса изохронной передачи данных существенно зависит требуемого времени доверительной (безошибочной) работы и количества каналов передачи данных. На практике принимают уровень гарантоспособности для сложных программных комплексов систем с ФАР, равным 0,95, а время доверительной работы системы – не менее шести часов.

Вероятность каждого типа ошибок в зависимости от количества каналов P_m^N комплекса рассчитывается по формуле

$$P_m^N = (1 - (1 - P_m)^N) \cdot W_m, \quad (1)$$

где P_m – вероятность ошибки в одном канале;

N – количество каналов;

W_m – весовой коэффициент метрики.

Общая вероятность для каждого атрибута P_a определяется по формуле

$$P_a = \left(1 - (1 - P_{m1}^N) \cdot (1 - P_{m2}^N)\right) \cdot W_a, \quad (2)$$

где W_a – весовой коэффициент атрибута.

Общий уровень гарантоспособности оценивается по формуле

$$G = 1 - \left(1 - (1 - P_{a1}) \cdot (1 - P_{a2}) \cdot (1 - P_{a3})\right). \quad (3)$$

Был проведен расчет гарантоспособности для базового метода. Анализ показал, что заданный уровень гарантоспособности 0,95 обеспечивается при числе каналов данных в системе не более 10900.

Для оценки гарантоспособности программной реализации комбинированного метода изохронной передачи данных необходимо ввести коэффициенты парирования ошибок, поскольку в реализации комбинированного метода, в отличии от базового метода, используются средства обнаружения и парирования неисправностей.

В программе, реализующей комбинированный метод, применены средства парирования наиболее вероятных типов ошибок, связанных с отключением канала, нарушением целостности данных и превышением допустимого диапазона рассогласования. Остальные типы ошибок не обнаруживаются и не парируются данным методом, так как их вероятность крайне низкая и на заданном времени доверительной работы и фиксированном числе каналов практически не повлияет на общий уровень гарантоспособности. Добавление средств обнаружения и парирования наименее вероятных типов ошибок увеличит занимаемый ресурс в ПЛИС и не даст заметного прироста общего уровня гарантоспособности.

Коэффициенты парирования наиболее вероятных ошибок для реализации комбинированного метода изохронной передачи данных приведены в табл. 2. Коэффициент парирования устанавливается экспертными методами в диапазоне от 0 до 1, где 0 – отсутствие парирования ошибки.

Таблица 2

Коэффициенты парирования для реализации комбинированного метода

№	Тип ошибки	Коэффициент парирования
1	Коэффициент битовых ошибок	0,55
2	Вероятность нарушения целостности формата данных	0,4
3	Вероятность отключения канала	0,77
4	Вероятность ошибки оператора	0,6
5	Вероятность превышения допустимого значения рассогласования задержки канала	0,85
6	Вероятность совпадения задержки с периодом следования массивов данных	0

Добавим коэффициент парирования ошибок K_p в формулу (3) и получим следующее выражение:

$$P_m^N = (1 - (1 - P_m)^N) \cdot W_m \cdot K_{p.} \quad (4)$$

Расчет гарантоспособности выполним по той же методике, что и для базового метода. Зависимость гарантоспособности от количества каналов показана на рис. 8.

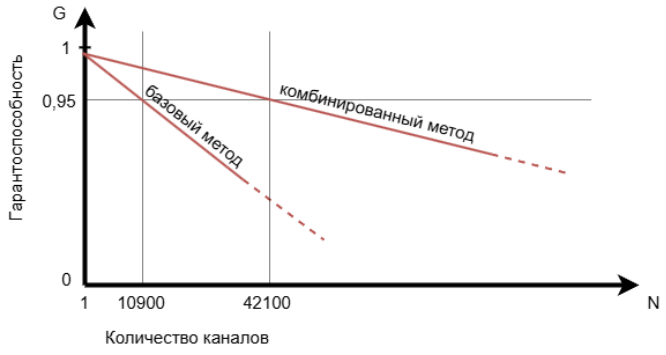


Рис. 8. Зависимость уровня гарантоспособности от количества каналов

Из графика видно, что заданный уровень гарантоспособности 0,95, а программа, реализующая комбинированный метод, обеспечивает уровень при числе каналов 42500.

Можно сделать вывод, что использование комбинированного метода изохронной передачи данных в совокупности со средствами обнаружения и парирования наиболее вероятных аварийных ситуаций сможет обеспечить в четыре раза большее количество каналов данных по сравнению с известным базовым методом при заданном уровне гарантоспособности.

Модернизированный метод изохронной передачи данных. Системы с ФАР постоянно развиваются, возникают новые трудоемкие научно-технические задачи, например, оперативное обнаружение космического мусора, увеличение количества которого в последние годы стало серьезной угрозой безопасности космических полетов [18, 19]. На сегодняшний день отмечается необходимость обнаружения космических объектов меньшего размера в отличие от тех, которые на данный момент могут быть обнаружены современными радиолокационными станциями (РЛС).

Чтобы улучшить разрешающую способность радиолокационной станции с фазированной антенной решеткой, обычно увеличивают количество её антенных элементов [20]. Это даёт возможность создать более сфокусированный луч благодаря уменьшению ширины основного лепестка диаграммы направленности. Это дает возможность предоставлять более детальную информацию о местоположении и перемещении целей в зоне действия РЛС. Исходя из этого, требуются новые перспективные РЛС, содержащие большее число антенных элементов, а следовательно, и каналов данных. При значительном увеличении количества каналов представленный комбинированный метод изохронной передачи данных уже не сможет обеспечить заданный уровень гарантоспособности.

В этой связи требуется модернизировать комбинированный метод, для того чтобы сохранить заданный высокий уровень гарантоспособности при значительном увеличении числа каналов системы. Для этого необходимо улучшить качество парирования ошибок, связанных с отключением канала, нарушением целостности данных и превышением допустимого диапазона рассогласования. В дополнение к этому целесообразно разработать процедуры парирования ошибок, которые ранее не обрабатывались, поскольку при значительном увеличении числа каналов их влияние будет значительным.

Эксперименты на системах с ФАР показали, что на практике наиболее часто встречаются ошибки целостности данных. В реализации комбинированного метода такие ошибки успешно обнаруживаются с помощью контрольных сумм, однако их успешное парирование происходит, только когда число ошибок достигнет установленного порога. Этот подход позволил обеспечить минимальную латентность (задержку) данных, а ошибки, пропущенные до достижения установленного порога количества ошибок, не оказывали существенного влияния на результат обработки. Однако при значительном увеличении числа каналов такой подход не обеспечивает требуемого уровня гарантоспособности, поскольку вырастет общая вероятность возникновения ошибок целостности данных, что может оказать негативное влияние на результат обработки. В этой связи предложено производить предварительную проверку контрольных сумм фрагментов массивов операндов.

В программной реализации комбинированного метода флаг старта одновременного считывания данных из памяти read_start формировался в блоке управления при поступлении флага not_empty от всех FIFO активных каналов, прошедших контроль на соответствие задержки допустимому диапазону рассогласования.

При реализации модернизированного метода флаг read_start формируется в блоке управления после того, как будут проверены контрольные суммы активных каналов, прошедших контроль на соответствие задержки. При этом блок обработки ошибок целостности данных упростится. Он будет устанавливать флаг отключения канала ch_offline при получении флага несовпадении контрольных сумм crc_fail, полученного от блока расчета контрольных сумм и сбрасывать при получении флага crc_pass, означающего совпадение контрольных сумм.

Применения такого подхода к парированию ошибок целостности данных позволит контролировать целостность данных до того, как массивы операндов будут отправлены на выход, тем самым увеличить процент парирования ошибок, что положительно по-

влияет на общей уровень гарантоспособности. Следует отметить увеличение латентности для модернизированного метода на величину размера массива операндов и объема буферной памяти, которая должна будет вместить в себя весь массив операндов.

Следующими по влиянию являются ошибки, связанные с отключением каналов. Программная реализация комбинированного метода эффективно справляется с их обнаружением и устранением последствий. Однако существует потенциально опасный сценарий: отключение канала, назначенного опорным, относительно которого формируется несколько управляющих сигналов и счетчиков, в том числе диапазон допустимого рассогласования, что может привести к нарушению работы всех обслуживаемых каналов. В такой ситуации для модернизированного метода предусмотрена возможность переключения опорного канала на другой работоспособный. Переключение должно производиться в процессе работы без остановки процесса передачи при обеспечении изохронного потока операндов.

В реализации комбинированного метода главный счетчик pkg_int_cntr, находящийся в блоке управления, генерирует управляющие сигналы, среди которых особенно важен флаг allow_window_flag, определяющий границы допустимого рассогласования. Счетчик начинает работу на этапе инициализации, как только определен опорный канал. При отключении опорного канала в программной реализации модернизированного метода счетчик pkg_int_cntr в блоке управления корректируется, чтобы система правильно работала с новым опорным каналом. Для этого вводятся дополнительные независимые счетчики в каждом канале, которые запускаются с момента начала поступления массивов данных, синхронно с началом массива. При смене опорного канала значение такого вспомогательного счетчика скорректирует параметры основного счетчика pkg_int_cntr, обеспечивая синхронизацию всех управляющих сигналов с новым опорным каналом. Использование этого приема позволит сохранить работоспособность системы даже при выходе из строя опорного канала.

Следует отметить, что при определенных условиях рассогласования массива операндов может достичь критического значения, равного интервалу следования массивов. В результате обрабатываемый массив оказывается либо сильно запаздывающим, либо опережающим остальные массивы на один или даже более периодов их следования. Это создает опасную ситуацию, поскольку программа не способна обнаружить подобную ошибку через проверку попадания в допустимый диапазон рассогласования, так как, с точки зрения алгоритма, в программной реализации комбинированного метода нарушения нет. Пропускание данных такого канала на выход программы недопустимо, так как это нарушает принципы изохронной передачи данных и может негативно повлиять в целом на формирование диаграммы направленности ФАР. К тому же, как правило, это - не разовая ошибка, если возникли неисправности в системе синхронизации, которые привели к возникновению рассогласования, то, вероятней всего, это критическое значение задержки сохранится до перезапуска или пересинхронизации комплекса. Это означает, что на протяжение этого времени в канале будут невалидные данные.

Для того чтобы обнаруживать такие ошибки, в передающем узле применяется счетчик массивов, значение которого записывается в служебный промежуток перед массивом операндов перед его отправкой, тем самым позволяя пронумеровать массивы операндов. На стороне приемника данных в блоке приема данных реализован алгоритм проверки значения этого счетчика, и при его несоответствии значению счетчика опорного канала устанавливается флаг pkg_miss, свидетельствующий о превышении допустимой задержки рассогласования. Таким образом, будет обнаружена и парирована ошибка рассогласования, совпадающая с периодом следования массивов операндов.

Коэффициенты парирования для модернизированного метода изохронной передачи данных представлены в табл. 3.

Таблица 3

Коэффициенты парирования для реализации модернизированного метода

№	Тип ошибки	Коэффициент парирования
1	Коэффициент битовых ошибок	0,98
2	Вероятность нарушения целостности формата данных	0,95
3	Вероятность отключения канала	0,88
4	Вероятность ошибки оператора	0,86
5	Вероятность превышения допустимого значения рассогласования задержки канала	0,85
6	Вероятность совпадения задержки с периодом следования массивов данных	0,95

Используя ту же методику оценки гарантоспособности, что и для комбинированного метода, получили зависимость гарантоспособности от количества каналов для модернизированного метода, показанную на рис. 9.

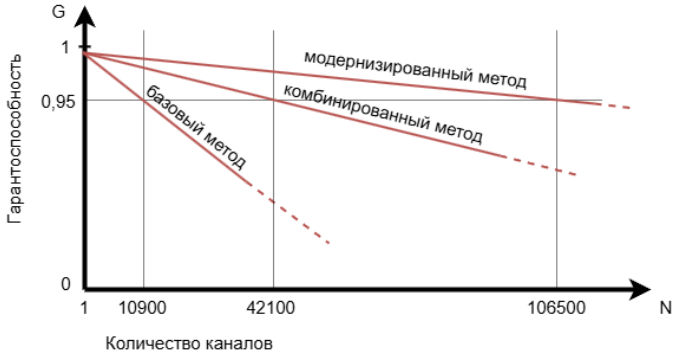


Рис. 9. Зависимость уровня гарантоспособности от количества каналов

Из графика видно, что заданный уровень гарантоспособности – 0,95, программа, реализующая модернизированный метод, обеспечивает уровень при числе каналов 106500.

Заключение. Разработан комбинированный метод, включающий алгоритмы для обнаружения и парирования потенциальных аварийных ситуаций в системе передачи данных. Внедрение комбинированного метода позволило добиться четырёхкратного роста гарантоспособности программного комплекса по сравнению с традиционными решениями, обеспечивая заданный уровень гарантоспособности 0,95 при 42100 каналов.

В связи с развитием систем с ФАР возникла потребность в обработке ещё большего количества каналов, что потребовало дальнейшей модернизации метода. В модернизированном методе были усовершенствованы алгоритмы обнаружения и парирования аварийных ситуаций и добавлены новые алгоритмы для обработки типов ошибок, которые становились критичными при масштабировании системы. После модернизации метод продемонстрировал способность обеспечить уровень гарантоспособности 0,95 с доверительным интервалом шесть часов при работе с 106500 каналов. Это позволит создать более совершенные системы с ФАР, отвечающие современным требованиям.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Воскресенский Д.И., Гостюхин В.О., Максимов В.М., Пономарев Л.И.* Устройства СВЧ и антенны / под ред. Д.И. Воскресенского. – 2-е, изд. доп. и перераб. – М.: Радиотехника, 2006. – 376 с.
2. *Фомин А.Н., Тяпкин В.Н., Дмитриев Д.Д.* Теоретические и физические основы радиолокации и специального мониторинга: учебник / под ред. Ищук И.Н. – Красноярск: СФУ, 2016. – 292 с.

3. *Савочкин И.А., Тройников Г.М., Тройникова Н.С., Турлаков П.В.* Система единого времени для высокоточной синхронизации разнесённых радиолокационных постов // Вестник Концерна ВКО «Алмаз – Антей». – 2014. – № 2. – С. 49-53.
4. *Страшун Ю.П.* Протокол точного времени Ртр для обеспечения работы АСУТП в режиме жесткого реального времени // ГИАБ. – 2014. – №S. – URL: https://cyberleninka.ru/article/n/protokol-tochnogo-vremeni-rtr-dlya-obespecheniya-raboty-asutp-v-rezhime-zhestkogo-realnogo-vremeni-2 (дата обращения: 31.03.2025).
5. *Сухман С.М., Бернов А.В., Шевкопляс Б.В.* Синхронизация в телекоммуникационных системах: Анализ инженерных решений. – М.: Эко-Трендз, 2002. – 268 с.
6. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – 4-е изд. – СПб.: Питер, 2006. – 672 с.
7. *Горобец А.В., Суков С.А., Триас Ф.Х.* Проблемы использования современных суперкомпьютеров при численном моделировании в гидродинамике и аэроакустике // Ученые записки ЦАГИ. – 2010. – № 2. – URL: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-sovremennyh-superkompyuterov-pri-chislennom-modelirovanii-v-gidrodinamike-i-aeroakustike (дата обращения: 25.10.2024).
8. *Хаханов В.И., Обризан В.И., Мельникова О.В.* Обзор международного рынка электронных технологий // Вестник НТУ ХПИ. – 2004. – № 46. – URL: https://cyberleninka.ru/article/n/obzor-mezhdunarodnogo-rynka-elektronnyh-tehnologiy (дата обращения: 25.10.2024).
9. *Каляев И.А., Левин И.И., Семерников Е.А.* Высокопроизводительные реконфигурируемые вычислительные системы для цифровой обработки сигналов // Тр. Российского научно-технического общества радиотехники, электроники и связи имени А.С. Попова. Серия: Цифровая обработка сигналов и ее применение. – 2010. – Вып. XII – 1. – С. 13-18.
10. *Чкан А.В.* Повышение реальной производительности РВС при решении задач цифровой обработки изображений с использованием быстрого преобразования Фурье // Известия ЮФУ. Технические науки. – 2020. – № 7 (217). – URL: https://cyberleninka.ru/article/n/povyshenie-realnoy-proizvoditelnosti-rvs-pri-reshenii-zadach-tsifrovoy-obrabotki-izobrazheniy-s-ispolzovaniem-bystrogo (дата обращения: 25.10.2024).
11. *Дордопуло А.И., Каляев И.А., Левин И.И., Семерников Е.А*. Высокопроизводительные многопроцессорные системы с реконфигурируемой архитектурой для цифровой обработки сигналов // Вестник Концерна ПВО «Алмаз-Антей». – 2011. – № 2 (6). – С. 88-104.
12. *Куан И.А., Азимбаев Д.Ж., Щербаченя А.Н., Гербер А.С.* Волоконно-оптические линии связи // Вестник науки. – 2018. – № 5 (5). – URL: https://cyberleninka.ru/article/n/volokonno-opticheskie-linii-svyazi (дата обращения: 25.10.2024).
13. *Пятибратов А.П., Гудыно Л.П., Кириченко А.А.* П99 Вычислительные системы, сети и телекоммуникации: учебник. – 2-е изд., перераб. и доп. / под ред. А.П. Пятибратова. – М.: Финансы и статистика, 2004. – 512 с.
14. *Клименко С.В., Яковлев В.В., Благовещенская Е.А.* Исследование реализаций алгоритмов контрольной суммы CRC32 // Известия Петербургского университета путей сообщения. – 2018. – № 3. – URL: https://cyberleninka.ru/article/n/issledovanie-realizatsiy-algoritmov-kontrolnoy-summy-crc32 (дата обращения: 31.03.2025).
15. *Соловьев В.В.* Архитектуры ПЛИС фирмы Xilinx: CPLD и FPGA 7-й серии. – М.: Горячая линия – Телеком, 2019. – 392 с.
16. *Avizienis A., Laprie J., Randell B., Landwehr C.* Basic concepts and taxonomy of dependable and secure computing // IEEE Transactions on Dependable and Secure Computing. – 2004. – No. 1. – P. 11-33.
17. *Муха Ар А.* Количественная оценка уровня гарантоспособности компьютерных систем // ММС. – 2019. – № 4. – URL: https://cyberleninka.ru/article/n/kolichestvennaya-otsenka-urovnya-garantosposobnosti-kompyuternyh-sistem (дата обращения: 31.03.2025).
18. *Вениаминов С.С.* Космический мусор угрожает планете // Воздушно-космическая сфера. – 2016. – № 1 (86). – URL: https://cyberleninka.ru/article/n/kosmicheskiy-musor-ugrozhaet-planete (дата обращения: 24.07.2024).
19. *Клюшников В.Ю.* Синдром Кесслера: будет ли закрыта дорога в космос? // ВКС. – 2021. – № 4 (109). – URL: https://cyberleninka.ru/article/n/sindrom-kesslera-budet-li-zakryta-doroga-v-kosmos (дата обращения: 25.10.2024).
20. *Дзюба А.П.* Перспективы развития фазированных антенных решеток // Вестник ДГТУ. Технические науки. – 2013. – № 3. – URL: https://cyberleninka.ru/article/n/perspektivy-razvitiya-fazirovannyh-antennyh-reshetok (дата обращения: 25.10.2024).

REFERENCES

1. *Voskresenskiy D.I., Gostyukhin V.O., Maksimov V.M., Ponomarev L.I.* Ustroystva SVCh i antenny [Microwave devices and antennas], ed. by D.I. Voskresenskogo. 2nd ed. Moscow: Radiotekhnika, 2006, 376 p.
2. *Fomin A.N., Tyapkin V.N., Dmitriev D.D.* Teoreticheskie i fizicheskie osnovy radiolokatsii i spetsial'nogo monitoringa: uchebnik [Theoretical and physical foundations of radar and special monitoring: textbook], ed. by Ishchuk I.N. Krasnoyarsk: SFU, 2016, 292 p.
3. *Savochkin I.A., Troynikov G.M., Troynikova N.S., Turlakov P.V.* Sistema edinogo vremeni dlya vysokotochnoy sinkhronizatsii raznesennykh radiolokatsionnykh postov [Unified time system for high-precision synchronization of distributed radar posts], *Vestnik Kontserna VKO «Almaz – Antey»* [Bulletin of the Almaz-Antey Air and Space Defense Concern], 2014, No. 2, pp. 49-53.
4. *Strashun Yu.P.* Protokol tochnogo vremeni Rtr dlya obespecheniya raboty ASUTP v rezhime zhestkogo real'nogo vremeni [Precise time protocol Rtr for ensuring the operation of automated process control systems in hard real time mode], *GIAB* [Mountain Information and Analytical Bulletin], 2014, No. S. Available at: https://cyberleninka.ru/article/n/protokol-tochnogo-vremeni-rtr-dlya-obespecheniya-raboty-asutp-v-rezhime-zhestkogo-realnogo-vremeni-2 (accessed 31 March 2025).
5. *Sukhman S.M., Bernov A.V., Shevkoplyas B.V.* Sinkhronizatsiya v telekommunikatsionnykh sistemakh: Analiz inzhenernykh resheniy [Synchronization in telecommunication systems: Analysis of engineering solutions]. Moscow: Eko-Trendz, 2002, 268 p.
6. *Olifer V., Olifer N.* Komp'yuternye seti. Printsipy, tekhnologii, protokoly: uchebnik dlya vuzov [Computer networks. Principles, technologies, protocols: textbook for universities]. 4th ed. Saint. Petersburg: Piter, 2006, 672 p.
7. *Gorobets A.V., Sukov S.A., Trias F.Kh.* Problemy ispol'zovaniya sovremennykh superkomp'yuterov pri chislennom modelirovanii v gidrodinamike i aeroakustike [Problems of using modern supercomputers in numerical modeling in hydrodynamics and aeroacoustics], *Uchenye zapiski TsAGI* [Scientific notes of TsAGI], 2010, No. 2. Available at: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-sovremennyh-superkompyuterov-pri-chislennom-modelirovanii-v-gidrodinamike-i-aeroakustike (accessed 25 October 2024).
8. *Khakhanov V.I., Obrizan V.I., Mel'nikova O.V.* Obzor mezhdunarodnogo rynka elektronnykh tekhnologiy [Review of the international market of electronic technologies], *Vestnik NTU KhPI* [Bulletin of NTU KhPI], 2004, No. 46. Available at: https://cyberleninka.ru/article/n/obzor-mezhdunarodnogo-rynka-elektronnyh-tehnologiy (accessed 25 October 2024).
9. *Kalyaev I.A., Levin I.I., Semernikov E.A*. Vysokoproizvoditel'nye rekonfiguriruemye vychislitel'nye sistemy dlya tsifrovoy obrabotki signalov [High-performance reconfigurable computing systems for digital signal processing], *Tr. Rossiyskogo nauchno-tekhnicheskogo obshchestva radiotekhniki, elektroniki i svyazi imeni A.S. Popova. Seriya: Tsifrovaya obrabotka signalov i ee primenenie* [Proceedings of the Russian Scientific and Technical Society of Radio Engineering, Electronics and Communications named after A.S. Popov. Series: Digital signal processing and its application], 2010, Issue XII – 1, pp. 13-18.
10. *Chkan A.V.* Povyshenie real'noy proizvoditel'nosti RVS pri reshenii zadach tsifrovoy obrabotki izobrazheniy s ispol'zovaniem bystrogo preobrazovaniya Fur'e [Improving the real performance of RCS in solving digital image processing problems using the fast Fourier transform], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2020, No. 7 (217). Available at: https://cyberleninka.ru/article/n/povyshenie-realnoy-proizvoditelnosti-rvs-pri-reshenii-zadach-tsifrovoy-obrabotki-izobrazheniy-s-ispolzovaniem-bystrogo (accessed 25 October 2024).
11. *Dordopulo A.I., Kalyaev I.A., Levin I.I., Semernikov E.A.* Vysokoproizvoditel'nye mnogoprotsessornye sistemy s rekonfiguriruemoy arkhitekturoy dlya tsifrovoy obrabotki signalov [High-performance multiprocessor systems with reconfigurable architecture for digital signal processing], *Vestnik Kontserna PVO «Almaz-Antey»* [Bulletin of the Almaz-Antey Air Defense Concern], 2011, No. 2 (6), pp. 88-104.
12. *Kuan I.A., Azimbaev D.Zh., Shcherbachenya A.N., Gerber A.S.* Volokonno-opticheskie linii svyazi [Fiber-optic communication lines], *Vestnik nauki* [Bulletin of Science], 2018, No. 5 (5). Available at: https://cyberleninka.ru/article/n/volokonno-opticheskie-linii-svyazi (accessed 25 October 2024).
13. *Pyatibratov A.P., Gudyno L.P., Kirichenko A.A.* P99 Vychislitel'nye sistemy, seti i telekommunikatsii: uchebnik [P99 Computing systems, networks and telecommunications: textbook]. 2nd ed., ed by. A.P. Pyatibratova. Moscow.: Finansy i statistika, 2004, 512 p.
14. *Klimenko S.V., Yakovlev V.V., Blagoveshchenskaya E.A.* Issledovanie realizatsiy algoritmov kontrol'noy summy CRC32 [Study of implementations of CRC32 checksum algorithms], *Izvestiya Peterburgskogo universiteta putey soobshcheniya* [Bulletin of the Petersburg University of Railway Engineering], 2018, No. 3. Available at: https://cyberleninka.ru/article/n/issledovanie-realizatsiy-algoritmov-kontrolnoy-summy-crc32 (accessed 31 March 2025).

15. *Solov'ev V.V.* Arkhitektury PLIS firmy Xilinx: CPLD i FPGA 7-y serii [Xilinx FPGA architectures: CPLD and FPGA 7th series]. Moscow: Goryachaya liniya – Telekom, 2019, 392 p.
16. *Avizienis A., Laprie J., Randell B., Landwehr C.* Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing,* 2004, No. 1, pp. 11-33.
17. *Mukha Ar A.* Kolichestvennaya otsenka urovnya garantosposobnosti komp'yuternykh sistem [Quantitative assessment of the level of guarantee capacity of computer systems], *MMS* [MMS], 2019, No. 4. Available at: https://cyberleninka.ru/article/n/kolichestvennaya-otsenka-urovnya-garantosposobnosti-kompyuternyh-sistem (accessed 31 March 2025).
18. *Veniaminov S.S.* Kosmicheskiy musor ugrozhaet planete [Space debris threatens the planet], *Vozdushno-kosmicheskaya sfera* [Air and space sphere], 2016, No. 1 (86). Available at: https://cyberleninka.ru/article/n/kosmicheskiy-musor-ugrozhaet-planete (accessed 24 July 2024).
19. *Klyushnikov V.Yu.* Sindrom Kesslera: budet li zakryta doroga v kosmos? [Kessler syndrome: will the road to space be closed?], *VKS* [VKS], 2021, No. 4 (109). Available at: https://cyberleninka.ru/article/n/sindrom-kesslera-budet-li-zakryta-doroga-v-kosmos (accessed 25 October 2024).
20. *Dzyuba A.P.* Perspektivy razvitiya fazirovannykh antennykh reshetok [Prospects for the development of phased antenna arrays], *Vestnik DGTU. Tekhnicheskie nauki* [Bulletin of DSTU. Technical sciences], 2013, No. 3. Available at: https://cyberleninka.ru/article/n/perspektivy-razvitiya-fazirovannyh-antennyh-reshetok (accessed 25 October 2024).

Левин Илья Израилевич – Южный федеральный университет; e-mail: levin@superevm.ru; г. Таганрог, Россия; тел.: +78634612111; кафедра интеллектуальных и многопроцессорных систем; зав. кафедрой; д.т.н.; профессор.

Буряков Дмитрий Сергеевич – Южный федеральный университет; e-mail: dburiakov@sfedu.ru; г. Таганрог, Россия; тел.: +79198955502; кафедра интеллектуальных и многопроцессорных систем; аспирант.

Levin Ilya Izrailevich – Southern Federal University; e-mail: levin@superevm.ru; Taganrog, Russia; phone: +78634612111; the Department of Intelligent and Multiprocessor Systems; head of department; dr. of eng. sc.; professor.

Buryakov Dmitrii Sergeevich – Southern Federal University; e-mail: dburiakov@sfedu.ru; Taganrog, Russia; phone: +79198955502; the Department of Intelligent and Multiprocessor Systems; postgraduate student.

УДК 004.932.75'1 DOI 10.18522/2311-3103-2025-3-134-144

Д.А. Безуглов, М.С. Мищенко, С.Е. Мищенко

АЛГОРИТМ ПОДГОТОВКИ ДАННЫХ ОБУЧЕНИЯ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РАСПОЗНАВАНИЯ БУКВ И СИМВОЛОВ

Точность распознавания текстовых изображений на практике остается ограниченной. Это связано с тем, что в алфавит символов могут входить строчные и прописные буквы со схожим начертанием, а также составные символы, образованные из нескольких более простых символов. Для решения этой проблемы систему распознавания символов дополняют системами семантического или структурного анализа, что существенно усложняет информационную систему для распознавания текста. В настоящее время для распознавания одиночных символов широко применяют сверточные нейронные сети, для обучения которых используют базу данных с изображениями распознаваемых символов. В работе предложен алгоритм, отличающийся тем, что в изображение одиночного символа для обучающей выборки включают фрагменты символов, которые могут быть расположены в строке в непосредственной близости от распознаваемого символа. Формирование изображений для обучающей выборки имитирует процесс сегментации символа по яркости, который обычно используют при выделении символа для дальнейшего распознавания. При этом оценивают размеры символа, дополняют его изображениями соседних символов, а затем оценивают размеры области, изображения, которое будет помещено в обучающую выборку. Полученное изображение масштабируют и обрезают таким образом, чтобы на вход нейронной сети поступали изображения заданного размера. В работе для распознавания алфавита символов, включающего прописные и строчные символы русского и английского алфавитов, цифры, символы

и знаки препинания предложено использовать множество сверточных нейронных сетей, каждая из которых обучена распознавать один символ. Выбор символа осуществляется путем сравнения откликов всех нейронных сетей и выбора максимального отклика. Проведено сравнение предложенного алгоритма подготовки данных для обучения с известным алгоритмом, основанным на использовании изображений одиночных символов. Установлено, что предложенный алгоритм подготовки данных для обучения обеспечивает повышение точности распознавания алфавита из 138 символов более, чем в два раза.

Алгоритм; алфавит; символ; распознавание; сверточная нейронная сеть; обучающая выборка.

D.A. Bezuglov, M.S. Mishchenko, S.E. Mishchenko

ALGORITHM FOR TRAINING DATA PREPARATION OF CONVOLUTIONAL NEURAL NETWORKS FOR LETTER AND CHARACTER RECOGNITION

The accuracy of text image recognition remains limited in practice. This is due to the fact that the alphabet of symbols can include lowercase and uppercase letters with a similar font, as well as composite characters formed from several simpler characters. To solve this problem, the character recognition system is supplemented with semantic or structural analysis systems, which significantly complicates the information system for text recognition. Currently, convolutional neural networks are widely used for recognizing single characters, for which a database with images of recognized characters is used for training. The paper proposes an algorithm characterized in that the image of a single character for a training sample includes fragments of characters that can be located in a line in close proximity to the recognized character. This allows you to expand the set of images for training and additionally include information in the image about the placement of the symbol in the string, its relative size and whether this symbol is composite. The formation of images for the training sample simulates the process of segmentation of a symbol by brightness, which is usually used when selecting a symbol for further recognition. At the same time, the size of the symbol is estimated, it is supplemented with images of neighboring symbols, and then the size of the area, the image that will be placed in the training sample, is estimated. The resulting image is scaled and cropped in such a way that images of a given size are received at the input of the neural network. In the work, to recognize the alphabet of symbols, including uppercase and lowercase characters of the Russian and English alphabets, numbers, symbols and punctuation marks, it is proposed to use a variety of convolutional neural networks, each of which is trained to recognize one character. The symbol is selected by comparing the responses of all neural networks and selecting the maximum response. The proposed algorithm for training data preparation is compared with a well-known algorithm based on the use of images of single characters. It is established that the proposed algorithm for preparing data for training provides an increase in the accuracy of recognizing the alphabet of 138 characters by more than two times.

Algorithm; alphabet; symbol; recognition; convolutional neural network; training sample.

Введение. Распознавание символов на изображениях представляет собой одну из первых задач теории распознавания образов, которая начала интенсивно развиваться со второй половины 50-х годов [1] и была связана с созданием машинного зрения и читающих автоматов. В 1957г. Ф. Розенблатом был предложен подход к распознаванию образов на основе персептрона [1], что послужило отправной точкой для создания современных сверточных нейронных сетей (СНС), способных распознавать символы и тексты [2–5]. В настоящее время системы распознавания текстовых изображений применяют при автоматическом переводе, для распознавания автомобильных номеров, регистрации железнодорожных составов [6–9]. Эффективность распознавания текстов значительно зависит от многих факторов. К их числу могут быть отнесены искажения при проецировании трехмерных объектов с текстовой информацией на плоскость, шумы, турбулентность атмосферы, разрешение текстового документа при сканировании. В результате в теории и практике распознавания текстов сложилось противоречие. С одной стороны, обучить СНС распознавать одиночные символы не сложно. При этом точность распознавания может достигать 99%. Однако, с другой стороны, при извлечении символов из текста приходится строить сложные классификаторы, которые анализируют различные дополнительные признаки, учитывающие контекстное содержание документа. Это

значительно усложняет систему распознавания текстов, а точность распознавания может снижаться приблизительно до 80% [8]. В информационных системах распознавания текстов с высокой стоимостью ошибки (в государственных или экономических структурах) системы распознавания текстов требуют участия оператора для контроля за корректностью работы искусственной нейронной сети (ИНС).

В известной литературе, посвященной глубокому обучению классическим примером является структура СНС, обеспечивающая распознавание рукописных изображений цифр [2, 10]. Цифр всего 10, они имеют одинаковую высоту кегля. Это позволяет использовать достаточно простой классификатор, состоящий из двух чередующихся сверточных слоев и слоев агрегирования, а также полносвязной нейронной сети с 10-ю выходами. На вход классификатора поступают изображения размером 32x32 или 28x28 пикселей. Примеры программной реализации подобных классификаторов известны и ссылаются на уже готовые базы для обучения [10].

Недостатком такого классификатора является то, что при увеличении алфавита символов для распознавания сложность СНС должна возрастать. При расширении алфавита символов будет увеличиваться число выходов СНС. Следовательно, при этом потребуется переобучение всей СНС.

В связи с этим в работе [8] было предложено строить классификатор из множества нейронных сетей. Каждая нейронная сеть имеет единственный выход и обучена распознавать только один символ. После того, как символу ставятся в соответствие выходные сигналы всех нейронных сетей принимается решение о том, изображение какого символа поступало на вход.

В этом случае для решения задачи распознавания одного символа достаточно применить простейшую полносвязную сеть, состоящую из трех слоев (входного, скрытого и выходного). Число нейронов входного слоя соответствует длине входного вектора. В скрытом слое было предложено сократить число нейронов до 70% по сравнению со входным слоем. Выходной слой содержит один нейрон. Для упрощения нейронной сети вместо сверточных слоев было предложено использовать аппарат вейвлет-преобразований и метод главных компонент. В то же время очевидно, что использование данного математического аппарата было продиктовано необходимостью подавления импульсных шумов на изображении.

Авторы [11] указывали, что распознавание символов при помощи нейронных сетей сталкивается с трудностями при распознавании схожих по начертанию (строчных и прописных). В связи с этим при принятии решения учитывались два максимальных отклика множества нейронных сетей. Однако в работе [11] отсутствует подробное описание этой части работы алгоритма.

В работе [11] также указывалось, что в ряде случаев при распознавании текстов могут возникать сложности распознавания некоторых символов, которые сложно разделить, используя обычную сегментацию по яркости.

Наконец, требуется отметить известную проблему распознавания составных символов, распознавание которых потребует использования контекстных анализаторов [3, 12–15].

Цель работы состоит в повышении точности распознавания текстовых документов при помощи ИНС без дополнения системы распознавания текстов контекстными или иными дополнительными классификаторами.

Алгоритм подготовки данных для распознавания символов и формирования обучающей выборки. На наш взгляд, проблемы с распознаванием текстов в работах [8, 11] были связаны не с общим подходом к построению к классификатора, а с подготовкой данных для обучения. В связи с этим для распознавания текста на изображении будем использовать множество идентичных СНС, структура которых показана на рис. 1.

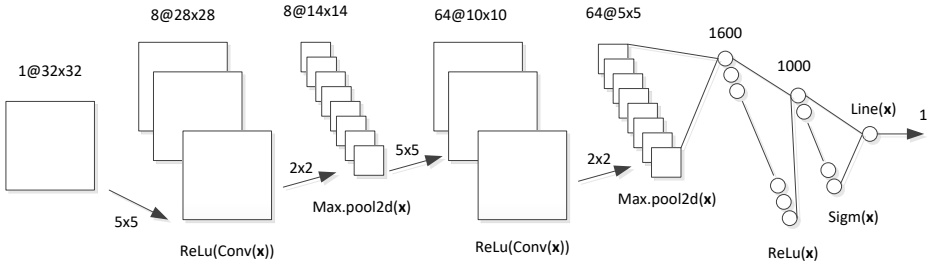


Рис. 1. Структура СНС для распознавания символа

Поступающее на вход классификатора изображение получает набор откликов всех нейронных сетей (см. рис. 1), из которых выбирают сеть с максимальным откликом. Поскольку выбранная СНС обучена распознавать единственный символ, то решение о выборе символа становится однозначным.

В соответствии с работой [8] для формирования обучающей выборки и проведения экспериментов с распознаванием использовались файлы шрифтов. Известно, что файлы шрифтов операционной системы содержат векторные изображения символов шрифта. При формировании растрового изображения, выводимого на экран, задают H_0 размер (высоту) кегля символа, что позволяет требуемым образом масштабировать векторное изображение символа. Отметим, что в отличие от типографской печати ширина кегля символа может варьироваться. В результате при подготовке символа задавалось имя шрифта и высота кегля. Далее изображение масштабировалось до необходимого размера. При необходимости к изображению добавляются пустые строки и столбцы.

При работе с ИНС входное изображение символа помещают в центр квадратной области размером $L \times L$ (как правило, $L = 32$ или 28 [8]). При этом, если $H_0 < L$, изображение символа масштабируют с коэффициентом C так, что $L \approx \lfloor H_0 \rfloor \le L$ (здесь $\lfloor H_0 \rfloor$ обозначает операцию округления).

Это позволяет формировать обучающую выборку из изображений символа одного и того же шрифта с разными значениями H_0. Расширения вариаций изображений символа в обучающей выборке также добиваются использованием нескольких шрифтов с различными стилями (могут использоваться шрифты с засечками и без, нормальные и жирные начертания символа). В работе [8] для формирования обучающей выборки использовались 10 размеров кегля от 12 до 36, 8 шрифтов (4 без засечек и 4 с засечками), а также гарнитуры с нормальным и жирным представлением символа. В результате каждому символу можно было поставить в соответствие 160 изображений. Обучающая выборка состоит из нескольких тысяч изображений, в которой число изображений распознаваемого символа приблизительно равно числу других изображений символов.

В качестве примера на рис. 2 приведены примеры изображений символа «А» с высотой кегля 24 и 12, извлекаемые из файла шрифта arial.ttf и преобразуемые до изображения заданного размера. Как видно из данного рисунка, изменение размеров кегля позволяет варьировать изображение символа, для создания обучающей выборки.

Недостаток такого подхода становится очевиден, если формировать изображения символов не из файла шрифта, а из изображения с текстом. В этом случае понятие высоты кегля не может быть использовано. После сегментации символа из текста он имеет высоту и ширину, которые обозначим h_0, w_0. На самом деле эти размеры могут отличаться от размеров символа и соответствовать его части. Дело в том, что при сегментации по яркости или при помощи других алгоритмов [16–18] вместо символа «Й» можно получить изображение «И», а вместо символа «Ы» – только «Ь» или «І». Большие сложности могут возникнуть при выделении небольших по высоте элементов, например «.».

В этом случае вероятна ошибка в выборе коэффициента масштабирования C. Эта ошибка, скорее всего, приведет к ошибке распознавания символа. Для разрешения данных проблем в систему распознавания приходится внедрять сложную многоуровневую логическую или контекстную обработку.

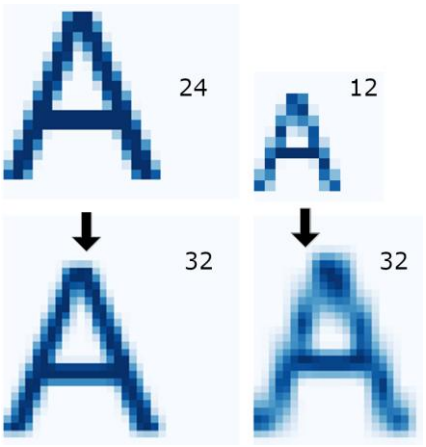


Рис. 2. Преобразование изображений различной высоты в стандартное изображение 32x32 пикселя

В работе предлагается при формировании входного изображения для распознавания и обучения СНС использовать следующий алгоритм.

1. Выполним сегментацию изображения и выделим фрагмент символа с размерами h_0, w_0. Массив соответствующего изображения обозначим $\mathbf{b}_0$. Изображение $\mathbf{b}_0$ содержит яркие точки, пустые строки и столбцы по краям изображения отсутствуют. Если символ составной, то выделенный фрагмент должен занимать наибольшую площадь.

В качестве примера на рис. 3 показан процесс выделения фрагмента составного символа «Й» с исходным размером 24. Параметры фрагмента символа $h_0 = 17, w_0 = 15$. Отметим, что высота исходного изображения всего символа больше на 4 пикселя.

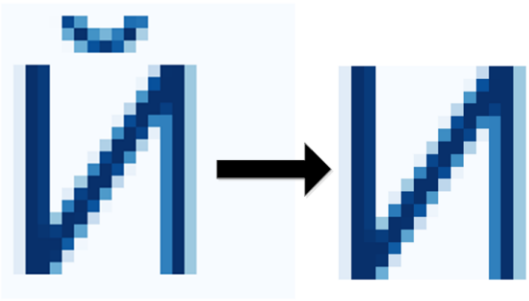


Рис. 3. Сегментация фрагмента символа, занимающего максимальную площадь

2. Дополним изображение $\mathbf{b}_0$ с размерами h_0, w_0 так, чтобы получить новое изображение $\mathbf{b}_1$ с размерами h_1, w_1. Изображение $\mathbf{b}_1$ должно быть размещено в центральной области изображения $\mathbf{b}_1$, высота h_1 должна быть выбрана таким образом, чтобы в новое изображение не попали целые изображения символов из текстовых строк над и под символом, но были включены все элементы символа, которые могли быть утеряны при сегментации по яркости. По всей видимости достаточно задать $h_1 = 1.5h_0 ... 2h_0$. Несколь-

ко сложнее с выбором w_1. Минимальная ширина символа может занимать несколько пикселей, а максимальная – совпадать с его высотой. В связи с этим данный параметр предлагается выбирать из соотношения $w_1 = 9w_0$.

На рис. 4 представлено изображение символа «Й», размещенного между двумя другими символами, выбранными случайным образом.

Рис. 4. Изображение символа «Й» в окружении случайно выбранных символов

3. Далее определим высоту прямоугольной области h_2, которая содержит все яркие точки изображения $\mathbf{b}_1$.

4. Выделим центральную квадратную область изображения, включающую $\mathbf{b}_0$, но имеющую высоту и ширину, равные h_2. В результате того, что расширенное изображение в тексте сможет захватить фрагменты изображений соседних символов получим более корректную дополнительную информацию о фактической высоте символа и его положении на кегле.

5. Масштабируем изображение так, чтобы $\lfloor Ch_2 \rfloor = L$. В результате будет получено изображение для распознавания, показанное на рис. 5.

Особенность изображения состоит в том, что по краям изображение «зашумляется» фрагментами соседних символов, но содержит все необходимые фрагменты, образующие символ. Соседние символы несут информацию о высоте буквы, что позволяет корректно идентифицировать ее положение в строке.

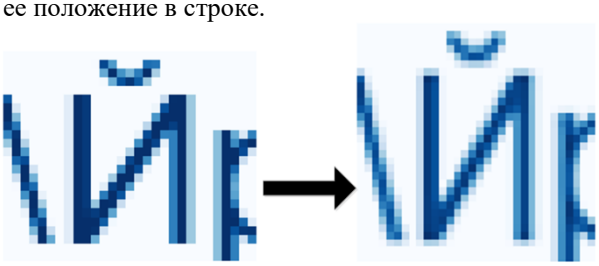


Рис. 5. Вариация изображения символа «Й», помещаемая в обучающую выборку

Предлагаемый алгоритм используется только для распознавания при извлечении символа из изображения. Для формирования обучающей выборки вместо расширения изображения символа и перехода от изображения $\mathbf{b}_0$ к $\mathbf{b}_1$ предлагается случайным образом генерировать изображения соседних символов текста, которые попадают в изображение для обучения. Вариации изображений символа будут включать в себя выбранные шрифты, гарнитуры, размеры символов и варианты фрагментов соседних символов. Естественно, что число вариантов изображений одного и того же символа может значи-

тельно увеличиться. Это приведет к необходимости увеличения обучающей выборки. При этом фрагменты соседних символов, попадающих в обучающую выборку должны в результате обучения восприниматься не только как шум, но и как дополнительная информация о положении символа в строке и, соответственно, на кегле.

Численные эксперименты. Предложенный алгоритм обучения был использован для подготовки данных для обучения СНС, представленной на рис. 1. При обучении СНС с данными, подготовленными по известной процедуре каждый символ варьировался 64 изображениями. Общее число символов включало в свой состав 138 символов (основные символы – 29, строчные и прописные символы русского алфавита – по 33 символа), 15 прописных и 18 строчных символов английского алфавита, отличающихся по начертанию от русских букв, а также 10 цифр. Перечень символов приведен в таблице 1.

Для обучения использовались 8 шрифтов: arial.ttf, arialbd.ttf, calibri.ttf, calibrib.ttf, cour.ttf, courbd.ttf, times.ttf, timesbd.ttf с размерами, 12, 16, 18, 20, 22, 24, 26, 32. При формировании обучающей базы изображений по предлагаемому алгоритму число сгенерированных изображений возросло в 10 раз.

Таблица 1

Перечень символов для распознавания

Группа символов	Символы
Прописные русские буквы	'А','Б','В','Г','Д','Е','Ё','Ж','З','И','Й','К','Л','М', 'Н','О','П','Р','С','Т','У','Ф','Х','Ц','Ч','Ш','Щ','Ъ', 'Ы','Ъ','Э','Ю','Я'
Строчные русские буквы	'а','б','в','г','д','е','ё','ж','з','и','й','к','л','м','н','о','п','р', 'с','т','у','ф','х','ц','ч','ш','щ','ь','ъ','ы','э','ю','я'
Символы и знаки препинания	'~','!','@','#','$','^','&','*','(',')','+','-','=','[',']','{','}','\\', '|','<','>','/','?',';',':',',',',.','№','%'
Цифры	'1','2','3','4','5','6','7','8','9','0'
Прописные английские буквы	'Q','W','R','Y','U','I','J','S','D','F','G','L','Z','V','N'
Строчные английские буквы	'q','w','r','t','i','j','s','d','f','g','h','k','l','z','v','b','n','m'

Модель СНС была реализована на языке Python с использованием фреймворка PyTorch [19, 20]. При обучении использовался оптимизатор Adam с параметром 0.001. Время обучения всех нейронных сетей для первого и второго набора данных отличалось приблизительно в 10 раз и для подготовленных данных по предлагаемому алгоритму составило около 12 часов. При обучении использовалось до 200 эпох обучения для каждого символа. При обучении использовались обучающая и тестовые выборки, разделенные по объему в соотношении 70% и 30%. Тестовая выборка использовалась для контроля переобучения. При этом в качестве критерия остановки процесса обучения использовалось монотонное удаление качества сети по тестовой выборке в течение 8-ми эпох обучения. При достижении предельного числа эпох или обнаружения переобучения сети использовались коэффициенты СНС, при которых качество сети на тестовых данных было наилучшим.

После обучения был проведен эксперимент по распознаванию символов с использованием двух вариантов обучения при распознавании символов, генерируемых с использованием шрифта calibril.ttf, cambriab.ttf. Перечень ошибок распознавания приведен в табл. 2.

Таблица 2

Перечень ошибок при распознавании

Данные для обучения	Шрифт	Число ошибок (процент ошибок)	Не распознанные символы
Одиночные символы	cambriab.ttf	53 (38%)	'(', '+', '=', ']', '|', '<', '>', '/', ';', '.', '№', '%', 'В', 'Г', 'Д', 'Ё', 'Й', 'О', 'П', 'У', 'Х', 'Ц', 'Ш', 'Ы', 'Э', 'б','е', 'ё', 'ж', 'и', 'о', 'ч', 'ш', 'э', 'Q', 'Y', 'U', 'I', 'J', 'F', 'G', 'q', 'r', 'i', 's', 'l', 'v', 'ь', '3', '5', '7', '8', '0'
	calibril.ttf	20 (14%)	'=', ']', '|', ';', ',', '№', '%', 'Ё', 'З', 'Й', 'Щ', 'Ь', 'Ы', 'г', 'ё', 'й', 'р', 'ы', 'Q', 'I'
Предлагаемый алгоритм	cambriab.ttf	21 (15%)	'~', '+', ';', '.', '№', 'Д', 'Л', 'О', 'Ц', 'Ш', 'Ы', 'Ю', 'б', 'ш', 'W', 'J', 'Z', '3', '5', '8', '9'
	calibril.ttf	9 (5%)	'№', 'З', 'Ы', 'к', 'о', 'ы', 'I', 'l', '3'

Анализ результатов в табл. 2 показывает, что в некоторых случаях использование СНС, обученных для распознавания одиночных символов, позволяет правильно распознать составные символы. Такой результат может иметь место в том случае, если при одном и том же входном сигнале отклик СНС близок. Однако в этом случае результат распознавания можно считать неустойчивым. Это подтверждают зависимости, приведенные на рис. 6 и 7. На рис. 6 приведены отклики СНС при распознавании символов, в которых допущена ошибка. На рис. 7, напротив, обе сети распознали символ. Кривая 1 на рис. 6 и 7 соответствует обучению СНС на одиночных символах, а кривая 2 при подготовке данных для обучения предлагаемым алгоритмом. Данные штриховой кривой показывают, что буква «Ы» (номер 57) перепутана с символами «о», «Ь», «b» – номера 77, 56, 125 в порядке убывания по амплитуде. Сплошная кривая предлагает два наиболее вероятных кандидата для распознавания и перепутала «Ь» и букву «Ы». Возможно, эту неоднозначность можно устранить, если обучение производить на большем числе вариаций изображений символов. Как видно, несмотря на ошибку при распознавании составного символа «Ы», он является вторым кандидатом на распознавание. В то же время обучение по одиночным символам даже не предлагает такой вариант для распознавания. Для рассмотренных примеров число ошибок благодаря использованию предложенного алгоритма подготовки символов для распознавания сокращено более чем в 2 раза.

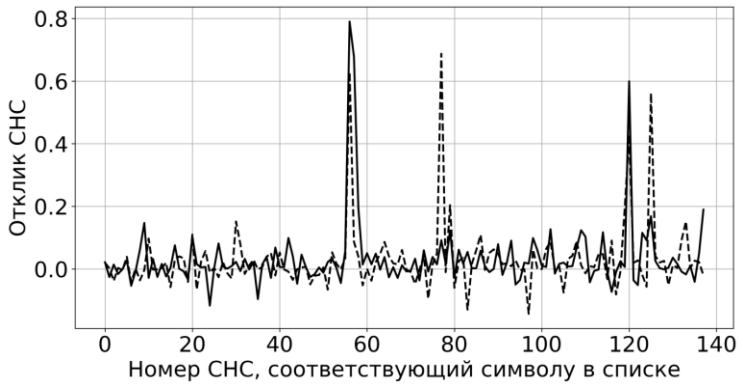


Рис. 6. Отклики СНС при неправильном распознавании символа «Ы» – номер 57: штриховая кривая – СНС обучена на одиночных символах, сплошная – предлагаемый алгоритм

Рис. 7 Отклики СНС при правильном распознавании символа «А» – номер 29: штриховая кривая – СНС обучена на одиночных символах, сплошная – СНС обучена после преобразования данных

Выводы. Таким образом, предложенный алгоритм подготовки символов для распознавания отличается от известных включением в формируемое изображение фрагментов других символов, соответствующих соседним символам в строке и фрагментов, расположенных от связного множества ярких точек символа, образующих основной по площади неразрывный фрагмент символа. Для рассмотренных примеров предлагаемый алгоритм обеспечивает сокращение числа ошибок более чем в 2 раза по сравнению с СНС, обученной для распознавания одиночных символов. Процент ошибок предлагаемого алгоритма находится в диапазоне от 15% до 5%, без использования предложенного алгоритма ошибки изменяются в диапазоне от 14% до 38%.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Горелик А.Л., Скрипкин В.А.* Методы распознавания. – М.: Высшая школа, 1984. – 208 с.
2. *Goodfellow I., Bengio Y., Courville A.* Deep Learning. – MIT Press, 2016. – httpp://www.deeplearningbook.org.
3. Патент РФ 2661750: МПК G06K 9/20. Распознавание символов с использованием искусственного интеллекта / *Чупинин Ю.Г.*; заявл. 30.05.2017; опубл. 19.07.2018; Бюл. № 20.
4. *Николенко С., Кадурин А., Архангельская Е.* Глубокое обучение. Погружение в мир нейронных сетей. – СПб.: Питер, 2021. – 476 с.
5. *Forsyth D.A., Ponce J.* Computer Vision: A Modern Approach. – 2nd ed. – New Jersey: Prentice Hall, 2011. – 792 p.
6. *Болотова Ю.А., Спицын В.Г., Рудомёткина М.Н.* Распознавание автомобильных номеров на основе метода связных компонент и иерархической временной сети // Компьютерная оптика. – 2015. – Т. 39, № 2. – С. 275-280.
7. *Казанский Н.Л., Попов С.Б.* Распределённая система технического зрения регистрации железнодорожных составов // Компьютерная оптика. – 2012. – Т. 36, № 3. – С. 419-428.
8. *Изотов П.Ю., Суханов С.В., Головашкин Д.Л.* Технология реализации нейросетевого алгоритма в среде CUDA на примере распознавания рукописных цифр // Компьютерная оптика. – 2010. – Т. 34, № 2. – С. 243-251.
9. *Спицын В.Г., Болотова Ю.А., Фан Н.Х., Буй Т.Т.Ч.* Применение вейвлет-преобразования Хаара, метода главных компонент и нейронных сетей для оптического распознавания символов на изображениях в присутствии импульсного шума // Компьютерная оптика. – 2016. – Т. 40, № 2. – С. 249-257. – DOI: 10.18287/2412-6179-2016-40-2-249-257.
10. *Загинайло М.В., Фатхи В.А.* Распознавание символов с помощью аппарата искусственных нейронных сетей // Инновации и инвестиции. – 2005. – № 5. – С. 145-147.
11. *Рашид Т.* Создаем нейронную сеть. – СПб.: ООО «Альфа-книга», 2017. – 272 с.
12. *Фан Н.Х., Буй Т.Т.Ч., Спицын В.Г.* Распознавание печатных текстов на основе применения вейвлет-преобразования и метода главных компонент // Известия Томского политехнического университета. – 2012. – Т 36, № 5. – С. 154-157.
13. *Miller E.G., Viola P.A.* Ambiguity and constraint in mathematical expression recognition // in AAAI-98/IAAI-98 Proceedings, July 26-30, 1998, Madison, Wisconsin: AAAI, 1998. – P. 784-791.

14. *Ong Kai Bin, Yew Kwang Hooi, Said Jadid Abdul Kadir, Haruhiro Fujita and Luqman Hakim Rosli*. Enhanced Symbol Recognition based on Advanced Data Augmentation for Engineering Diagrams // International Journal of Advanced Computer Science and Applications (IJACSA). – 2022. – 13 (5). – http://dx.doi.org/10.14569/IJACSA.2022.0130563.
15. *Bhanbhro H., Yew K.H., Kusakunniran W., Amur Z.* A Symbol Recognition System for Single-Line Diagrams Developed Using a Deep-Learning Approach // Applied Sciences. – 2023. – 13. – P. 8816. – https: // doi.org/10.3390/app13158816.
16. *Moreno-García, C.F.; Elyan, E.; Jayne, C.* Heuristics-Based Detection to Improve Text/Graphics Segmentation in Complex Engineering Drawings // In Proceedings of the Engineering Applications of Neural Networks: 18th International Conference (EANN 2017), Athens, Greece, 25–27 August 2017. – P. 87-98.
17. *Pratt W.K.* Digital image processing. – New York: Wiley, 1991. – 698 p.
18. *Muthukrishnan R, Radha M.* Contour selection algorithms for image segmentation // International Journal of Computer Science & Information Technology (IJCSIT). – 2014. –Vol. 3, No. 6. – P. 259-267.
19. *Пойнтер Я.* Программируем с PyTorch: Создание приложений глубокого обучения. – СПб.: Питер, 2020. – 256 с.
20. *Liu Yuxi (Hayden).* PyTorch 1.x Reinforcement Learning Cookbook. Over 60 recipes to design, develop, and deploy self-learning AI models using Python. – Birmingham–Mumbai: Packt, 2019. – 527 p.

REFERENCES

1. *Gorelik A.L., Skripkin V.A.* Metody raspoznavaniya [Recognition methods]. Moscow: Vysshaya shkola, 1984, 208 p.
2. *Goodfellow I., Bengio Y., Courville A.* Deep Learning. MIT Press, 2016. Available at: httpp: // www.deeplearningbook.org.
3. *Chupinin Yu.G.* Patent RF 2661750: MPK G06K 9/20. Raspoznavanie simvolov s ispol'zovaniem iskusstvennogo intellekta [Patent Ru No. 2661750, G06K 9/20. Character recognition using artificial intelligence]; Prior. 30.05.2017, Publ. 07/19/2018, Bul. No. 20.
4. *Nikolenko S., Kadurin A., Arkhangel'skaya E.* Glubokoe obuchenie. Pogruzhenie v mir neyronnykh setey [Deep learning. Dive into the world of neural networks]. Saint Petersburg: Piter, 2021, 476 p.
5. *Forsyth D.A., Ponce J.* Computer Vision: A Modern Approach. 2nd ed. New Jersey: Prentice Hall, 2011, 792 p.
6. *Bolotova Yu.A., Spitsyn V.G., Rudometkina M.N.* Raspoznavanie avtomobil'nykh nomerov na osnove metoda svyaznykh komponent i ierarkhicheskoy vremennoy seti [Recognition of license plates based on the method of connected components and a hierarchical time network], *Komp'yuternaya optika* [Computer Optics], 2015, Vol. 39, No. 2, pp. 275-280.
7. *Kazanskiy N.L., Popov S.B.* Raspredelennaya sistema tekhnicheskogo zreniya registratsii zheleznodorozhnykh sostavov [Distributed vision system for registration of railway trains], *Komp'yuternaya optika* [Computer Optics], 2012, Vol. 36, No. 3, pp. 419-428.
8. *Izotov P.Yu., Sukhanov S.V., Golovashkin D.L.* Tekhnologiya realizatsii neyrosetevogo algoritma v srede CUDA na primere raspoznavaniya rukopisnykh tsifr [The technology of implementing a neural network algorithm in the cuda environment using the example of handwriten digit recognition], *Komp'yuternaya optika* [Computer Optics], 2010, Vol. 34, No. 2, pp. 243-251.
9. *Spitsyn V.G., Bolotova Yu.A., Fan N.Kh., Buy T.T.Ch.* Primenenie veyvlet-preobrazovaniya Khaara, metoda glavnykh komponent i neyronnykh setey dlya opticheskogo raspoznavaniya simvolov na izobrazheniyakh v prisutstvii impul'snogo shuma [Application of the Haar wavelet transform, the principal component method and neural networks for optical character recognition in images in the presence of pulsed noise], *Komp'yuternaya optika* [Computer Optics], 2016, Vol. 40, No. 2, pp. 249-257. DOI: 10.18287/2412-6179-2016-40-2-249-257.
10. *Zaginaylo M.V., Fatkhi V.A.* Raspoznavanie simvolov s pomoshch'yu apparata iskusstvennykh neyronnykh setey [Character recognition using artificial neural networks], *Innovatsii i investitsii* [Innovations and Investments], 2005, No. 5, pp. 145-147.
11. *Rashid T.* Sozdaem neyronnuyu set' [Make your own neural network]. Saint Petersburg: OOO «Al'fakniga», 2017, 272 p.
12. *Fan N.Kh., Buy T.T.Ch., Spitsyn V.G.* Raspoznavanie pechatnykh tekstov na osnove primeneniya veyvlet-preobrazovaniya i metoda glavnykh komponent [Recognition of printed texts based on the application of the wavelet transform and the principal component method], *Izvestiya Tomskogo politekhnicheskogo universiteta* [Proceedings of Tomsk Polytechnic University], 2012, Vol. 36, No. 5, pp. 154-157.

13. *Miller E.G., Viola P.A.* Ambiguity and constraint in mathematical expression recognition, *in AAAI-98/IAAI-98 Proceedings, July 26-30, 1998, Madison, Wisconsin: AAAI, 1998,* pp. 784-791.
14. *Ong Kai Bin, Yew Kwang Hooi, Said Jadid Abdul Kadir, Haruhiro Fujita and Luqman Hakim Rosli.* Enhanced Symbol Recognition based on Advanced Data Augmentation for Engineering Diagrams, *International Journal of Advanced Computer Science and Applications (IJACSA),* 2022, 13 (5). Available at: http://dx.doi.org/10.14569/IJACSA.2022.0130563.
15. *Bhanbhro H., Yew K.H., Kusakunniran W., Amur Z.* A Symbol Recognition System for Single-Line Diagrams Developed Using a Deep-Learning Approach, *Applied Sciences,* 2023, 13, pp. 8816. Available at: https: // doi.org/10.3390/app13158816.
16. *Moreno-García, C.F.; Elyan, E.; Jayne, C.* Heuristics-Based Detection to Improve Text/Graphics Segmentation in Complex Engineering Drawings, *In Proceedings of the Engineering Applications of Neural Networks: 18th International Conference (EANN 2017), Athens, Greece, 25–27 August 2017,* pp. 87-98.
17. *Pratt W.K.* Digital image processing. New York: Wiley, 1991, 698 p.
18. *Muthukrishnan R, Radha M.* Contour selection algorithms for image segmentation, *International Journal of Computer Science & Information Technology (IJCSIT),* 2014,Vol. 3, No. 6, pp. 259-267.
19. *Poynter Ya.* Programmiruem s PyTorch: Sozdanie prilozheniy glubokogo obucheniya [Programming PyTorch for Deep Learning]. Saint Petersburg: Piter, 2020, 256 p.
20. *Liu Yuxi (Hayden).* PyTorch 1.x Reinforcement Learning Cookbook. Over 60 recipes to design, develop, and deploy self-learning AI models using Python. Birmingham–Mumbai: Packt, 2019, 527 p.

Безуглов Дмитрий Анатольевич – Ростовский филиал Российской таможенной академии; e -mail: bezuglovda@mail.ru; г. Ростов-на-Дону, Россия; д.т.н.; профессор.

Мищенко Марина Сергеевна – Южный федеральный университет; e-mail: yourhuckleberrybtw@mail.ru; г. Ростов-на-Дону, Россия; студент.

Мищенко Сергей Евгеньевич – ФГУП «Ростовский научно-исследовательский институт радиосвязи»; e-mail: mihome@yandex.ru; г. Ростов-на-Дону, Россия; д.т.н.; профессор.

Bezuglov Dmitry Anatolyevich – Rostov branch of the Russian Customs Academy; e-mail: bezuglovda@mail.ru; Rostov-on-Don, Russia; dr. of eng. sc.; professor.

Mishchenko Marina Sergeevna – Southern Federal University; e -mail: yourhuckleberrybtw@mail.ru; Rostov-on-Don, Russia; student.

Mishchenko Sergey Evgenievich – FSUE Rostov Scientific Research Institute of Radio Communications; e-mail: mihome@yandex.ru; Rostov-on-Don, Russia; dr. of eng. sc.; professor.

УДК 004.67 DOI 10.18522/2311-3103-2025-3-144-159

А.Г. Бондаренко, А.Г. Кравец

ИДЕНТИФИКАЦИЯ КЛЮЧЕВЫХ ТЕХНОЛОГИЙ НА ОСНОВЕ СБОРА И АНАЛИЗА ДАННЫХ ИЗ ОТКРЫТЫХ РУССКОЯЗЫЧНЫХ ИСТОЧНИКОВ

Данная статья посвящена разработке и апробации нового подхода к сбору, обработке и анализу открытых данных на русском языке для идентификации ключевых технологических направлений. Для решения задачи формирования и последующего анализа структурированных датасетов разработаны и программно реализованы методы веб-скрейпинга, обработки естественного языка и анализа временных рядов. Описанный в статье подход впервые применен для извлечения и структурирования информации из научных статей, новостных ресурсов и патентной документации на русском языке. В результате анализа полученного датасета научных публикаций выделены 30 наиболее часто упоминаемых биграмм и столько же триграмм технологических терминов. На основе анализа частотности биграмм и триграмм выделены ключевые технологические термины, которые затем использованы для комплексной фильтрации по ключевым технологиям. Комплексная фильтрация позволила осуществить поиск русскоязычных патентов и их сбор для дальнейшего анализа. В результате предварительной обработки полученной патентной информации сформированы временные ряды патентной активности. Программная система идентификации ключевых технологий реализована на JavaScript и Python с использованием библиотек Selenium

и BeautifulSoup для веб-скрейпинга, NLTK и Scikit-learn для обработки и анализа текстовых данных. Исследование динамики развития ключевых технологий во времени позволило выявить периоды интенсивной патентной деятельности и снижения интереса к той или иной технологии. Результаты, изложенные в статье, создают основу для дальнейшей разработки методов машинного обучения с целью прогнозирования технологического развития и выявления перспективных направлений прикладных исследований.

Веб-скрейпинг; анализ текста; обработка естественного языка; ключевые термины; биграммы; триграммы; патентная активность; временные ряды; прогнозирование технологического развития; открытые данные.

A.G. Bondarenko, A.G. Kravets

IDENTIFICATION OF KEY TECHNOLOGIES BASED ON COLLECTION AND ANALYSIS OF DATA FROM OPEN RUSSIAN-LANGUAGE SOURCES

This article is devoted to the development and approbation of a new approach to the collection, processing and analysis of open data in the Russian language for identification of key technological trends. To solve the problem of formation and subsequent analysis of structured datasets methods of web scraping, natural language processing and analysis of time-series have been developed and implemented via programming. The approach described in the article has been applied for the first time in order to extract and structure information from scientific articles, news resources and patent documentation in the Russian language for the first time. As a result of analyzing the obtained dataset of scientific publications, 30 most frequently mentioned bigrams and the same number of trigrams of technological terms have been identified. Based on the frequency analysis of bigrams and trigrams, key technological terms were identified which then were used for complex filtration on key technologies. Complex filtration enabled to fulfill the search of patents in Russian and their collection for further analysis. As a result of preprocessing of the obtained patent data time series of patent activity have been formed. The programme system of key technological identification has been implemented in JavaScript and Python using Selenium and BeautifulSoup libraries for web scraping, NLTK and Scikit-learn for text data processing and analysis. The study focused on the dynamics of the development of key technologies over time has allowed to identify periods of intensive patent activity and declining interest in this or that kind of technology. The results presented in the article provide a basis for further development of machine learning methods for the purpose of predicting technological development and identifying promising areas of applied research.

Web scraping; text analysis; natural language processing; key terms; bigrams; trigrams; patent activity; time series; predicting of technological development; open data.

Введение. Прогнозирование развития технологий становится все более важной задачей в условиях стремительного роста количества инноваций, глобализации науки и новых направлений технологического лидерства [1, 2]. Анализ актуальных инструментов прогнозирования технологического развития [3] позволил выявить ряд несовершенств и проблем существующих подходов. Прежде всего, они касаются качества прогноза, а именно недостаточно высокой точности и ошибок прогноза. Как российские, так и зарубежные ученые подчеркивают сложность идентификации «прорывных» технологий на основе анализа открытых данных [4, 5]. Современные подходы к прогнозированию опираются на использование больших объемов данных из разнообразных источников, таких как научные статьи, патенты, новости и социальные сети [6, 7]. Однако, несмотря на доступность этих данных, остается актуальной проблема их эффективного сбора, анализа и интерпретации для целей прогнозирования [8, 9]. При этом необходимо отметить явный дефицит качественных наборов данных (датасетов) на русском языке, несмотря на многочисленные попытки реализации таких проектов [10, 11].

Актуальность исследования обусловлена необходимостью разработки новых подходов к анализу технологических тенденций, основанных на обработке открытых данных на русском языке [12]. Основной целью исследования является разработка и апробация нового подхода к сбору, обработке и анализу открытых данных для идентификации ключевых технологических направлений. Сбор, обработка и анализ открытых данных с использованием методов веб-скрейпинга и анализа текстовых данных позволит выявить ключевые технологические термины и тенденции, а также сформировать перечень технологий для дальнейшего анализа патентной активности.

Подходы к анализу патентных баз данных для идентификации и прогнозирования технологических тенденций широко обсуждаются современными исследователями [13, 14]. Все большее внимание в публикациях уделяется разработке и совершенствованию методов машинного обучения для анализа патентов [15]. Наилучших результатов по точности моделей достигают проекты, связанные с идентификацией вакантных и перспективных технологий в отдельных предметных областях [16, 17]. Также задача идентификации технологических тенденций актуальна для отдельных высокотехнологичных компаний [18]. Однако такие подходы существенно снижают возможности идентификации «прорывных» результатов междисциплинарных исследований. Для нивелирования этого риска применимы методы конструирования будущих событий [19], но они уступают по своим показателям методам машинного обучения в случае использования качественных датасетов.

Ключевым аспектом представленного в данной статье исследования является реализация методов интеллектуального анализа текстовых данных для выявления значимых технологических терминов и последующее формирование временных рядов патентной активности. Разработанный подход позволяет визуализировать динамику развития технологий и выявить периоды интенсификации инновационной деятельности, что необходимо для более глубокого понимания текущего состояния и тенденций в исследуемых технологических областях.

Статья структурирована следующим образом. Раздел 2 посвящен детальному описанию процессов сбора данных из открытых источников, включая использование методов веб-скрейпинга и извлечения информации из различных типов ресурсов. Раздел 3 фокусируется на этапе обработки собранных данных, включающем в себя предобработку текстовой информации, выделение ключевых терминов, а также формирование биграмм и триграмм для последующего анализа. Раздел 4 охватывает процесс формирования временных рядов на основе патентной активности выделенных технологий, а также создание визуализаций для анализа динамики их развития. Наконец, Раздел 5, содержит основные выводы, полученные в результате проведенного исследования, и намечены перспективы дальнейшего развития работы.

Сбор данных из открытых источников. Процедура сбора данных обычно реализуется с помощью веб-краулинга [20] или парсинга веб-страниц и хранилищ документов [21]. Однако эти подходы ограничивают возможности анализа собранных данных семантикой изначальных поисковых запросов. Поэтому, в рамках исследования реализован метод веб-скрейпинга (рис. 1) для сбора данных о технологиях из открытых русскоязычных источников, включая научные статьи, новостные ресурсы и патенты.

Результатом этого процесса является формирование структурированных датасетов. Полученные данные, после предварительной обработки, представляются в виде наборов ключевых терминов (биграмм и триграмм) и их частотности. Это позволяет определить перечень технологий, которые в дальнейшем используются для фильтрации патентной информации.

Сбор данных из научных статей. Для сбора данных из научных статей выполняется поиск ссылок на публикации. Полученные URL-адреса сохраняются в текстовый файл, где каждая ссылка отделена переносом строки.

Для извлечения структурированных данных из этих веб-страниц разработан специализированный веб-скрейпер. Этот веб-скрейпер предназначен для сбора данных с сайта eLibrary. Он обеспечивает авторизацию на сайте посредством Selenium, с использованием логина и пароля, и работает в headless-режиме браузера. Ссылки на страницы статей загружаются из созданного текстового файла. Далее, Selenium загружает HTML-код каждой страницы, а BeautifulSoup извлекает необходимые данные: название статьи, год публикации, аннотацию и ключевые слова. Ключевые слова извлекаются из таблиц с определенной структурой.

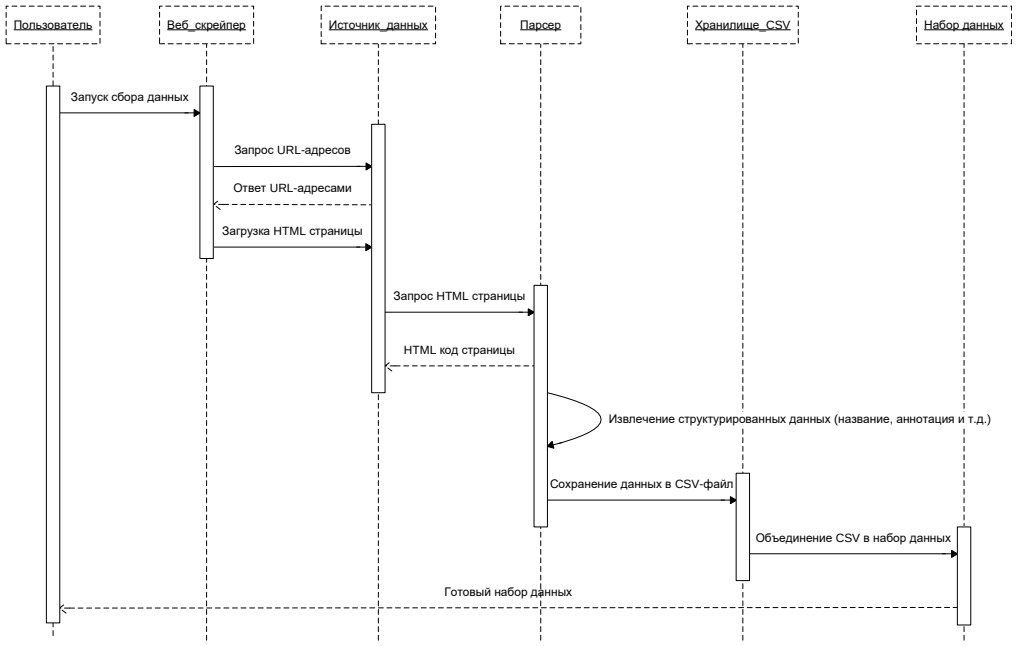


Рис. 1. Диаграмма последовательности метода веб-скрейпинга

В дальнейшем, отдельные CSV-файлы объединяются в единый файл для проведения дальнейшего анализа, с сохранением информации о годах публикации (как временных рядов) и полных текстах документов.

Собранные данные сохраняются в единый датасет, содержащий всю необходимую информацию о научных статьях (рис. 2).

	title	year	abstract	keywords
0	ЦИФРОВИЗАЦИЯ ПРОИЗВОДСТВА: ТЕОРЕТИЧЕСКАЯ СУЩНОСТЬ ...	2018	В современных условиях развитие экономики связываю...	ЭКОНОМИЧЕСКАЯ СИСТЕМА, ПРОМЫШЛЕННОЕ ПРОИЗВОДСТВО, ...
1	ОБ УСТАНОВКАХ КОГНИТИВНОЙ НАУКИ И АКТУАЛЬНЫХ ПРОБЛ...	2004	Начальные этапы становления когнитивной науки были...	Ключевые слова не найдены
2	ЦИФРОВАЯ СОЦИАЛИЗАЦИЯ В КУЛЬТУРНО-ИСТОРИЧЕСКОЙ ПАР...	2018	В настоящей статье раскрываются методология, метод...	КУЛЬТУРНО-ИСТОРИЧЕСКАЯ ПСИХОЛОГИЯ, ЦИФРОВЫЕ ТЕХНОЛ...
...	...	...	...	...
647	НОВЫЕ ПРОЕКТЫ ОСВОЕНИЯ РОССИЙСКОЙ АРКТИКИ: ПРОСТРА...	2020	В статье обобщаются результаты анализа 23 современ...	ПРОЕКТЫ РЕСУРСНОГО ОСВОЕНИЯ АРКТИКИ, ПРОСТРАНСТВЕН...
648	LEGALTECHИ ЮРИСТЫ БУДУЩЕГО	2017	Роботизация юридической профессии стала одной из н...	Ключевые слова не найдены
649	ОБУЧЕНИЕ ЦИФРОВЫМ НАВЫКАМ РАБОТНИКОВ КОНТРАКТНЫХ С...	2019	Цифровизация затронула все сферы жизнедеятельности...	Ключевые слова не найдены

Рис. 2. Датасет по собранным статьям

Датасет имеет следующую структуру:

- title – название статьи;
- year – год публикации статьи;
- abstract – аннотация статьи;
- keywords – ключевые слова.

В результате получено 650 научных публикаций на русском языке, связанных с развитием технологий.

Сбор данных из новостных ресурсов. Для расширения базы данных исследования, включающей информацию о технологических трендах выполняется сбор URL-адресов новостных источников. Этот этап реализуется посредством JavaScript-скрипта, предназначенного для автоматического сбора ссылок на новостные веб-сайты.

Принцип сбора данных с новостных ресурсов аналогичен процессу, применяемому для научных статей. Разработанный Python-скрипт использует библиотеки Selenium и BeautifulSoup для анализа структуры веб-страниц и извлечения необходимых данных из списка полученных URL-адресов. Скрипт автоматически собирает информацию о категории новости, времени публикации, заголовке и полном тексте новостной статьи. Полученные структурированные данные затем агрегируются и сохраняются в CSV-файл для дальнейшей обработки и анализа (рис. 3).

	category	publication_time	title	text	url
0	Город	2024-11-19T10:30:05+03:00	Ракова объяснила внедрение искусственного интеллек...	Столичные власти активно внедряют цифровизацию в о...	https://www.rbc.ru/rbcfreenews/673c37ea9a7947bc84c...
1	Технологии и медиа	2024-11-19T10:21:15+03:00	Ученые назвали год максимума солнечной активности ...	Максимальная активность Солнца в текущем цикле наи...	https://www.rbc.ru/rbcfreenews/673c34559a794763747...
2	Технологии и медиа	2024-11-19T07:40:41+03:00	Bloomberg узнал, что Минюст США потребует от Googl...	Высокопоставленные сотрудники антимонопольного упр...	https://www.rbc.ru/rbcfreenews/673c01989a7947e6bc2...
...	...	...	...	...	...
197	Как защититься от мошенников	2024-10-07T20:12:41+03:00	«Лаборатория Касперского» предложила сообщать об у...	Информировать россиян об утечках персональных данн...	https://www.rbc.ru/rbcfreenews/670414619a794795ac1...
198	Задержание Павла Дурова	2024-10-07T10:54:58+03:00	Сеул попросил Париж помочь с расследованием о дипф...	Полиция Сеула обратилась к властям Франции с просьб...	https://www.rbc.ru/rbcfreenews/6703896c9a79477da05...
199	Технологии и медиа	2024-10-07T10:47:50+03:00	ВГТРК сообщила о «беспрецедентной» хакерской атаке...	В ночь на 7 октября онлайн-сервисы ВГТРК подвергли...	https://www.rbc.ru/rbcfreenews/670391c89a794705c58...

Рис. 3. Датасет по собранным новостям

Датасет имеет следующую структуру:

- category – категория новости;
- publication_time – дата и время публикации новости;
- title – название новости;
- text – содержание новости;
- url – ссылка на публикацию.

В итоге получено 200 новостных источников, связанных с развитием технологий в России.

Сбор данных из патентов. Для проведения анализа технологических трендов в качестве источника патентной информации используется датасет, который состоит из 89 отдельных файлов. Каждый файл содержит данные о патентах, относящихся к определенной технологической области.

В целях проведения интеллектуального анализа и выявления ключевых технологических направлений, данные патентов объединяются в единый структурированный датасет, представленный на рис. 4.

Анализ объединенного датасета патентов демонстрирует недостаточность текстовых данных для проведения полноценного анализа. В связи с этим, на текущем этапе принято решение о дополнении датасета аннотациями к патентам. Для этого разработан процесс автоматизированного сбора описаний патентов посредством парсинга URL-ссылок, содержащихся в исходном датасете. На первом этапе извлекаются все доступные

ссылки на патентные описания. Затем эти ссылки передаются специально разработанному парсеру, который использует библиотеки Selenium и BeautifulSoup для извлечения аннотаций из веб-страниц.

	id	title	assignee	inventor/author	priority date	filing/creation date	publication date	grant date	result link	representative figure link
0	RU-2486412-C1	Отопительная...	Данфосс А/С	Ян Эрик ТОРС...	2010-11-10	2011-11-09	2013-06-27	2013-06-27	https://patents...	https://patenti...
1	RU-105973-U1	Односекцион...	Керми Гмбх	Роджер ШЕНБ...	2007-07-31	2007-10-22	2011-06-27	2011-06-27	https://patents...	nan
2	RU-2719170-C2	Устройство от...	Киунгдонг На...	Чанг Хеой ХЕ...	2015-06-22	2016-05-04	2020-04-17	2020-04-17	https://patents...	https://patenti...
...	...	...	...	...	...	...	...	...	...	...
67456	RU-2557151-C2	Аппарат охла...	Л'Эр Ликид, С...	Патрис КАВАНЬ	2010-07-09	2011-06-22	2015-07-20	2015-07-20	https://patents...	nan
67457	RU-2530898-C2	Способ перер...	Ге Йенбахер Г...	Франц ПОКШ...	2009-10-02	2010-10-01	2014-10-20	2014-10-20	https://patents...	nan
67458	RU-2766594-C1	Установка для...	Общество С О...	Денис Алекса...	2020-12-22	2020-12-22	2022-03-15	2022-03-15	https://patents...	https://patenti...

Рис. 4. Датасет по собранным патентам

В результате собрано 67458 аннотаций к патентам. После завершения парсинга аннотации объединяются с исходным датасетом в единый структурированный датасет. Содержание результирующего датасета представлено на рисунке 5.

Структура датасета:

- id – уникальный номер патента;
- title – название патента;
- assignee – правообладатель;
- inventor/author – авторы патента;
- prioritydate – дата подачи заявки на патент;
- filing/creationdate – дата создания записи о патенте;
- publicationdate – дата удовлетворения заявки;
- grantdate – дата публикации патента;
- resultlink – ссылка на патент;
- representativefigurelink – ссылка на репрезентативный рисунок;
- abstact – аннотация патента.

	id	title	assignee	inventor/author	priority date	filing/creation date	publication date	grant date	result link	representative figure link	abstract
0	RU-2486412-...	Отопительн...	Данфосс А/С	Ян Эрик ТОР...	2010-11-10	2011-11-09	2013-06-27	2013-06-27	https://paten...	https://paten...	Данное изоб...
1	RU-105973-U1	Односекцио...	Керми Гмбх	Роджер ШЕ...	2007-07-31	2007-10-22	2011-06-27	2011-06-27	https://paten...	nan	1. По меньш...
2	RU-2719170-...	Устройство ...	Киунгдонг Н...	Чанг Хеой Х...	2015-06-22	2016-05-04	2020-04-17	2020-04-17	https://paten...	https://paten...	Изобретени...
...	...	...	...	...	...	...	...	...	...	...	...
67456	RU-2557151-...	Аппарат охл...	Л'Эр Ликид, ...	Патрис КАВ...	2010-07-09	2011-06-22	2015-07-20	2015-07-20	https://paten...	nan	Изобретени...
67457	RU-2530898-...	Способ пере...	Ге Йенбахер...	Франц ПОК...	2009-10-02	2010-10-01	2014-10-20	2014-10-20	https://paten...	nan	Изобретени...
67458	RU-2766594-...	Установка д...	Общество С ...	Денис Алекс...	2020-12-22	2020-12-22	2022-03-15	2022-03-15	https://paten...	https://paten...	Изобретени...

Рис. 5. Единый датасет по патентам с аннотациями

Обработка сформированного датасета и выявление ключевых технологических терминов. Для последующего анализа и выявления ключевых технологических терминов все текстовые данные, извлеченные из различных источников, на текущем этапе подвергаются ряду процедур обработки.

Последовательность действий метода анализа и выявления ключевых технологических терминов представлена на DFD-диаграмме ниже (рис. 6).

На первом этапе из каждого датасета извлекаются текстовые данные:

- для статей: title, abstract, keywords;
- для новостей: title, text;
- для патентов: title, abstract.

Затем (этап 2) все текстовые данные объединяются в один текстовый корпус (corpus) для анализа.

На третьем этапе текст разбивается на слова с использованием библиотеки NLTK (RegexpTokenizer). Убираются стоп-слова (предлоги, союзы и т.п.), а также знаки пунктуации. Также выполняется лемматизация текста, т.е. приведение слов в начальную форму. Это необходимо для корректного выявления ключевых терминов.

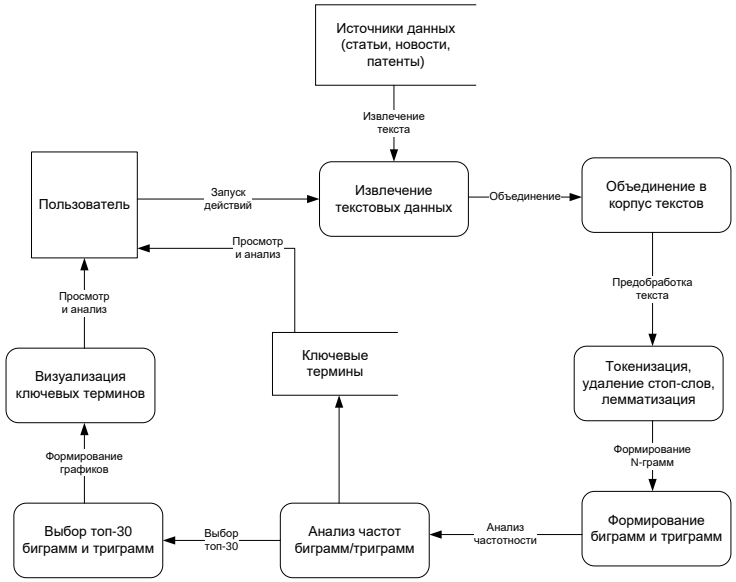


Рис. 6. Диаграмма потоков данных метода анализа и выявления ключевых технологических терминов

На этапе формирования биграмм и триграмм анализ реализован с помощью методов из библиотеки Scikit-learn, а точнее её модуля CountVectorizer из пакета sklearn.feature_extraction.text. Для каждой биграммы/триграммы рассчитана частота появления ключевого термина.

На основании частотности извлекаются 30 наиболее часто встречающихся биграмм и 30 триграмм.

На финальном этапе генерируются горизонтальные гистограммы с биграммами/триграммами и их частотами (рис. 7, 8).

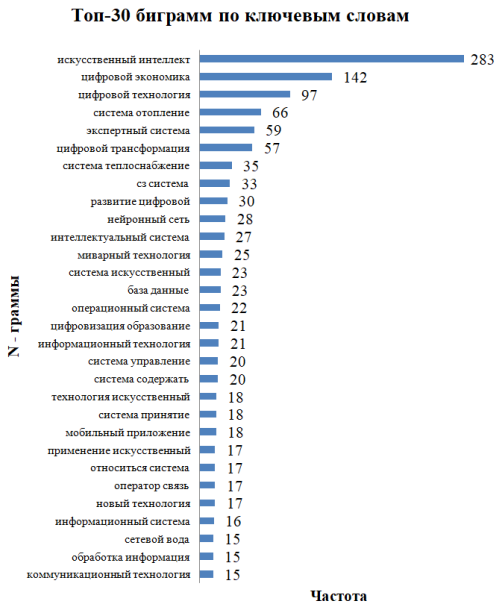


Рис. 7. График биграмм по ключевым терминам

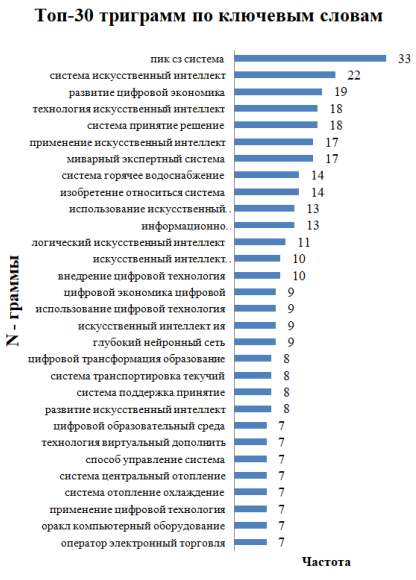


Рис. 8. График триграмм по ключевым терминам

Анализ частотности биграмм и триграмм позволил выявить доминирующие термины. Представленные гистограммы (рис. 7, 8) позволяют идентифицировать ключевые технологии и выявить наиболее значимые сочетания слов, отражающие основные концепции и направления в технологических областях.

Данная информация послужит основой для дальнейшего анализа и формирования перечня технологий, которые будут использованы для фильтрации патентной информации.

Формирование временных рядов ключевых терминов и анализ патентной активности. На основе полученных данных биграмм и триграмм идентифицирован ряд ключевых технологий. Следующим шагом исследования стала разработка метода идентификации ключевых технологий (МИКТ) на основе анализа временных рядов патентной активности (рис. 9).

Формирование временных рядов ключевых терминов. В связи с тем, что на предварительном этапе была выполнена лемматизация слов для идентификации ключевых терминов, в дальнейшем они приводятся к стандартным формам. Технологии, представленные в виде биграмм и триграмм, приведены в табл. 1, в которой также указано количество найденных патентов для каждой технологии.

В табл. 1 наблюдается существенное различие в количестве найденных патентов, содержащих биграммы и триграммы. Это объясняется тем, что многие триграммы, идентифицированные на этапе анализа частотности в текстах научных публикаций, непосредственно не упоминаются в патентной документации, связанной с ключевыми технологиями.

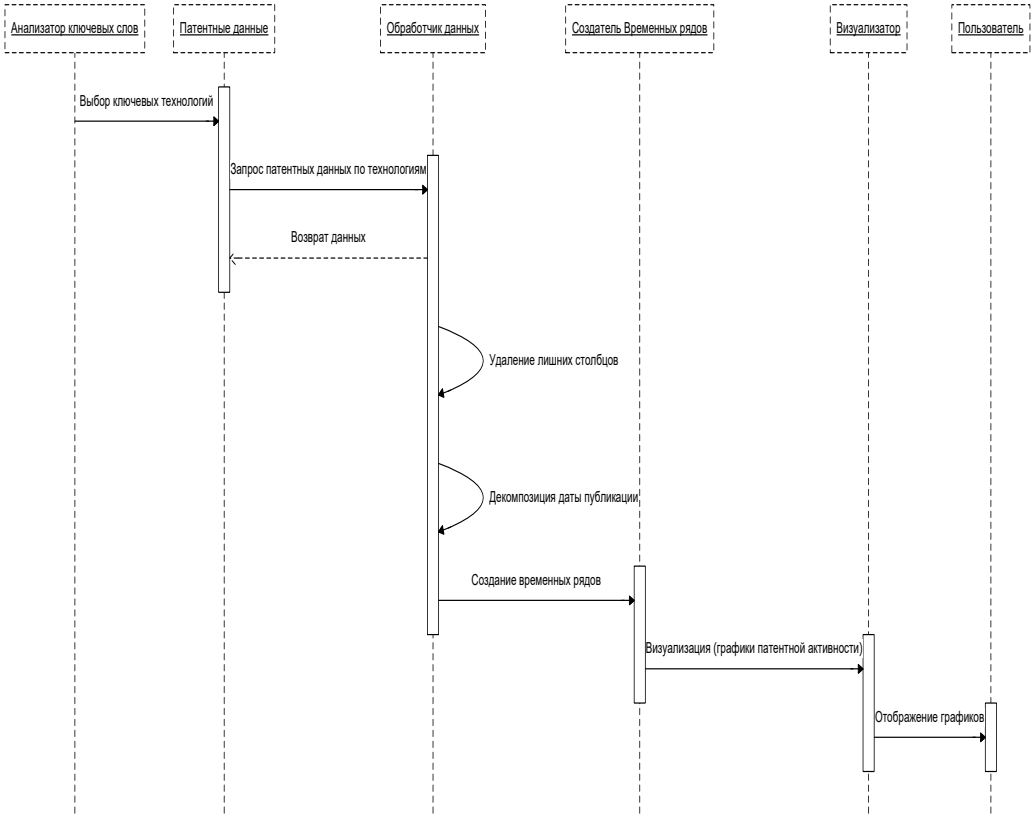


Рис. 9. Диаграмма последовательности метода идентификации ключевых технологий на основе анализа временных рядов патентной активности

Таблица 1

Биграммы и триграммы ключевых технологий и количество найденных патентов

Биграммы	Число патентов	Триграммы	Число патентов
искусственный интеллект	397	системы искусственного интеллекта	1376
цифровая экономика	28	система принятия решений	5755
цифровые технологии	8466	система горячего водоснабжения	1412
система отопления	4383	информационно коммуникационные технологии	87
экспертная система	604	логический искусственный интеллект	51
цифровая трансформация	75	глубокие нейронные сети	104
система теплоснабжения	1780	поддержка принятия решений	422
нейронные сети	1417	система текучей транспортировки	2787
интеллектуальная система	1306	цифровая трансформация образования	36
базы данных	17160	оператор электронной торговли	174
искусственные технологии	2907	система отопления/охлаждения	1520
операционная система	4517	система центрального отопления	536
информационные технологии	5246	технология виртуальной реальности	590
цифровизация образования	16		
система управления	17321		
искусственные системы	5683		
коммуникационные технологии	1234		
обработка информации	17068		
компьютерное оборудование	1366		

По указанным выше технологиям анализируется патентная активность. В рамках МИКТ была применена комплексная фильтрация по наименованию ключевых технологий для поиска русскоязычных патентов и их сбор для дальнейшего анализа. Последую-

щая обработка включает удаление избыточных столбцов из полученных датасетов с сохранением только класса технологии и даты публикации патента. Для анализа временных рядов дата публикации патента декомпозируется на отдельные поля, представляющие месяц и год публикации (табл. 2).

Таблица 2

Итоговый формат датасета временных рядов ключевых технологий (фрагмент)

Название технологии	Год	Месяц	Количество публикаций
Искусственный интеллект	2021	11	5
Искусственный интеллект	2021	12	7
…			
Нейронные сети	2022	6	11

Для демонстрации процесса формирования датасета временных рядов используется пример технологии «Искусственный интеллект». Для остальных датасетов применяется аналогичный принцип, отличие заключается лишь в названии ключевой технологии.

В рамках обработки удаляются все колонки, кроме даты публикации патента, и в первой колонке устанавливается название ключевой технологии. Также дата публикации разделяется на колонки year (год публикации патента) и month (месяц публикации патента). Наконец, добавляется колонка count_publication, отражающая количество патентов за указанный временной период. Месяцы и годы должны следовать последовательно, что означает, что если в каком-либо месяце не было опубликовано ни одного патента, то для него устанавливается значение 0. Результат обработки представлен на рис. 10.

	technology	year	month	count_publication
0	Искусственный интеллект	1980	1	0
1	Искусственный интеллект	1980	2	0
2	Искусственный интеллект	1980	3	0
...	...	...	...	...
537	Искусственный интеллект	2024	10	6
538	Искусственный интеллект	2024	11	2
539	Искусственный интеллект	2024	12	0

Рис. 10. Данные временных рядов технологии «Искусственный интеллект»

Анализ патентной активности. На этапе анализа патентной активности выявлены тенденции развития (подъем Rise или спад Fall) ключевых технологий, которые были отфильтрованы и представлены в виде временных рядов (рис. 11, 12).

Визуализация патентной активности на представленных графиках (рис. 11, 12.) позволяет оценить динамику развития каждой идентифицированной технологии. Например, патентование в области систем управления и обработки информации достигло максимальной активности в 2008 году, после чего последовал значительный спад, что свидетельствует о стабилизации или смене технологических приоритетов. В то же время патентование в областях систем искусственного интеллекта и глубоких нейронных сетей демонстрирует активное развитие в последние годы. Это подтверждает тенденцию на расширение сфер применения методов искусственного интеллекта.

Наблюдаемые пики на графиках отражают периоды интенсивной патентной деятельности, свидетельствующие о повышенном интересе к данной технологии в этот временной промежуток. Эти всплески могут быть связаны с прорывными открытиями, появлением новых применений технологии или же с общей активизацией инновационной деятельности в определенной области.

В свою очередь, падения на графиках могут сигнализировать о снижении интереса к технологии, возможно, в связи с насыщением рынка, появлением более перспективных альтернатив или же в результате смены технологических парадигм. Анализ продолжительности и интенсивности этих пиков и падений позволяет выявить жизненный цикл технологии, определить ее текущее состояние и потенциальные перспективы развития.

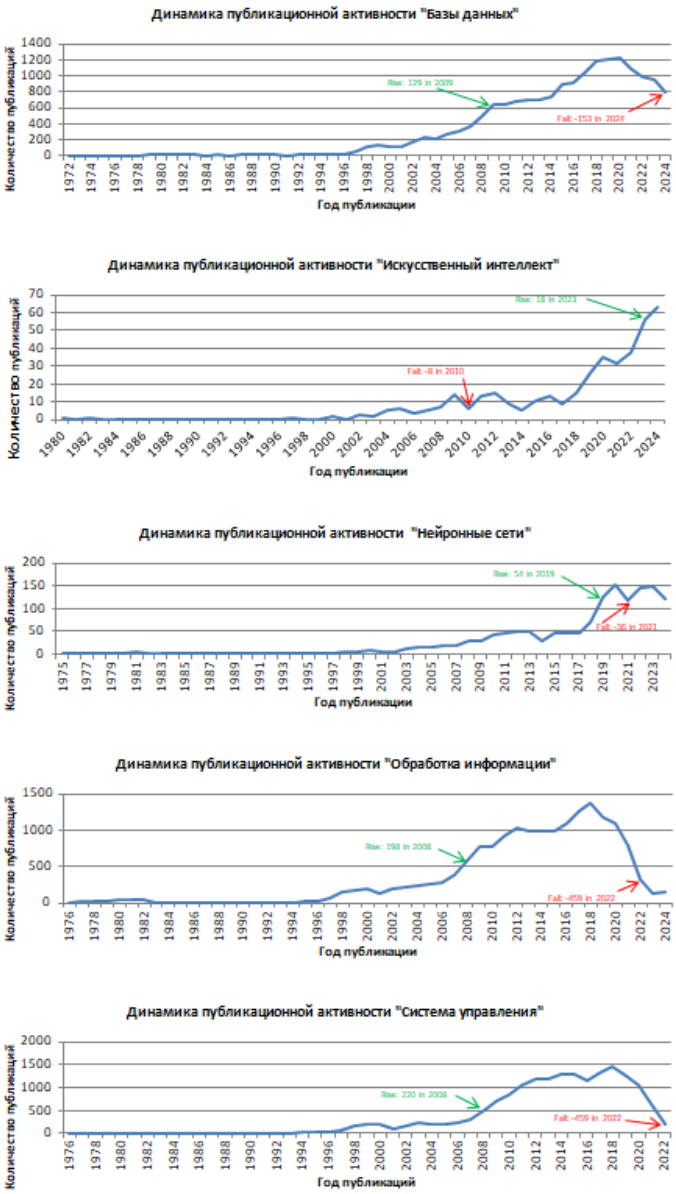


Рис. 11. Графики патентной активности исследуемых технологий-биграмм (фрагмент)

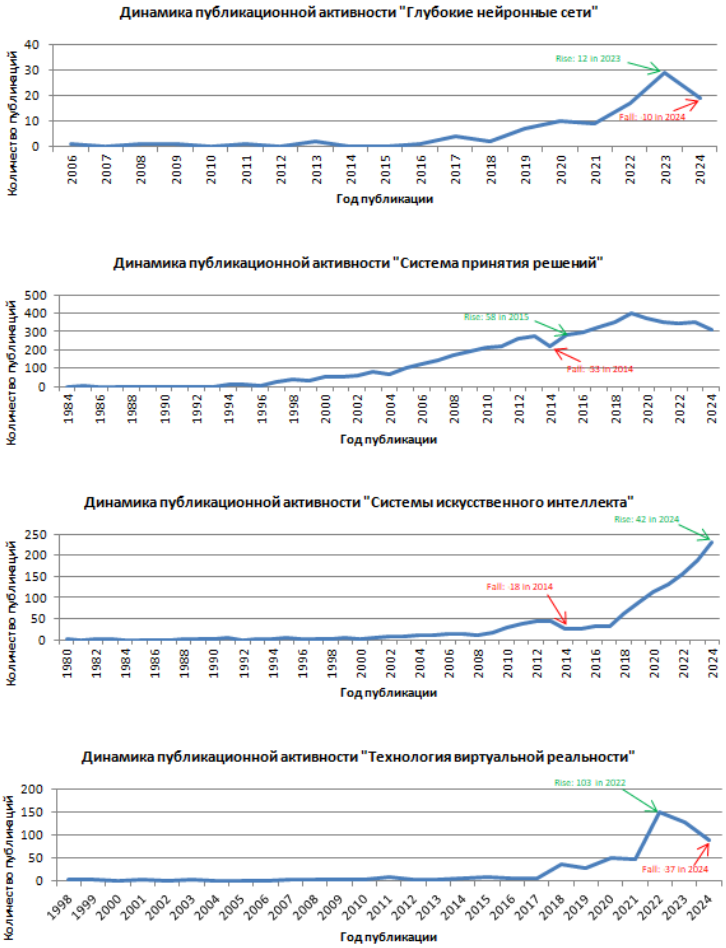


Рис. 12. Графики патентной активности исследуемых технологий-триграмм (фрагмент)

Итоговые результаты, представленные в табл. 3, подтверждают эффективность предложенного подхода к идентификации ключевых технологий.

Таблица 3

Результаты исследования

Технология	Частота встречаемости в текстах	Количество патентов	Год начала активности технологий	Пик активности / прирост числа публикаций	Спад активности/ убыль числа публикаций
Искусственный интеллект	283	397	1980 г.	2023 г. /18	2010 г. /-8
Нейронные сети	28	1417	1975 г.	2019 г. /54	2021 г. /-36
Базы данных	23	17160	1972 г.	2009 г. /149	2024 г. /-153
Система управления	20	17321	1976 г.	2008 г. /220	2022 г. /-459

Окончание табл. 3

Технология	Частота встречаемости в текстах	Количество патентов	Год начала активности технологий	Пик активности / прирост числа публикаций	Спад активности/ убыль числа публикаций
Обработка информации	15	17068	1976 г.	2008 г. /198	2022 г. /-459
Системы искусственного интеллекта	22	1376	1980 г.	2024 г. /42	2014 г. /-18
Система принятия решений	18	5755	1984 г.	2015 г. /58	2014 г. /-53
Глубокие нейронные сети	9	104	2006 г.	2023 г. /12	2024 г. /-10
Технология виртуальной реальности	7	590	1998 г.	2022 г. /108	2024 г. /-37

Заключение. В рамках проведенного исследования был разработан и реализован комплексный подход к сбору, обработке и анализу открытых данных с целью идентификации ключевых технологий. Разработка метода веб-скрейпинга, использование методов обработки естественного языка и анализа временных рядов позволило сформировать структурированные датасеты. На основе анализа частотности биграмм и триграмм были выделены ключевые технологические термины, которые в дальнейшем легли в основу для МИКТ. В рамках исследования проанализированы исключительно русскоязычные документы, что позволяет учитывать специфику отечественного технологического развития.

Выполненный с помощью МИКТ анализ временных рядов патентной активности позволил визуализировать динамику развития каждой исследуемой технологии, выявить периоды интенсивной патентной деятельности и снижения интереса к ним. На основе полученного датасета были сформированы графики патентной активности. Это является важным шагом для дальнейшего анализа и кластеризации, а также для прогнозирования развития ключевых технологий.

Анализ частоты упоминания технологических терминов в текстах и их патентной активности позволил выявить динамику развития различных технологий, определить периоды их интенсивного роста и спада.

В результате проведенного исследования были созданы необходимые основы для дальнейшего применения методов машинного обучения с целью прогнозирования технологического развития, что является следующим шагом в исследовании и выходит за рамки данной статьи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Безруков А.О., Байдаров Д.Ю., Файков Д.Ю.* Технологическое лидерство государства: концептуальное понимание и механизмы формирования // Экономическое возрождение России. – 2024. – № 1 (79). – С. 75-89. – DOI 10.37930/1990-9780-2024-1-79-75-89. – EDN ZSGGUU.
2. *Елисеев В.А.* Доминанты прогнозирования научно-технологического развития // Автоматизация. Современные технологии. – 2019. – Т. 73, № 10. – С. 461-466.
3. *Бондаренко А.Г., Кравец А.Г.* Инструменты прогнозирования технологического развития на основе данных из открытых источников: систематическое исследование русскоязычных документов // Прикаспийский журнал: управление и высокие технологии. – 2024. – № 3 (67). – С. 49-62.

4. *Porter A.L. et al.* Emergence scoring to identify frontier R&D topics and key players // Technol. Forecast. Soc. Change. 2019. – Vol. 146. – P. 628-643. – DOI: 10.1016/j.techfore.2018.04.016.
5. *Кравец А.Г., Нгуен Т.В.* Прогнозирование технологических тенденций на основе анализа разнородных данных // Программные продукты и системы. – 2022. – № 3. – С. 396-412. – DOI: 10.15827/0236-235X.139.396-412.
6. *Nivash J.P., Babu L.D.D.* Analyzing the impact of news trends on research publications and scientific collaboration networks // Concurrency and Computation-Practice & Experience. – 2019. – Vol. 31, No. 14. – P. 10.
7. *Injadat M.N., Salo F., Nassif A.B.* Data mining techniques in social media: A survey. Neurocomputing. – 2016. – Vol. 214. – P. 654-670. – DOI: 10.1016/j.neucom.2016.06.045.
8. *Antons D. et al.* The application of text mining methods in innovation research: current state, evolution patterns, and development priorities // R & D Management. – 2020. – P. 329-351. – DOI: 10.1111/radm.12408.
9. *Zhou Y. et al.* Forecasting emerging technologies using data augmentation and deep learning // Scientometrics. – 2020. – DOI: 10.1007/s11192-020-03351-6.
10. *Каленов Н.Е., Власова С.А.* О реализации многофункциональной web-системы регистрации и учета результатов интеллектуальной деятельности ученых // Программные продукты и системы. – 2021. – № 4. – С. 501-510. – DOI: 10.15827/0236-235X.136.501-510.
11. *Сотников А.Н., Каленов Н.Е., Власова С.А.* Развитие системы «Экспертиза» как инструмента для формирования энциклопедий и наполнения Единого цифрового пространства научных знаний // Программные продукты и системы. – 2022. – № 4. – С. 541-548. – DOI: 10.15827/0236-235X.140.541-548.
12. *Vasiliev S.S., Korobkin D.M., Kravets A.G. et al.* Extraction of Cyber-Physical Systems Inventions' Structural Elements of Russian-Language Patents // Studies in Systems, Decision and Control. – 2020. – Vol. 259. – P. 55-68. – DOI: 10.1007/978-3-030-32579-4_5.
13. *Song K., Kim K., Lee S.* Identifying promising technologies using patents: A retrospective feature analysis and a prospective needs analysis on outlier patents // Technol. Forecast. Soc. Change. – 2018. – DOI: 10.1016/j.techfore.2017.11.008.
14. *Коробкин Д.М., Рублев А.А., Фоменков С.А.* Прогнозирование значимости запатентованных технологий на основе метрик инновационного потенциала // Программная инженерия. – 2024. – Т. 15, № 5. – С. 243-253. – DOI: 10.17587/prin.15.243-253.
15. *Lee C., Kwon O., Kim M., Kwon D.* Early identification of emerging technologies: A machine learning approach using multiple patent indicators // Technol. Forecast. Soc. Change. – 2018. – DOI: 10.1016/j.techfore.2017.10.002.
16. *Yu J. et al.* Identification of vacant and emerging technologies in smart mobility through the GTM-based patent map development // Sustain. – 2020. – DOI: 10.3390/su12229310.
17. *Jun S. et al.* Identification of promising vacant technologies for the development of truck on freight train transportation systems // Appl. Sci. – 2021. – DOI: 10.3390/app11020499.
18. *Yoon B., Park I., Yun D., Park, G.* Exploring promising vacant technology areas in a technology-oriented company based on bibliometric analysis and visualization // Technol. Anal. Strateg. Manag. – 2019. – DOI: 10.1080/09537325.2018.1516864.
19. *Белевцев А.А., Белевцев А.М., Балыбердин В.А.* Методика прогнозирования развития технологических трендов и построения дорожных карт на основе конструирования будущих событий // Известия ЮФУ. Технические науки. – 2023. – № 3(233). – С. 56-64. – DOI: 10.18522/2311-3103-2023-3-56-64.
20. *Вьет Н.Т., Кравец А.Г.* Алгоритм работы веб-краулера для решения задачи сбора данных из открытых интернет источников // Известия Санкт-Петербургского государственного технологического института (технического университета). – 2019. – № 51 (77). – С. 115-119. – DOI: 10.36807/1998-9849-2019-51-77-115-119.
21. *Козина С.А., Кулинченко И.А., Коробкин Д.М., Фоменков С.А.* Концепция и архитектура парсинга и хранения единой базы патентов и научных журнальных публикаций // Моделирование, оптимизация и информационные технологии. – 2024. – Т. 12, № 4. – 15 с. – DOI: 10.26102/2310-6018/2024.47.4.024. – URL: https://moitvivt.ru/ru/journal/pdf?id=1740.

REFERENCES

1. *Bezrukov A.O., Baydarov D.Yu., Faykov D.Yu.* Tekhnologicheskoye liderstvo gosudarstva: kontseptual'noye ponimaniye i mekhanizmy formirovaniya [Technological leadership of the state: conceptual understanding and mechanisms of formation], *Ekonomicheskoye vozrozhdenie Rossii* [Economic Revival of Russia], 2024, No. 1 (79), pp. 75-89. DOI: 10.37930/1990-9780-2024-1-79-75-89.

2. *Eliseev V.A.* Dominanty prognozirovaniya nauchno-tekhnologicheskogo razvitiya [Dominants of forecasting scientific and technological development], *Avtomatizatsiya. Sovremennye tekhnologii* [Automation. Modern Technologies], 2019, Vol. 73, No. 10, pp. 461-466.
3. *Bondarenko A.G., Kravets A.G.* Instrumenty prognozirovaniya tekhnologicheskogo razvitiya na osnove dannykh iz otkrytykh istochnikov: sistematicheskoye issledovaniye russkoyazychnykh dokumentov [Tools for forecasting technological development based on data from open sources: a systematic study of Russian-language documents], *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2024, No. 3 (67), pp. 49-62.
4. *Porter A.L. et al.* Emergence scoring to identify frontier R&D topics and key players, *Technol. Forecast. Soc. Change*, 2019, Vol. 146, pp. 628-643. DOI: 10.1016/j.techfore.2018.04.016.
5. *Kravets A.G., Nguyen T.V.* Prognozirovaniye tekhnologicheskikh tendentsiy na osnove analiza raznorodnykh dannykh [Forecasting technological trends based on the analysis of heterogeneous data], *Programmnye produkty i sistemy* [Software & Systems], 2022, No. 3, pp. 396-412. DOI: 10.15827/0236-235X.139.396-412.
6. *Nivash J.P., Babu L.D.D.* Analyzing the impact of news trends on research publications and scientific collaboration networks, *Concurrency and Computation-Practice & Experience*, 2019, Vol. 31, No. 14, pp. 10.
7. *Injadat M.N., Salo F., Nassif A.B.* Data mining techniques in social media: A survey, *Neurocomputing,* 2016, Vol. 214, pp. 654-670. DOI: 10.1016/j.neucom.2016.06.045.
8. *Antons D. et al.* The application of text mining methods in innovation research: current state, evolution patterns, and development priorities, *R & D Management*, 2020, pp. 329-351. DOI: 10.1111/radm.12408.
9. *Zhou Y. et al.* Forecasting emerging technologies using data augmentation and deep learning, *Scientometrics,* 2020. DOI: 10.1007/s11192-020-03351-6.
10. *Kalenov N.E., Vlasova S.A.* O realizatsii mnogofunktsional'noy web-sistemy registratsii i ucheta rezul'tatov intellektual'noy deyatel'nosti uchenykh [On the implementation of a multifunctional web-system for registration and accounting of the results of intellectual activity of scientists], *Programmnye produkty i sistemy* [Software & Systems], 2021, No. 4, pp. 501-510. DOI: 10.15827/0236-235X.136.501-510.
11. *Sotnikov A.N., Kalenov N.E., Vlasova S.A.* Razvitiye sistemy «Ekspertiza» kak instrumenta dlya formirovaniya entsiklopediy i napolneniya Edinogo tsifrovogo prostranstva nauchnykh znaniy [Development of the "Expertise" system as a tool for the formation of encyclopedias and filling the Unified Digital Space of Scientific Knowledge], *Programmnye produkty i sistemy* [Software & Systems], 2022, No. 4, pp. 541-548. DOI: 10.15827/0236-235X.140.541-548.
12. *Vasiliev S.S., Korobkin D.M., Kravets A.G. et al.* Extraction of Cyber-Physical Systems Inventions' Structural Elements of Russian-Language Patents, *Studies in Systems, Decision and Control*, 2020, Vol. 259, pp. 55-68. DOI: 10.1007/978-3-030-32579-4_5.
13. *Song K., Kim K., Lee S.* Identifying promising technologies using patents: A retrospective feature analysis and a prospective needs analysis on outlier patents, *Technol. Forecast. Soc. Change,* 2018. DOI: 10.1016/j.techfore.2017.11.008.
14. *Korobkin D.M., Rublev A.A., Fomenkov S.A.* Prognozirovanie znachimosti zapatenovannykh tekhnologiy na osnove metrik innovatsionnogo potentsiala [Forecasting the significance of patented technologies based on metrics of innovative potential], *Programmnaya Inzheneriya* [Software Engineering], 2024, Vol. 15, No. 5, pp. 243-253. DOI: 10.17587/prin.15.243-253.
15. *Lee C., Kwon O., Kim M., Kwon D.* Early identification of emerging technologies: A machine learning approach using multiple patent indicators, *Technol. Forecast. Soc. Change*, 2018. doi:10.1016/j.techfore.2017.10.002.
16. *Yu J. et al.* Identification of vacant and emerging technologies in smart mobility through the GTM-based patent map development, *Sustain,* 2020. DOI: 10.3390/su12229310.
17. *Jun S. et al.* Identification of promising vacant technologies for the development of truck on freight train transportation systems, *Appl. Sci.,* 2021. DOI: 10.3390/app11020499.
18. *Yoon B., Park I., Yun D., Park, G.* Exploring promising vacant technology areas in a technology-oriented company based on bibliometric analysis and visualisation, *Technol. Anal. Strateg.Manag.,* 2019. DOI: 10.1080/09537325.2018.1516864.
19. *Belevtsev A.A., Belevtsev A.M., Balyberdin V.A.* Metodika prognozirovaniya razvitiya tekhnologicheskikh trendov i postroyeniya dorozhnykh kart na osnove konstruirovaniya budushchikh sobytiy [Methodology for forecasting the development of technological trends and building roadmaps based on the construction of future events], *Izvestiya YuFU. Tekhnicheskiye Nauki* [Izvestiya SFedU. Engineering Sciences], 2023, No. 3(233), pp. 56-64. DOI: 10.18522/2311-3103-2023-3-56-64.

20. *Viet N.T., Kravets A.G.* Algoritm raboty web-kraulera dlya resheniya zadachi sbora dannykh iz otkrytykh internet istochnikov [The algorithm of the web crawler for solving the problem of collecting data from open Internet sources], *Izvestiya Sankt-Peterburgskogo gosudarstvennogo tekhnologicheskogo instituta (tekhnicheskogo universiteta)* [Izvestiya of Saint-Petersburg State Technological Institute (Technical University)], 2019, No. 51 (77), pp. 115-119. DOI: 10.36807/1998-9849-2019-51-77-115-119.
21. *Kozina S.A., Kulinchenko I.A., Korobkin D.M., Fomenkov S.A.* Kontseptsiya i arkhitektura parsinga i khraneniya edinoy bazy patentov i nauchnykh zhurnal'nykh publikatsiy [The concept and architecture of parsing and storing a unified database of patents and scientific journal publications], *Modelirovanie, optimizatsiya i informatsionnye tekhnologii* [Modeling, Optimization and Information Technology], 2024, Vol. 12, No. 4, 15 p. DOI: 10.26102/2310-6018/2024.47.4.024. Available at: https://moitvivt.ru/ru/journal/pdf?id=1740.

Бондаренко Артём Геннадьевич – Волгоградский государственный технический университет; e-mail: temdit01@yandex.ru; г. Волгоград, Россия; тел.: +79375596156; кафедра систем автоматизированного проектирования и поискового конструирования; магистрант.

Кравец Алла Григорьевна – Волгоградский государственный технический университет; e-mail: AllaGKravets@yandex.ru; г. Волгоград, Россия; тел.: +79023639186; кафедра систем автоматизированного проектирования и поискового конструирования; д.т.н.; профессор.

Bondarenko Artem Gennadevich – Volgograd State Technical University; e-mail: temdit01@yandex.ru; Volgograd, Russia; phone: +79375596156; the Department of CAD&RD; master student.

Kravets Alla Grigorievna – Volgograd State Technical University; e-mail: AllaGKravets@yandex.ru; Volgograd, Russia; phone: +79023639186; the Department of CAD&RD; dr. of eng. sc.; professor.

УДК 004.89 DOI 10.18522/2311-3103-2025-3-159-171

А.М. Мансур, Ж.Х. Мохаммад, Ю.А. Кравченко

РАЗРАБОТКА ЧАТ-БОТА ДЛЯ КЛАССИФИКАЦИИ И АНАЛИЗА ТЕКСТОВ НА ЕСТЕСТВЕННОМ ЯЗЫКЕ С ИСПОЛЬЗОВАНИЕМ ЛОКАЛЬНЫХ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

Исследуются локальные большие языковые модели (Local large language models, Local LLM) и их применение в задачах классификации текста, а также проводится сравнение их производительности с традиционными методами. Статья предоставляет всесторонний обзор ряда ключевых локальных LLM, уделяя особое внимание их архитектурным преимуществам, характеристикам и областям применения. В частности, рассматриваются модели с различным количеством параметров, их способность адаптироваться к специализированным доменам, а также требования к вычислительным ресурсам при их развертывании на локальном оборудовании. Особый акцент делается на компромиссах между производительностью и эффективностью использования ресурсов. В качестве практического вклада разработан чат-бот, использующий локальные LLM (такие как DeepSeek, Gemma и Llama2 через Ollama) для классификации входящих текстов по заранее заданным категориям, демонстрируя работу этих моделей без использования облачных вычислений. Система реализована с модульной архитектурой, позволяющей легко интегрировать новые модели и сравнивать их эффективность. Вычислительный эксперимент включает оценку точности и скорости вывода локальных LLM в сравнении с более простыми методами, такими как Sentence-BERT, TF-IDF и BoWC, выделяя сценарии, в которых локальные модели превосходят традиционные подходы или уступают им. Тестирование проводилось на основе эталонного набора данных BBC. Результаты показывают, что языковые модели (включая модели с 7 миллиардами параметров) демонстрируют сильную и логически обоснованную классификационную производительность при обработке текстов на естественном языке, однако их результаты не являются идеальными для эталонных наборов данных. В частности, обнаружены случаи, когда все тестируемые модели, включая традиционные методы, ошибочно классифицировали документы, что указывает на возможные проблемы в разметке данных. Полученные результаты указывают на необходимость пересмотра эталонных меток в стандартных наборах данных. Это особенно

важно для доменов с субъективными категориями, где экспертные оценки могут значительно расходиться. С другой стороны, хотя локальные LLM уступают облачным в скорости, их преимущества в конфиденциальности данных и оффлайн-работе делают их пригодными для специализированных задач.

Локальные большие языковые модели; БЯМ; классификация; Ollama; Sentence-BERT; BoWC; децентрализованный ИИ.

A.M. Mansour, J.H. Mohammad, Yu.A. Kravchenko

DEVELOPMENT OF A CHATBOT FOR CLASSIFICATION AND ANALYSIS OF NATURAL LANGUAGE TEXTS USING LOCAL LARGE LANGUAGE MODELS

This paper explores local large language models (LLMs) and their application in text classification tasks, while also comparing their performance with traditional methods. The paper provides a comprehensive review of several key local LLMs, with particular focus on their architectural advantages, characteristics, and application domains. Specifically, we examine models with varying numbers of parameters, their ability to adapt to specialized domains, and their computational requirements when deployed on local hardware. Special emphasis is placed on the trade-offs between performance and resource efficiency. As a practical contribution, we developed a chatbot that utilizes local LLMs (such as DeepSeek, Gemma, and Llama2 via Ollama) to classify incoming texts into predefined categories, demonstrating the operation of these models without cloud computing. The system features a modular architecture that allows for easy integration of new models and comparison of their effectiveness. The computational experiment involves evaluating the accuracy and inference speed of local LLMs compared to simpler methods such as Sentence-BERT, TF-IDF and BoWC, highlighting scenarios in which local models outperform or underperform traditional approaches. Testing was conducted using the benchmark BBC dataset. The results show that language models (including 7-billion parameter models) demonstrate strong and logically consistent classification performance in natural language text processing. However, their results are not perfect for benchmark datasets. Notably, we identified cases where all tested models, including traditional methods, misclassified documents, suggesting potential issues with data labeling. These findings indicate the need to reconsider benchmark labels in standard datasets, particularly for domains with subjective categories where expert evaluations may vary significantly. On the other hand, while local LLMs lag behind cloud-based solutions in speed, their advantages in data privacy and offline operation make them suitable for specialized tasks. This is particularly valuable in medical and financial institutions where protection of sensitive information is critical, and where local models can be fine-tuned for specific business processes without the constraints of cloud APIs.

Local large language models; LLM; classification; Ollama; SBERT; BoWC; decentralized AI.

Введение. Стремительное развитие больших языковых моделей (LLM) произвело революцию в области обработки естественного языка (NLP), обеспечив значительный прогресс в таких задачах, как классификация текста и разработка диалоговых систем. Хотя облачные модели, такие как GPT-4, в настоящее время доминируют в этой сфере, их зависимость от внешних API порождает серьёзные проблемы, связанные с конфиденциальностью данных, задержками при обработке и эксплуатационными расходами. Это стимулирует растущий интерес к локальным LLM – моделям машинного обучения, способным понимать и генерировать естественно-языковые тексты исключительно на пользовательском оборудовании (например, персональных компьютерах, серверах или периферийных устройствах), без необходимости подключения к облачным сервисам [1, 2].

Классификация текста представляет собой базовую задачу обработки естественного языка (NLP), суть которой заключается в отнесении текстовых данных к заранее определённым категориям на основе их содержания [3]. Данный процесс играет ключевую роль в извлечении знаний и поддержке принятия решений, поскольку позволяет выявлять ценную информацию в массивах текстовых данных. В условиях экспоненциального роста объёмов цифровой информации значимость эффективных методов текстовой классификации существенно возрастает.

Компактные, но эффективные архитектуры, такие как LLaMA2 [4], DeepSeek [5, 6] и Gemma [7], демонстрируют высокую универсальность в классификации неструктурированных данных благодаря использованию методов zero-shot и few-shot обучения.

В этих подходах модели работают либо исключительно на основе инструкций, либо с минимальным количеством размеченных примеров, что позволяет быстро адаптироваться к новым предметным областям. Локальные LLM предлагают существенные преимущества, включая контроль над данными, возможность кастомизации и автономную функциональность.

Несмотря на эти преимущества, существуют серьезные проблемы, связанные с точностью, вычислительной эффективностью и практическим применением, которые требуют дальнейшего совершенствования. Предыдущие исследования подтвердили полезность локальных LLM для задач классификации, но большинство работ сосредоточено на отдельных моделях или узких приложениях, не предлагая всестороннего сравнения различных архитектур. В частности, отсутствуют систематические сравнительные оценки с традиционными методами, такими как Sentence-BERT [8], TF-IDF или Bag-of-Weighted-Concepts (BoWc) [9–11], которые остаются конкурентоспособными благодаря своей проверенной эффективности и оптимальному использованию ресурсов. Это особенно важно для специалистов, которым необходимо учитывать компромиссы между производительностью и аппаратными ограничениями в реальных сценариях.

В данной работе проводится эмпирическое сравнение современных локальных LLM (включая DeepSeek R1, Gemma и LLaMA2, реализованные через Ollama) с традиционными методами при решении задачи классификации текстов. Исследование оценивает:

- эффективность LLM в задачах классификации текстов;
- скорость вывода, объем используемой памяти и требования к оборудованию;
- особенности развертывания LLM в периферийных и серверных средах.

Проведенный анализ предоставляет практические рекомендации по выбору моделей LLM на основе баланса между точностью, скоростью и ресурсозатратностью.

1. Архитектура больших языковых моделей (LLM). Современные LLM используют трансформерную архитектуру [12], которая состоит из:

А. Слой встраивания (англ. embedding layer). Слой встраивания выполняет критически важную функцию преобразования текстовых данных в числовое представление, понятное нейронной сети. На этом этапе исходный текст сначала разбивается на токены (отдельные слова или части слов), которые затем переводятся в плотные векторные представления – встраивания **(**эмбеддинги). Этот процесс включает два основных компонента: токенные встраивания, отображающие семантические свойства языковых единиц в многомерном векторном пространстве, и позиционные встраивания, кодирующие информацию о порядке следования элементов в последовательности, что принципиально важно для понимания контекста и синтаксических отношений.

*Б. Блоки-трансформеры (англ. Transformer Blocks)***.** Основу архитектуры составляют блоки-трансформеры, организованные в виде последовательности идентичных слоёв. Каждый такой блок содержит три ключевых элемента. Во-первых, механизм многоголовой само-внимательности (Self-Attention) анализирует взаимосвязи между всеми словами входной последовательности, используя матрицы Query (запросов), Key (ключей) и Value (значений) для динамического определения значимости каждого элемента контекста. Этот механизм обеспечивает параллельную обработку последовательностей и выявление сложных семантических зависимостей. Во-вторых, прямая нейронная сеть (Feed-Forward Network) выполняет нелинейное преобразование выходов механизма внимания, обычно реализуемое как двухслойная структура с активацией ReLU или GELU. В-третьих, система остаточных связей и слой нормализации (Residual + LayerNorm) стабилизирует процесс обучения: остаточные соединения позволяют передавать исходные данные через несколько слоёв, предотвращая проблему затухающих градиентов, а нормализация активаций способствует более устойчивому обучению.

С. Выходной слой (англ. Output layer). Завершающий этап обработки - выходной слой – преобразует полученные скрытые состояния в вероятностное распределение над словарём модели. Используемая здесь функция активации softmax обеспечивает нормализацию выходных значений, превращая их в вероятности следующего токена, что позволяет модели генерировать осмысленные и когерентные продолжения текста. Эта ар-

хитектурная схема, сочетающая мощные механизмы анализа контекста с эффективными методами нормализации, лежит в основе современных достижений в области обработки естественного языка. В табл. 1 описаны основные компоненты, составляющие каждую большую языковую модель, и функции каждого из них.

Таблица 1

Ключевые компоненты LLM

Компонент	Назначение
Токенизация	Разбивает текст на подслова/символы
Маска внимания	Управляет видимостью токенов (например, для паддинга/авторегрессии)
KV-кэш	Сохраняет предыдущие состояния внимания (оптимизация инференса)
Адаптеры LoRA	Облегчённые слои для тонкой настройки (снижают потребление памяти)

Генерация выходного текста реализуется через авто-регрессивный процесс [13, 14]: модель последовательно предсказывает наиболее вероятные следующие токены, используя различные стратегии декодирования (жадный поиск для максимальной детерминированности, *beam search* для баланса качества и разнообразия, или вероятностное сэмплирование для творческих задач), при этом каждый новый токен рекурсивно включается в контекст для генерации последующих элементов, что обеспечивает когерентность и связность выходного текста.

Математическая основа описывается формулой (1):

$$\text{Attention}(Q, K, V) = softmax(\frac{QK^T}{\sqrt{d_k}})V, \quad (1)$$

где d_k – размерность ключевых векторов.

Далее приведены некоторые примеры для локальных больших языковых моделей.

2. Локальные открытые большие языковые модели (Local LLM). Локальные LLM демократизируют ИИ, предоставляя пользователям мощные инструменты прямо в их руки – хотя и с компромиссами в скорости и масштабируемости по сравнению с облачными аналогами. Ниже приводится описание набора распространенных локальных языковых моделей, которые будут использоваться в данном исследовании.

Llama 2 [4] – это большая языковая модель с открытым исходным кодом, разработанная компанией Meta совместно с Microsoft, которая предназначена для генерации и понимания текста на естественном языке. Она использует архитектуру трансформеров с авторегрессией и дополнительно обучается с помощью методов обучения с подкреплением и обратной связью от человека (RLHF), что повышает её безопасность и эффективность. Llama 2 доступна в различных вариантах с количеством параметров до 70 миллиардов и подходит для решения задач от программирования до творческого письма.

DeepSeek R1 [5] – представляет собой серию крупномасштабных языковых моделей (LLM), посвящённых созданию экономически эффективных ИИ-решений с улучшенными возможностями логического и эмерджентного мышления. В рамках серии были разработаны такие модели, как DeepSeek-LLM, DeepSeek-V2, DeepSeek-V3 и DeepSeek-R1, каждая из которых демонстрирует прогресс в области машинного обучения, особенно в крупномасштабном обучении с подкреплением (RL).

DeepSeek-R1 – это передовая LLM, оптимизированная для сложных логических и структурированных рассуждений. В отличие от традиционных подходов, она использует методы RL с минимальным предварительным обучением с учителем (включая режим «Zero Supervised Fine-Tuning»), что позволяет развивать расширенные способности к цепочечным рассуждениям (chain-of-thought) и саморефлексии. Модель применяет архитектуру смешанных экспертов (англ. *Mixture of Experts*, *MoE*), обеспечивая высокую эффективность и масштабируемость при решении задач в математике, программировании и логическом анализе.

DeepSeek-R1 успешно конкурирует с закрытыми коммерческими аналогами (такими как OpenAI o1), превосходя или соответствуя их показателям в тестах на логическое мышление, оставаясь при этом открытой, прозрачной и экономически выгодной альтернативой. Её способность наглядно демонстрировать ход рассуждений делает её особенно ценной для научных исследований и разработки ПО. Серия DeepSeek в целом иллюстрирует, как совместная оптимизация алгоритмов и аппаратного обеспечения может значительно повысить производительность LLM, способствуя демократизации передового ИИ.

Gemma [7] – это крупномасштабная языковая модель (LLM), разработанная для универсального применения в задачах обработки естественного языка. Модель выделяется высокой точностью в генерации текстов, понимании контекста и адаптации к различным стилям общения благодаря использованию современного трансформерного архитектурного подхода. Gemma применяется в широком спектре областей, включая автоматический перевод, создание контента и анализ текста, обеспечивая поддержу многоязычности и устойчивость к шуму данных.

Особенностью *Gemma* является сбалансированное сочетание производительности и ресурсной эффективности, что делает её удобной для интеграции в коммерческие и исследовательские проекты. Благодаря оптимизированным алгоритмам обучения, модель демонстрирует способность быстро обучаться на дополнительной информации и адаптироваться к новым задачам без значительных потерь качества. Это позволяет использовать Gemma как надёжный инструмент для ускорения работы с большими объёмами текстовой информации и улучшением качества взаимодействия с пользователями. Таким образом, Gemma представляет собой мощный и гибкий инструмент в арсенале современных LLM, сочетающий высокие показатели понимания текста с доступностью и удобством эксплуатации.

В целом, разницу между локальными и облачными LLM-моделями можно обобщить в следующих ключевых пунктах, представленных в табл. 2. Локальные модели обеспечивают приватность, оффлайн-работу и кастомизацию, но уступают в производительности и скорости. Облачные решения (например, GPT-4) предлагают высокую точность и минимальные задержки, однако зависят от сторонних серверов, платных API и интернет-соединения. Локальные модели дают полный контроль над данными, но требуют мощного железа, тогда как облачные легко масштабируются – ценой конфиденциальности и регулярных платежей.

Таблица 2

Сравнение: локальные и облачные LLM

Характеристика	**Локальные LLM (LLaMA 2, DeepSeek)**	**Облачные LLM (GPT-4, Claude)**
Конфиденциальность	✅ Данные не покидают устройство	❌ Обработка на сторонних серверах
Оффлайн-работа	✅ Полная функциональность без интернета	❌ Требуется постоянное подключение
Производительность	⚠ Зависит от мощности оборудования	✅ Максимальная производительность
Кастомизация	✅ Полная свобода модификации	❌ Ограничена провайдером
Стоимость	✅ Разовые затраты на оборудование	❌ Плата за использование (подписка)
Масштабируемость	⚠ Ограничена локальными ресурсами	✅ Автоматическое масштабирование
Точность	⚠ Хорошая, но ниже облачных аналогов	✅ Передовые результаты

Для локального запуска больших языковых моделей (LLM) на ПК используется Ollama – это платформа для локального запуска открытых языковых моделей (LLM), таких как Llama2, llama2 и DeepSeek, на macOS, Linux и Windows. Она упрощает развертывание, объединяя веса моделей, конфигурации и данные в готовые оптимизированные пакеты с поддержкой GPU-ускорения.

3. Постановка задачи. Дан набор текстовых документов $\boldsymbol{D} = \{d_1, d_2, ..., d_{|D|}\}$, требующих классификации по заданным категориям (классам) $\boldsymbol{C} = \{\mathbf{c_1, c_2, ..., c_{|C|}}\}$.

Первичная классификация, выполняется с помощью традиционной модели (например, SBERT), которая выявляет подмножество документов с ошибочной классификацией. Для неверно классифицированных документов необходимо оценить точность больших языковых моделей (LLM) в анализе текстового содержания и корректном отнесении документов к истинным категориям.

Задача классификации заключается в построении аппроксимирующей функции $\boldsymbol{\Phi'}$, максимально приближенной к целевой функции $\boldsymbol{\Phi: D \times C \rightarrow \{0, 1\}}$, определяющая принадлежность документа к категории (1 – принадлежит, 0 – не принадлежит). Для решения данной задачи используются методы машинного обучения, которые опираются на наличие коллекции заранее классифицированных документов $\boldsymbol{\Omega} = \{d_1, d_2, ..., d_{|\Omega|}\}$.

Тогда задача состоит в нахождении такой функции $\boldsymbol{\Phi'}$, которая минимизирует суммарные потери на коллекции $\boldsymbol{\Omega}$:

$$\min_{\Phi'} \sum_{\mathbf{d} \in \Omega} \mathbf{L}(\Phi(\mathbf{d}), \Phi'(\mathbf{d})),$$

где $\mathbf{L}(\Phi(\mathbf{d}), \Phi'(\mathbf{d}))$ – функция потерь, оценивающая качество аппроксимации $\boldsymbol{\Phi'}$ относительно $\boldsymbol{\Phi}$ для документа $\mathbf{d}$.

Результаты позволят определить, может ли дополнение традиционных моделей LLM повысить точность классификации, или же требуются гибридные подходы для баланса между точностью, эффективностью и затратами.

4. Архитектура чат-бота для классификации текста с использованием локальных LLM. В данном разделе представлено проектирование чат-бота на основе LLM, предназначенного для классификации пользовательских текстов на одну из $\boldsymbol{N}$ предопределенных категорий с использованием локально размещенных больших языковых моделей (LLM), таких как DeepSeek, Gemma и llama2. Система использует *Ollama* для локального вывода моделей и *FastAPI* [15] для обеспечения структурированного *backend API*, обеспечивающего взаимодействие между пользовательским интерфейсом и языковыми моделями (рис. 2).

1. Пользовательский интерфейс (фронтенд), доступный через веб-приложение или командную строку, обеспечивает ввод текста и отображение результатов классификации.

2. Бэкенд на FastAPI выступает центральным связующим звеном, предоставляя RESTful API для выбора моделей (DeepSeek, Gemma или Llama 2), обработки текстовых запросов и мониторинга состояния системы, с обязательной валидацией данных через Pydantic.

3. Интеграция с Ollama (Слой вывода LLM): Система взаимодействует с локальным сервером вывода Ollama (localhost:11434), отправляя хорошо структурированные промпты выбранной языковой модели для обеспечения согласованного вывода классификации. Полученные сырые ответы модели обрабатываются для извлечения предсказанной категории, что гарантирует согласованный формат вывода.

4. Инженерия промптов (англ. Prompt engineering) – это методика, заключающаяся в тщательном формулировании инструкций для оптимального управления выводом больших языковых моделей (LLM) с целью получения желаемых результатов [16, 17]. В нашем исследовании промпты разрабатываются для работы в условиях zero-shot обучения, где:

1. *Метод Zero-Shot (ZS)*: В данном подходе модель получает исключительно базовую инструкцию для выполнения задачи, без каких-либо дополнительных указаний или примеров. В таких условиях языковая модель опирается исключительно на свои предварительно полученные знания в ходе предобучения (pre-training), чтобы сгенерировать ответ [18, 19].

2. *Метод Few-Shot (FS)*: В отличие от Zero-Shot, этот метод предоставляет модели не только основную инструкцию, но и небольшое количество демонстрационных примеров (обычно от 2 до 5), которые помогают "настроить" её понимание задачи и улучшить качество ответа.

Инженерия промптов для классификации: Входной текст преобразуется в строго формализированный промпт, явно инструктирующий LLM отнести текст к одной из пяти предопределенных категорий. Промпт специально ограничивает ответ модели только названием категории, исключая избыточные объяснения. Пример промпта:

```
22      def generate_answer(self, model, user_input: str, categories) -> str:
23          """Generate answer using Ollama """
24          prompt = f"""
25          Classify the following text into one of these categories: {', '.join(categories)}.
26          Text: {user_input}
27          Respond ONLY with category name.
28          """
```

Рис. 1. Пример промпта для классификации текста

Для повышения эффективности система реализует LRU-кэш (Least Recently Used, наименее недавно использованный), сохраняющий результаты последних классификаций и минимизирующий избыточные запросы к LLM при повторяющихся входах.

На представленной схеме (рис. 2) детально отображен процесс обработки запросов в системе классификации текста. Архитектура реализует последовательный рабочий процесс (англ. workflow), начинающийся с этапа взаимодействия пользователя с фронтенд-интерфейсом, и заканчивая получением результата классификации.

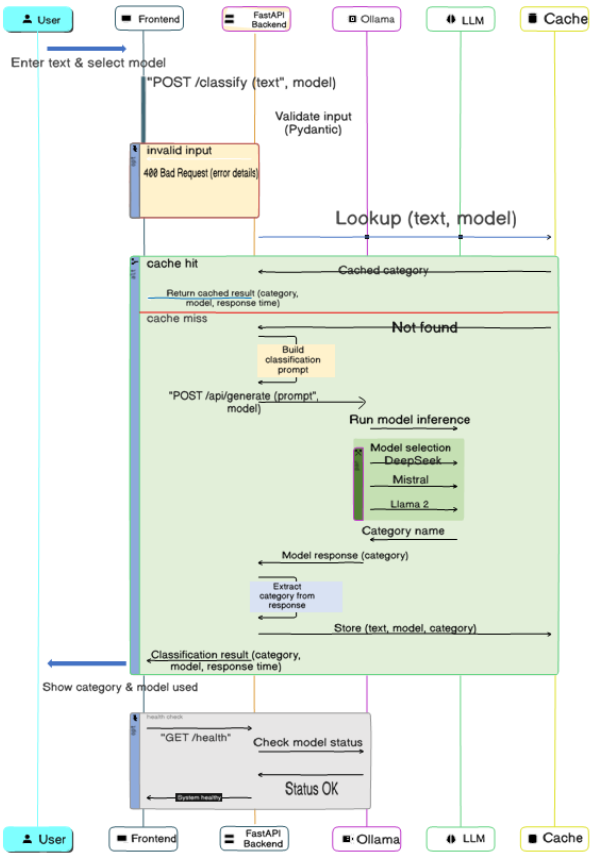


Рис. 2. Процесс обработки запросов в системе классификации текста

Пользователь отправляет текст через фронтенд-интерфейс, указывая предпочитаемую языковую модель. Полученный запрос поступает в FastAPI бэкенд, где происходит валидация входных данных и формирование структурированного промпта для классификации. Сформированный промпт передается в Ollama, которая выполняет локальный вывод выбранной LLM-модели. После обработки запроса Ollama возвращает сырой ответ модели в виде названия категории.

На стороне бэкенда осуществляется извлечение предсказанной категории из ответа модели. При активированном механизме кэширования результат сохраняется для оптимизации обработки идентичных запросов в будущем.

Окончательный результат, содержащий название категории, информацию о используемой модели и времени отклика, отправляется обратно во фронтенд, где отображается пользователю.

Развертывание моделей. Для корректной работы системы необходимо предварительно запустить локальный сервер Ollama с загруженными моделями (DeepSeek, Gemma, Llama 2). Сервер FastAPI должен быть развернут с реализацией механизмов обработки ошибок на случай недоступности Ollama или отсутствия требуемых моделей.

Данная архитектура обеспечивает гибкую и эффективную структуру для развертывания локально размещенного чат-бота для классификации текста на основе LLM. Используя FastAPI для бэкэнд-коммуникации и Ollama для локального вывода, система обеспечивает конфиденциальность, низкую задержку и офлайн-функциональность. Будущие улучшения могут включать тонкую настройку моделей для лучшей точности классификации, интеграцию более сложного фронтенда и сравнительный анализ производительности в различных конфигурациях оборудования.

5. Вычислительный эксперимент и анализ полученных результатов. Для проведения эксперимента и оценки рассматриваемых методов в задаче классификации текстов использовался набор данных BBC [20], который включает 2225 документов, полученных с веб-сайта новостей *BBC* за период 2004-2005 гг. (табл. 3). Набор данных охватывает пять тем: спорт (Sport, S), бизнес (Business, B), развлечения (entertainment, E), политику (Politics, P) и технологии (Tech, T).

Таблица 3

Набор использованных данных BBC

Набор данных	***BBC***
Количество документов	2225
Количество категорий	5
Среднее количество слов в документе	2262
Среднее количество словарных слов в одном документе	207

Для реализации классификатора на основе традиционных методов векторизации были выбраны SBERT, BoWC и TF-IDF для построения векторов документов набора данных BBC. В качестве классификатора был выбран алгоритм опорных векторов (SVM) на основе результатов предыдущих работ авторов [9–11].

Также, реализован классификатор на основе больших языковых моделей, использующий архитектурное решение, подробно описанное в разделе 2. Экспериментальная оценка проводилась для следующих современных больших языковых моделей:

Gemma3:1b – это предпоследняя версия модели Gemma3, представляющая собой наиболее производительный вариант, способный эффективно работать на одной видеокарте (GPU).

DeepSeek-R1:7b (DS-r1:7b) и DeepSeek-R1:1.5b (DS-r1:1.5b) – это версии крупномасштабной языковой модели DeepSeek-R1, разработанные с использованием методов обучения с подкреплением для улучшения рассуждений и решения сложных задач в математике, программировании и логике. DeepSeek-R1 показывает производительность,

сопоставимую с OpenAI-o1, и включает модели с разным числом параметров, в том числе версии 1.5B и 7B, которые являются уменьшенными дистиллятами оригинальной модели, обеспечивая хорошую производительность при меньших вычислительных ресурсах и оставаясь открытыми и доступными для коммерческого использования

Llama2:7B – это одна из моделей серии Llama 2, представляющая собой крупномасштабную языковую модель с 7 миллиардами параметров, разработанную Meta.

Метрика оценки классификации. F-мера – одна из распространенных метрик для оценки успешности классификатора [21]. Это среднее гармоническое между точностью и полнотой, которое определяется следующими формулами:

$$\text{Precision}_{C_i} = \frac{\text{TP}_{C_i}}{\text{TP}_{C_i}+\text{FP}_{C_i}}, \quad (1)$$

$$\text{Recall}_{C_i} = \frac{\text{TP}_{C_i}}{\text{TP}_{C_i}+\text{FN}_{C_i}}, \quad (2)$$

$$\text{мера } F1 = \frac{(1+\beta)\cdot\text{Precision}_{C_i}\cdot\text{Recall}_{C_i}}{\beta\cdot\text{Precision}_{C_i}+\text{Recall}_{C_i}}. \quad (3)$$

Здесь C – это метка класса, True Positive TP – это количество документов, правильно отмеченных классификатором как относящиеся к классу C, а False Positive FP – это количество документов, неправильно отмеченных классификатором как относящиеся к классу C. Между тем, False Negative FN ложноотрицательный – это количество документов, которые относятся к классу C и которые классификатор ошибочно определил как не относящиеся к классу C, а True Negative TN – это количество документов, не принадлежащих к классу C, правильно отмеченных классификатором как не относящиеся к классу C.

Результаты. В табл. 4 представлены сравнительные результаты классификации документов из набора данных BBC, полученные с использованием традиционных методов векторизации текстов. Наибольшую эффективность продемонстрировали методы SBERT и BoWC, что подтверждается метриками точности по мере F1.

Таблица 4

Точность классификации документов по мере F1

Метод (размер вектора)	мера F1 (%)
SBERT (768)	98.2
BoWC (200)	98.2
TF-IDF (26000)	97.89

На основе проведенного анализа были выделены 13 ошибочно классифицированных документов, которые вместе с перечнем пяти возможных категорий были переданы чат-боту для оценки способности больших языковых моделей (LLM) корректно определять категории текстов.

Несмотря на эффективность больших языковых моделей (LLM) в анализе текста, они не смогли корректно классифицировать все документы, используя только названия категорий. В табл. 5 и 6 представлены результаты классификации документов, с которыми традиционные методы обработки допустили ошибки. В табл. 5 показана точность каждой модели, а также объем используемой модели для вычислений. С другой стороны, в таблице 6 показаны подробные сведения о метках классов для каждой модели в сравнении с правильными метками.

Модель DeepSeek-R1:1.5b демонстрирует более высокую точность классификации документов по сравнению с DeepSeek-R1:7b. Однако данное наблюдение отражает не абсолютное превосходство архитектуры, а специфику анализа семантических признаков, существенных для конкретной задачи категоризации.

Таблица 5

Точность классификации выборки документов с использованием локальных LLM, измеренная мерой F1

Модель LLM	Размер модели (ГБ)	F1 (%)
Gemma3:1b	0.82	39.23
Deepseek r1:1.5b	1.1	**41.76**
Deepseek-r1:7b	4.7	35.77
Llama2:7b	4	15.38

Отмечается также, что модель Gemma, несмотря на свой небольшой размер (0,82 ГБ), обеспечивает баланс между точностью и потреблением памяти по сравнению с DeepSeek в обеих версиях.

Интересно, что существуют документы, которые все языковые модели классифицируют ошибочно. Например, в случае с документом 12 четыре модели вместе с традиционными методами (BoWC, SBERT) единогласно отнесли его к категории «политика», тогда как на самом деле он принадлежит к классу «развлечения». Это вызывает сомнения в правильности меток, установленных экспертами.

Таблица 6

Метки классов для каждой модели, по сравнению с правильными метками

	Метка класса	SBERT	BoWC	DS-r1:7b	Gemma	DS-r1:1.5b	Llama2
0	B	T	T	B	T	B	T
1	E	T	T	E	E	E	T
2	P	B	B	P	T	P	P
3	E	T	T	B	**S**	E	T
4	E	**T**	**T**	**B**	**B**	**T**	**T**
5	T	E	E	E	T	E	T
6	B	T	T	T	B	T	T
7	B	**T**	**T**	**P**	**P**	**T**	**T**
8	B	P	P	P	P	T	P
9	P	T	T	P	T	P	P
10	B	P	P	P	B	P	P
11	P	B	B	P	P	B	P
12	**E**	**P**	**P**	**P**	**T**	**P**	**P**

Для анализа ошибочной классификации документа (12) к категории "политика" вместо "развлечения" мы исследовали цепочку рассуждений (Chain-of-Thought) модели DeepSeek-к1:7b. Кроме того, чат-боту был задан следующий аналитический вопрос: «Какие признаки в тексте заставили вас отнести этот контент к политике, а не к бизнесу (business)?» Образец ответа чат-бота (Deepseek-r1: latest) на вопрос представлен на рис. 3.

Проведенный анализ свидетельствует, что языковые модели демонстрируют удовлетворительную, но не оптимальную эффективность классификации. Результаты указывают на необходимость пересмотра эталонной разметки в стандартных наборах данных. Несмотря на способность LLM анализировать категории (что подтверждается chain-of-thought рассуждениями), их точность при работе исключительно с названиями классов остается ограниченной. Для улучшения показателей рекомендуется: Few-Shot обучение с демонстрационными примерами, расширенные описания категорий, включающие семантические маркеры и пограничные случаи.

Что касается времени выполнения, были зафиксированы временные затраты каждой модели на обработку указанных документов. Анализ показал, что все протестированные модели демонстрируют четкую положительную корреляцию между объемом текста и временем выполнения, однако степень этой зависимости значительно варьируется (рис. 4).

[Вот анализ ключевых признаков, которые определили классификацию текста как "политика", а не "бизнес":
1. Государственные институты и политические решения
- Упоминание Pensions Policy Institute (PPI) — аналитического центра, влияющего на госполитику
- Ссылка на отчет Pensions Commission — официального органа по реформе пенсий
- Предложения о "гражданской пенсии" — изменение законодательной системы
2. Фокус на социально-экономической политике
- Обсуждение госгарантий (госпенсия vs. частные накопления)
- Темы неравенства и бедности — классические политические вопросы
- Варианты реформ через налоги или повышение пенсионного возраста — инструменты госрегулирования
3. Отсутствие бизнес-контекста
Нет признаков, характерных для категории "бизнес":
- Не анализируются корпоративные пенсионные программы
- Нет данных о рынке финансовых услуг
- Не упоминаются компании или прибыльность реформ
Пример из текста:
"Замена госпенсии на гражданскую пенсию сократит неравенство" — это политическое предложение, так как:
1. Требует изменений в законах
2. Нацелено на общественное благо
3. Инициируется госорганами
Для отнесения к "бизнесу" текст должен содержать:
- Анализ влияния на частные пенсионные фонды
- Финансовые показатели страховых компаний
- Рыночные механизмы (например, инвестиционные варианты)]

Рис. 3. Ответ чат-бота (Deepseek-r1: latest)

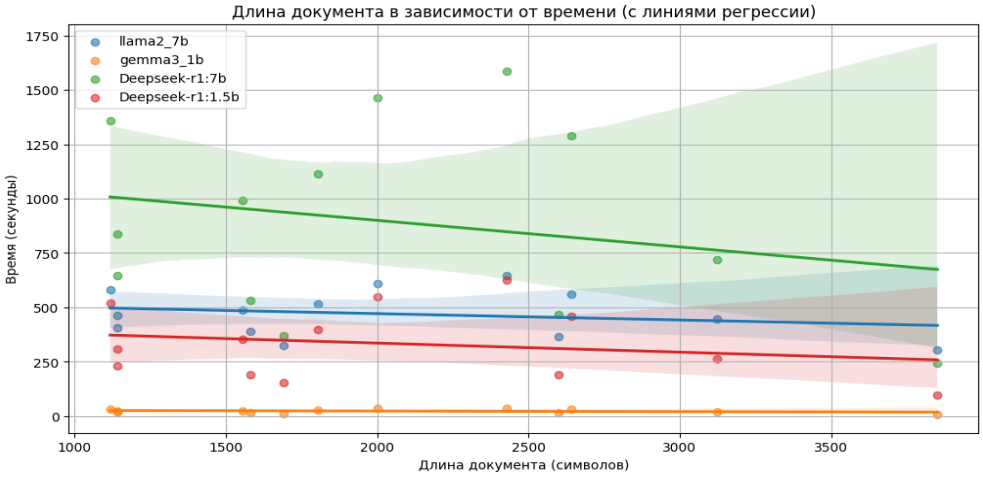


Рис. 4. Зависимость времени выполнения от длины документа

Наиболее выраженная чувствительность наблюдается у Deepseek-r1:7b, где увеличение длины документа приводит к практически линейному росту времени обработки. В противоположность этому, *Gemma* показывает удивительную стабильность работы,

демонстрируя наименьшую зависимость от объема текста. В будущих работах планируется систематически исследовать корреляцию времени обработки с: (1) длиной текста, (2) параметризацией модели и (3) характеристиками аппаратной платформы.

Заключение. В данной статье разработан интеллектуальный чат-бот с комплексным анализом его архитектуры и возможностей обработки текста, а также проведена оценка производительности локальных языковых моделей. Основное внимание уделялось анализу эффективности этих моделей при выполнении традиционных задач, таких как классификация текстов с использованием метода "одиночного примера" (One-Shot). Несмотря на значительный прогресс в аналитических возможностях этих моделей, они не смогли корректно классифицировать все документы. Примечательно, что увеличение размера модели – что предположительно должно повышать точность – не привело к значительному улучшению классификации, а в некоторых случаях даже вызвало снижение производительности. В этом контексте модель *Gemma* выделилась как оптимальный вариант с точки зрения баланса между размером модели и точностью классификации. Исследование также проанализировало взаимосвязь между временем выполнения и длиной текста, выявив положительную корреляцию между этими параметрами. В будущих исследованиях планируется более глубокий анализ этого аспекта, включая влияние других факторов, таких как архитектура модели и возможности тонкой настройки (Fine-Tuning) для улучшения производительности. Также будет проведена проверка достоверности экспертных меток в эталонных наборах данных для задач классификации текстов на естественных языках.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *OpenAI, J. Achiam, S. Adler, S. Agarwal, L. Ahmad, B. Zoph [et al.]*. OpenAI. GPT-4 Technical Report, 2024.
2. *Baktash J.A., Dawodi M.* Gpt-4: A Review on Advancements and Opportunities in Natural Language Processing, 2023.
3. *Allahyari M., Pouriyeh S., Assefi M., Safaei S., Trippe E.D., Gutierrez J.B., Kochut K.* A brief survey of text mining: Classification, clustering and extraction techniques, 2017.
4. *Roumeliotis K.I., Tselikas N.D., Nasiopoulos D.K.* Llama 2: Early Adopters' Utilization of Meta's New Open-Source Pretrained Model, 2023.
5. *DeepSeek-AI., Guo D., Yang D., Zhang H., Song J., Zhang Z. [et al.]*. DeepSeek-R1: Incentivizing Reasoning Capability in LLMs via Reinforcement Learning, 2025.
6. *Zhang C., Deng Y., Lin X., Wang B., Ng D., Ye H., Li X., Xiao Y., Mo Z., Zhang Q., Bing L.* 100 Days After DeepSeek-R1: A Survey on Replication Studies and More Directions for Reasoning Language Models, 2025.
7. *Team G., Mesnard T., Hardin C., Dadashi R., Bhupatiraju S., Kenealy K. [et al.]*. Gemma: Open Models Based on Gemini Research and Technology, 2024.
8. *Reimers N., Gurevych I.* Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks, *arXiv preprint arXiv,* 2019, Vol. abs/1908.10084.
9. *Mansour A., Mohammad J., Kravchenko Y., Kravchenko D., Silega N.* Harnessing Key Phrases in Constructing a Concept-Based Semantic Representation of Text Using Clustering Techniques, *International Workshop on Artificial Intelligence and Pattern Recognition*. Springer, 2023, pp. 190-201.
10. *Mansour A., Mohammad J., Kravchenko Y.* Text Vectorization Method Based on Concept Mining Using Clustering Techniques, *2022 VI International Conference on Information Technologies in Engineering Education (Inforino)*. IEEE, 2022, pp. 1-10.
11. *Mansour A.M., Mohammad J.H., Kravchenko Y.A.* Text vectorization using data mining methods, *Izvestia SFedU. Technical science,* 2021, No. 2.
12. *Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A.N., Kaiser Ł., Polosukhin I.* Attention is all you need, *Advances in neural information processing systems,* 2017, Vol. 30.
13. *Franceschelli G., Musolesi M.* Creative Beam Search: LLM-as-a-Judge For Improving Response Generation, 2024.
14. *Pryzant R., Iter D., Li J., Lee Y.T., Zhu C., Zeng M.* Automatic Prompt Optimization with "Gradient Descent" and Beam Search, 2023.
15. *Adeshina A.A.* Building Python Web APIs with FastAPI: A fast-paced guide to building high-performance, robust web APIs with very little boilerplate code. Packt Publishing Ltd, 2022.

16. *Giray L.* Prompt engineering with ChatGPT: a guide for academic writers, *Annals of biomedical engineering,* 2023, Vol. 51, No. 12. pp. 2629-2633.
17. *Marvin G., Hellen N., Jjingo D., Nakatumba-Nabende J.* Prompt Engineering in Large Language Models, *Data Intelligence and Cognitive Informatics: Algorithms for Intelligent Systems,* eds. I.J. Jacob, S. Piramuthu, P. Falkowski-Gilski. Singapore: Springer Nature Singapore, 2024, pp. 387-402. ISBN 978-981-9979-99-8.
18. *Mahmoud Bsharat S., Myrzakhan A., Shen Z.* Principled Instructions Are All You Need for Questioning LLaMA-1/2, GPT-3.5/4, *arXiv e-prints,* 2023, pp. arXiv-2312.
19. *Mann B., Ryder N., Subbiah M., Kaplan J., Dhariwal P., Neelakantan A., Shyam P., Sastry G., Askell A., Agarwal S.* Language models are few-shot learners, *arXiv preprint arXiv:2005.14165,* 2020, Vol. 1, pp. 3.
20. *Sabbah T., Selamat A., Selamat M.H., Al-Anzi F.S., Viedma E.H., Krejcar O., Fujita H.* Modified frequency-based term weighting schemes for text classification, *Applied Soft Computing,* 2017, Vol. 58, pp. 193-206.

Мансур Али Махмуд – Южный федеральный университет; e-mail: mansur@sfedu.com; г. Таганрог, Россия; тел.: +79880158697; кафедра систем автоматизированного проектирования им. В.М. Курейчика; программист.

Мохаммад Жуман Хуссайн – Южный федеральный университет; e-mail: zmohammad@sfedu.ru; г. Таганрог, Россия; тел.: +79880158697; кафедра систем автоматизированного проектирования им. В.М. Курейчика; соискатель.

Кравченко Юрий Алексеевич – Южный федеральный университет; e-mail: yakravchenko@sfedu.ru; г. Таганрог, Россия; тел.: +79289080151; кафедра систем автоматизированного проектирования им. В.М. Курейчика; профессор.

Mansour Ali Mahmoud – Southern Federal University; e-mail: mansur@sfedu.com; Taganrog, Russia; phone: +79880158697; the Department of Computer Aided Design named after V.M. Kureichik; programmer.

Mohammad Juman Hussain – Southern Federal University; e-mail: zmohammad@sfedu.ru; Taganrog, Russia; phone: +79880158697; the Department of Computer Aided Design named after V.M. Kureichik; applicant.

Kravchenko Yury Alekseevich – Southern Federal University; e-mail: yakravchenko@sfedu.ru; Taganrog, Russia; phone: +79289080151; the Department of Computer Aided Design named after V.M. Kureichi; professor.

УДК 621.396.969 DOI 10.18522/2311-3103-2025-3-171-180

В.А. Деркачев

КЛАССИФИКАЦИЯ РАДИОЛОКАЦИОННЫХ ИЗОБРАЖЕНИЙ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ МУЛЬТИРОТОРНОГО ТИПА С ПРИМЕНЕНИЕМ АЛГОРИТМА YOLO11

Рассматривается классификатор радиолокационных изображений беспилотных летательных аппаратов, основанный на нейронной сети, построенной на алгоритме YOLO 11 версии. Решение задачи обнаружения и классификации беспилотных летательных аппаратов стало одной из приоритетных задач в настоящее время. Увеличение числа модификаций беспилотных летательных аппаратов сильно усложняет применение статистических методов классификации, что требует применения новых подходов в решении задачи классификации. Развитие нейросетевых методов, одновременно с увеличением производительности вычислителей для обучения, с одной стороны, и встраиваемых решений, с другой, позволяет осуществлять классификацию летательных аппаратов с применением радиолокационных изображений в реальном масштабе времени. Применение алгоритма YOLO11 позволяет, помимо определения класса цели, осуществить оценку дальности до наблюдаемого объекта. Использование радиолокационных изображений оправданно в связи с тем, что визуальное наблюдение не всегда является возможным, из-за сложных погодных условий и темного времени суток. Для обучения нейронной сети предполагается использовать набор радиолокационных изображений, полученный с применением авторской модели генерации данных с произвольной конфигурацией беспилотных летательных аппаратов. Проведено обучение

нейронной сети класса Detection YOLO11s (9,4 млн. параметров) на выборке радиолокационных изображений двух классов общим числом 8192. В результате обучения получена точность 0,99 для классификации на 2 классах объектов (на тестовых модельных данных). Были проведены тесты с применением натурных данных, снятых с применением радиолокационной системы миллиметрового диапазона TI IWR1642, в результате которых достигнута безошибочная классификация объектов на малой выборке.

Классификатор; беспилотный летательный аппарат; радиолокационное изображение; нейронная сеть; БПЛА.

V.A. Derkachev

CLASSIFICATION OF RADAR IMAGES OF MULTI-ROTOR UNMANNED AERIAL VEHICLES USING THE YOLO11 ALGORITHM

This article discusses a classifier of radar images of unmanned aerial vehicles based on a neural network built on the YOLO algorithm version 11. Solving the problem of detecting and classifying unmanned aerial vehicles has become one of the priority tasks at present. The increase in the number of modifications of unmanned aerial vehicles greatly complicates the use of statistical classification methods, which requires the use of new approaches to solving the classification problem. The development of neural network methods, simultaneously with an increase in the performance of computers for training, on the one hand, and embedded solutions, on the other, allows for the classification of aircraft using radar images in real time. The use of the YOLO11 algorithm allows, in addition to determining the class of the target, to estimate the range to the observed object. The use of radar images is justified due to the fact that visual observation is not always possible due to difficult weather conditions and darkness. To train the neural network, it is proposed to use a set of radar images obtained using the author's model of data generation with an arbitrary configuration of unmanned aerial vehicles. The neural network of the Detection YOLO11s class (9.4 million parameters) was trained on a sample of radar images of two classes, a total of 8192. As a result of training, an accuracy of 0.99 was obtained for classification in 2 classes of objects (on test model data). Tests were conducted using natural data taken using the TI IWR1642 millimeter-range radar system, as a result of which error-free classification of objects on a small sample was achieved.

Classifier; unmanned aerial vehicle; radar image; neural network; UAV.

Введение. В последнее время к проблеме обнаружения и классификации беспилотных летательных аппаратов (БПЛА) наблюдается повышенный интерес [1, 2]. Задача классификации беспилотных летательных аппаратов с применением средств радиолокации может решаться применением двух подходов: статистического и нейросетового. Наиболее часто используемые статистические методы: корреляционный [3] и с применением оптимальных байесовских классификаторов [4]. Применение статистических методов является достаточно сложной задачей, ввиду необходимости выделения отдельных признаков в классифицируемых данных, особенно при наличии сложной структуры радиолокационного изображения. Прогресс в развитии архитектур нейронных сетей обработки данных в последние годы позволяет создавать классификаторы радиолокационных изображений [5–7].

В работе [8] описан алгоритм обнаружения с применением на основе сверточных нейронных сетей и профилей, полученных из дальностно-скоростных матриц. В статьях [9, 10] показана возможность классификации БПЛА с применением дальностно-скоростных изображений и различных архитектур нейронных сетей. В приведенных работах обучение и тестирование нейронных сетей осуществлялось на данных, полученных в результате натурных экспериментов.

Применение нейронных сетей приводит к необходимости формирования данных для обучения. В случае БПЛА можно осуществить генерацию дальностно-скоростных портретов мультироторных БПЛА с заданными параметрами (геометрией, скоростью полета, размером и расположением винтов) используя авторскую методику [11, 12]. Применяя последнюю версию архитектуры YOLO11 в паре с вышеупомянутым алгоритмом, становится возможно создать классификатор мультироторных БПЛА, имеющий возможность работы в реальном времени на мобильных устройствах [13, 14].

Постановка задачи. В данной работе необходимо осуществить создание классификатора БПЛА с применением нейронных сетей. В качестве обучающих данных применялись радиолокационные изображения синтезировались с применением авторской мето-

дики. Применение синтезированных изображений обусловлено необходимостью использования большого объема данных для обучения нейронной сети, что требует больших материальных и трудовых затрат. В качестве архитектуры нейронной сети используется YOLO11, которая совместима с набором синтезированных изображений. Тестирование проводилось с применением РЛС миллиметрового диапазона, что обусловило выбор параметров для синтеза радиолокационных изображений. Решаемую задачу можно разбить на два этапа. Первый этап – формирование набора радиолокационных изображений необходимых для обучения нейронной сети. Второй этап заключается в обучении нейронной сети и тестировании полученного классификатора.

Описание архитектуры нейронной сети. Обнаружение и классификация объектов является неотъемлемой частью компьютерного зрения. В настоящее время достигнуты большие успехи в развитии данной технологии в связи с развитием нейросетевых методов обработки визуальной информации [15]. Одним из представителей данного класса нейронных сетей является алгоритм You Only Look Once (YOLO) [16]. YOLO v1 использовал механику разделения изображения на сегменты и прогнозирования вероятностей классов для каждого сегмента [17]. Далее в версиях 2 и 3 были добавлены пакетная нормализация, опорные блоки и обнаружение с изменением размера окна [18], дальнейшие версии (с 4 по 7) были направленны на улучшения скорости, вычислительной эффективности, точности [19]. В YOLO v8 была представлена поддержка сегментации, отслеживания и механизмы обнаружения без привязки к опорным блокам, тем самым увеличивая эффективность обобщения данных при обучении [20].

Архитектура YOLO11 представлена в 2024 году, показана структурная схема модели показана на рис. 1 [21]. Данная версия основана на версии YOLOv8, и как предшественница включает многочисленные приложения, такие как обнаружение объектов, сегментация экземпляров, классификация изображений, оценка позы и ориентированное обнаружение объектов.

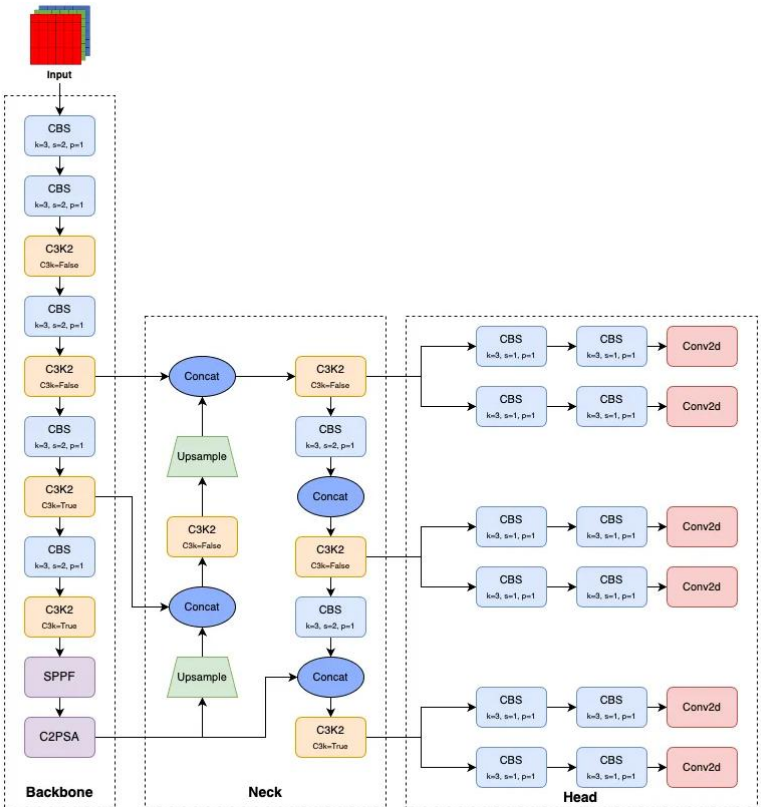


Рис. 1. Архитектура нейронной сети YOLO11

В архитектуре YOLO11 можно выделить 3 основные части: Backbone, Neck и Head. Backbone – это важнейший компонент архитектуры YOLO, отвечающий за извлечение признаков из входного изображения в нескольких масштабах. Этот процесс включает в себя наложение сверточных слоев и специализированных блоков для генерации карт признаков в различных разрешениях [22]. Neck объединяет признаки в разных масштабах и передает их в Head для прогнозирования. Head YOLOv11 отвечает за генерацию окончательных прогнозов с точки зрения обнаружения и классификации объектов. Она обрабатывает карты признаков, переданные из шеи, в конечном итоге выводя ограничивающие рамки и метки классов для объектов на изображении.

Архитектура YOLO11 представлена в виде 5 различных классов нейросетей: обнаружения (Detection, COCO), сегментации (Segmentation, COCO), классификации (Classification, ImageNet), оценки позы (Pose, COCO), ориентированного обнаружения (OBB, DOTAv1). В рамках задачи обнаружения и классификации радиолокационного изображения БПЛА на дальностно-скоростных портретах наиболее подходящей является нейросеть обнаружения (Detection, COCO). Выбранный класс архитектуры YOLO11 так же имеет 5 вариантов нейросетей различающихся числом параметров, а, соответственно, точностью, скоростью исполнения и требованиям к аппаратному обеспечению. В табл. 1 показаны основные характеристики нейросетей обнаружения архитектуры YOLO11. В представленной таблице фигурирует параметр mAPval 50-95, который является средней точностью, рассчитанной по пороговым значениям IoU (метрики степени пересечения между двумя ограничивающими рамками) от 0,5 до 0,95.

Таблица 1

Модель	mAPval 50-95	Кол-во параметров (млн.)	Сложность (GFLOPS)
YOLO11n	39,5	2,6	6,5
YOLO11s	47,0	9,4	21,5
YOLO11m	51,5	20,1	68,0
YOLO11l	53,4	25,3	86,9
YOLO11x	54,7	56,9	194,9

Формирование данных для обучения. Данные для обучения нейросети получены с применением авторского алгоритма формирования радиолокационных сигналов от БПЛА [11, 12, 23]. Обобщенная схема алгоритма показана на рис. 2.

Рис. 2. Обобщенный алгоритм построения радиолокационных изображений

В качестве радиолокационной системы выбрана РЛС миллиметрового диапазона TI IWR1642, основные параметры моделирования радиолокационного сигнала показаны в табл. 2.

Таблица 2

Параметр	Величина
Центральная частота сигнала	77 ГГц
Ширина спектра сигнала (используемая)	767,54 МГц
Частота дискретизации ВЧ	1,6 ГГц
Число периодов ЛЧМ импульсов	128
Длительность ЛЧМ импульса	60 мкс
Период ЛЧМ импульсов	160 мкс
Частота дискретизации АЦП	10 МГц
Число отсчетов АЦП за один период	256
Время моделирования	20 мс

Для обучения было выбрано 2 класса БПЛА Xiaomi Mi Drone Mini (рис. 3,а) и DJI Mavic2 PRO (рис. 3,б), основные характеристики данных БПЛА представлены в табл. 3.

а б

Рис. 3. Моделируемые БПЛА

Таблица 3

Параметр	Величина	
	Xiaomi Mi Drone Mini	DJI Mavic2 PRO
Число лопастей на роторе	2	2
Число роторов	4	4
Длина лопасти	0,038 м	0,107 м
Радиус оси ротора	0,0025 м	0,011 м
Ширина лопасти	0,005 м	0,022 м
Частота вращения лопастей	±100 Гц	±100 Гц

В результате работы модели формируются радиолокационные изображения без шума, далее добавляется шум с нецентральным χ^2-распределением, ОСШ при этом составляет 10 дБ. Далее сформированные изображения разрешением 128x128 точек интерполируются до разрешения 640x640 точек. Необходимость в этом связана с требованиями к входным данным нейронной сети и достаточно высокой вычислительной сложностью алгоритма формирования изображений. Для обучения генерируется по 4096 изображений каждого из классов, примеры полученных изображений показаны на рис. 4.

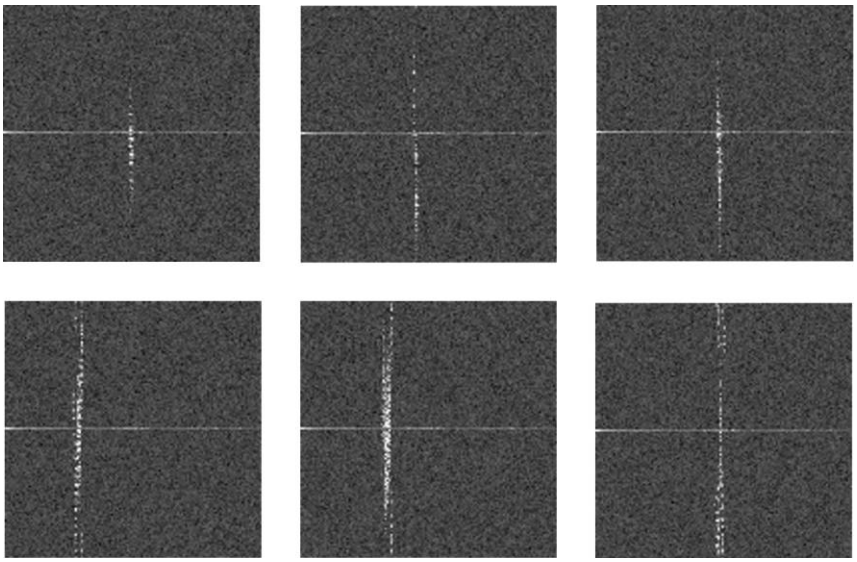


Рис. 4. Формируемые РЛИ

Обучение нейронной сети. Обучение нейронной сети производилось с применением библиотеки Ultralytics версии 8.3.72 построенной на основе библиотеки PyTorch версии 2.4.1+cu124. Моделируемые РЛИ, полученные в предыдущем разделе, разделены на 3 выборки: обучающую состоящую из 5734 изображения 2 классов (70% от всех изображений), валидационную, состоящую из 820 изображений 2 классов (10% от всех изображений) и тестовую, состоящую из 1638 изображений 2 классов (20% от всех изображений). Для обучения был выбран варианта YOLO11s, число эпох обучения 100. Время обучения составило 1,5 часа с применением видеокарты Nvidia RTX3090.

Анализ матрицы ошибок

Матрица ошибок (рис. 5) дает полное представление о точности классификации YOLO11 по различным типам БПЛА. Нейросеть демонстрирует высокую точность для определения всех классов, достигая высоких показателей классификации с минимальными ошибками классификации.

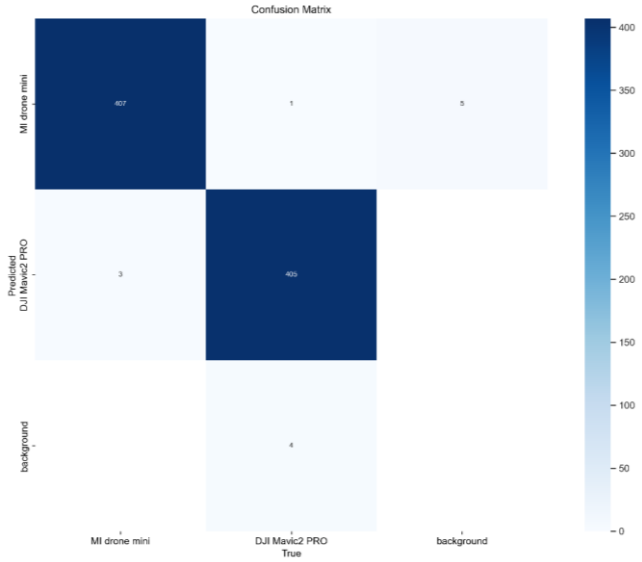


Рис. 5. Матрица ошибок

Для оценки полученного результата обучения использовались следующие метрики [24–26]: F-мера, Precision-Confidence Curve, Precision-Recall Curve, Recall-Confidence Curve, (рис. 6). Кривая достоверности F1 дает представление о компромиссе между порогом достоверности модели и ее оценкой F1. Обученная модель достигает оптимальной оценки F1 0,99 при пороге достоверности 0,619, что указывает на сбалансированную точность и полноту обученной нейронной сети. Кривая Precision-Confidence показывает, как точность меняется в зависимости от уровня достоверности для каждого типа класса. Модель поддерживает высокую точность при большинстве порогов. Кривая Precision-Recall Curve подчеркивает эффективность модели в балансировке точности и полноты по классам, уровень mAP@0.5 составляет 0,995 для всех классов. Кривая Recall-Confidence показывает, как точность меняется в зависимости от уровня достоверности для каждого типа БПЛА. Нейросеть сохраняет высокую точность при большинстве порогов, достигая 1,0 при пороге 0,996.

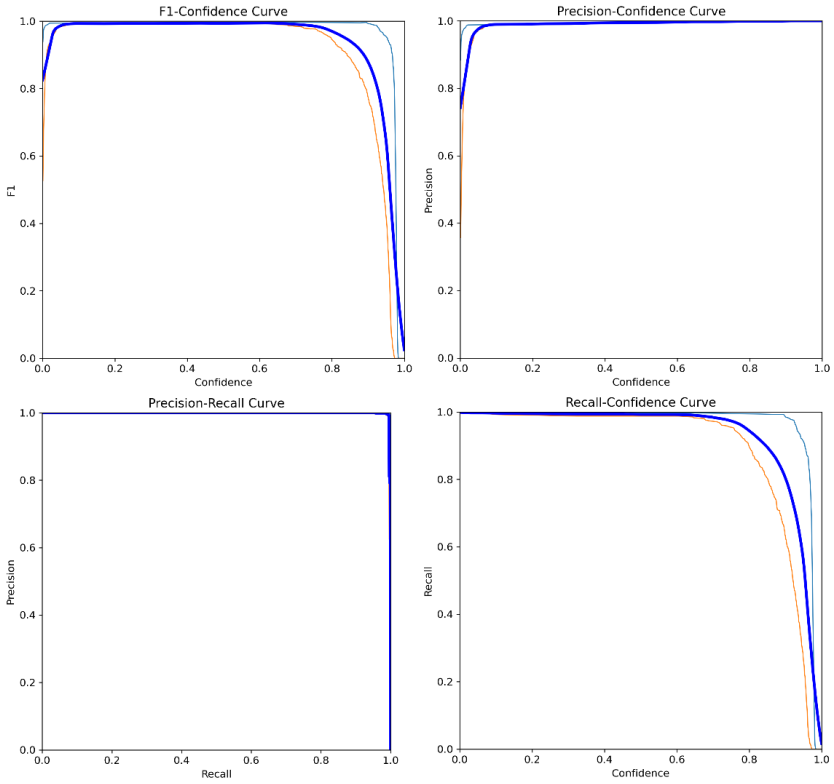


Рис. 6. Метрики оценки обученной модели

На рис. 7 показаны кривые обучения нейросети, кривая metrics/precision (B) показывает точность обнаружения объектов в процессе обучения, а кривая metrics/recall показывает, насколько полно нейросеть может найти объекты на изображении. Достигнута точность классификации 0,99 для двух классов изображений.

Тестирование на экспериментальных данных. Нейросеть протестирована с применением тестовых данных, полученных на полигоне в июле 2021 года с применением радиолокатора TI IWR1642 с параметрами сигнала, показанными в табл. 2 и БПЛА Xiaomi Mi Drone Mini и DJI Mavic2 PRO. В результате из 56 радиолокационных изображений было правильно классифицированы все изображения. На рис. 8,а показан пример правильной классификации РЛИ с БПЛА DJI Mavic2 PRO, а на рис. 8,б показан пример правильной классификации РЛИ с БПЛА Xiaomi Mi Drone Mini.

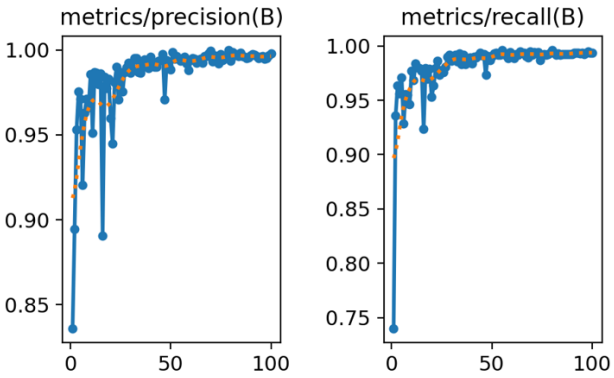
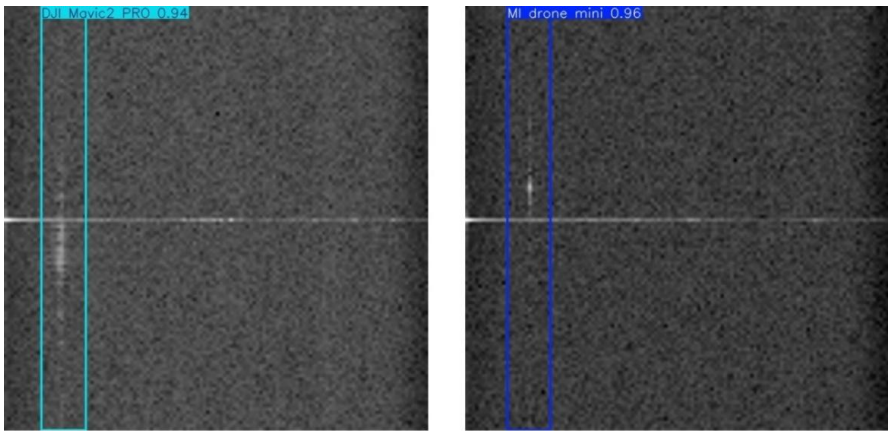


Рис. 7. Метрики точности во время обучения



а б

Рис. 8. Классификация экспериментальных РЛИ

Выводы. Предложенный нейросетевой классификатор БПЛА, основанный на применении архитектуры YOLO11, позволяет осуществить классификацию радиолокационных изображений, содержащих отклики от целевых БПЛА. Применение авторской модели рассеяния радиолокационных сигналов в качестве генератора обучающих данных позволило сформировать достаточно качественные изображения для обучения нейронной сети. Архитектура YOLO в основе классификатора позволяет получить стабильные результаты в классификации БПЛА. Точность на тестовых (сгенерированных) изображениях составила 0,99, а на малой выборке (из 56 изображений), полученных в результате натурного эксперимента, точность составила 1,0.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Coluccia A., Parisi G., Fascista A.* Detection and classification of multirotor drones in radar sensor networks: A review // Sensors. – 2020. – Vol. 20, No. 15. – P. 4172.
2. *Ezuma M. et al.* Micro-UAV detection and classification from RF fingerprints using machine learning techniques // 2019 IEEE Aerospace Conference. – IEEE, 2019. – P. 1-13.
3. *Гонсалез Р., Вудс Р.* Цифровая обработка изображений: пер. с англ. – М.: Издательский дом Техносфера, 2005. – 1073 с.
4. *Anderson T.W., Goodman L.A.* Statistical inference about Markov chains // The Annals of Mathematical Statistics. – 1957. – P. 89-110.
5. *Mendis G.J. et al.* Deep learning based doppler radar for micro UAS detection and classification // MILCOM 2016-2016 IEEE Military Communications Conference. – IEEE, 2016. – P. 924-929.
6. *Hinton G.E., Osindero S., Teh Y.W.* A fast learning algorithm for deep belief nets // Neural computation. – 2006. – Vol. 18, No. 7. – P. 1527-1554.

7. *Martinez J. et al.* Convolutional neural network assisted detection and localization of UAVs with a narrowband multi-site radar // 2018 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM). – IEEE, 2018. – P. 1-4.
8. *Samaras S. et al.* UAV classification with deep learning using surveillance radar data // International Conference on Computer Vision Systems. – Springer, Cham, 2019. – P. 744-753.
9. *Lee H. et al.* CNN-based UAV detection and classification using sensor fusion // IEEE Access. – 2023. – Vol. 11. – P. 68791-68808.
10. *Roldan I. et al.* DopplerNet: A convolutional neural network for recognising targets in real scenarios using a persistent range–Doppler radar // IET Radar, Sonar & Navigation. – 2020. – Vol. 14, No. 4. – P. 593-600.
11. *Деркачев В.А.* Программа для формирования набора радиолокационных изображений летательных аппаратов // Свидетельство о государственной регистрации программы для ЭВМ. №2021665908. 2021.
12. *Деркачев В.А.* Модель рассеяния радиолокационных сигналов от беспилотных летательных аппаратов // Известия ЮФУ. Технические науки. – 2021. – № 2 (219). – С. 120-129.
13. *Viswanatha V., Chandana R.K., Ramachandra A.C.* Iot based smart mirror using raspberry pi 4 and yolo algorithm: A novel framework for interactive display // Indian Journal of Science and Technology. – 2022. – Vol. 15, No. 39. – P. 2011-2020.
14. *Shin D.J., Kim J.J.* A deep learning framework performance evaluation to use YOLO in Nvidia Jetson platform // Applied Sciences. – 2022. – Vol. 12, No. 8. – P. 3734.
15. *Zhao X. et al.* A review of convolutional neural networks in computer vision // Artificial Intelligence Review. – 2024. – Vol. 57, No. 4. – P. 99.
16. *Redmon J.* You only look once: Unified, real-time object detection // Proceedings of the IEEE conference on computer vision and pattern recognition. – 2016.
17. *Alif M.A.R., Hussain M.* YOLOv1 to YOLOv10: A comprehensive review of YOLO variants and their application in the agricultural domain // arXiv preprint arXiv:2406.10139. – 2024.
18. *Joseph Redmon and Ali Farhadi.* Yolo9000: Better, faster, stronger. arxiv. arXiv preprint arXiv:1612.08242, 394, 2016.
19. *Wang C.Y., Bochkovskiy A., Liao H.Y.M.* YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors // Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. – 2023. – P. 7464-7475.
20. *Glenn Jocher, Ayush Chaurasia, and Jing Qiu*. Ultralytics yolov8, 2023.
21. *Glenn Jocher and Jing Qiu*. Ultralytics yolo11, 2024.
22. *Ghosh A.* YOLO11: Faster Than You Can Imagine! // LearnOpenCV. – https://learnopencv.com/yolo11. – 2024.
23. *Деркачев В.А., Бахчевников В.В, Бакуменко А.Н.* Классификатор БПЛА мультироторного типа // Известия ЮФУ. Технические науки. – 2023. – № 2 (232). – С. 90-99.
24. *Sanchez S.A., Romero H.J., Morales A.D.* A review: comparison of performance metrics of pretrained models for object detection using the TensorFlow framework // IOP Conf. Series: Materials Science and Engineering. – 2020. – 15 p. – DOI: 10.1088/1757-899X/844/1/012024.
25. *Sokolova M., Lapalme G.* A systematic analysis of performance measures for classification tasks // Information processing & management. – 2009. – Vol. 45, No. 4. – P. 427-437.
26. *Miao J., Zhu W.* Precision–recall curve (PRC) classification trees // Evolutionary intelligence. – 2022. – Vol. 15, No. 3. – P. 1545-1569.

REFERENCES

1. *Coluccia A., Parisi G., Fascista A.* Detection and classification of multirotor drones in radar sensor networks: A review, *Sensors,* 2020, Vol. 20, No. 15, pp. 4172.
2. *Ezuma M. et al.* Micro-UAV detection and classification from RF fingerprints using machine learning techniques, *2019 IEEE Aerospace Conference*. IEEE, 2019, pp. 1-13.
3. *Gonsalez R., Vuds R.* Tsifrovaya obrabotka izobrazheniy [Digital image processing]: transl. from English. Moscow: Izdatel'skiy dom Tekhnosfera, 2005, 1073 p.
4. *Anderson T.W., Goodman L.A.* Statistical inference about Markov chains, *The Annals of Mathematical Statistics,* 1957, pp. 89-110.
5. *Mendis G.J. et al.* Deep learning based doppler radar for micro UAS detection and classification, *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 924-929.
6. *Hinton G.E., Osindero S., Teh Y.W.* A fast learning algorithm for deep belief nets, *Neural computation,* 2006, Vol. 18, No. 7, pp. 1527-1554.
7. *Martinez J. et al.* Convolutional neural network assisted detection and localization of UAVs with a narrowband multi-site radar, *2018 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM)*. IEEE, 2018, pp. 1-4.

8. *Samaras S. et al.* UAV classification with deep learning using surveillance radar data, *International Conference on Computer Vision Systems*. Springer, Cham, 2019, pp. 744-753.
9. *Lee H. et al.* CNN-based UAV detection and classification using sensor fusion, *IEEE Access,* 2023, Vol. 11, pp. 68791-68808.
10. *Roldan I. et al.* DopplerNet: A convolutional neural network for recognising targets in real scenarios using a persistent range–Doppler radar, *IET Radar, Sonar & Navigation,* 2020, Vol. 14, No. 4, pp. 593-600.
11. *Derkachev V.A.* Programma dlya formirovaniya nabora radiolokatsionnykh izobrazheniy letatel'nykh apparatov [Program for generating a set of radar images of aircraft], *Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM. №2021665908. 2021* [Certificate of state registration of a computer program. No. 2021665908. 2021].
12. *Derkachev V.A.* Model' rasseyaniya radiolokatsionnykh signalov ot bespilotnykh letatel'nykh apparatov [Model of scattering of radar signals from unmanned aerial vehicles], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2021, No. 2 (219), pp. 120-129.
13. *Viswanatha V., Chandana R.K., Ramachandra A.C.* Iot based smart mirror using raspberry pi 4 and yolo algorithm: A novel framework for interactive display, *Indian Journal of Science and Technology,* 2022, Vol. 15, No. 39, pp. 2011-2020.
14. *Shin D.J., Kim J.J.* A deep learning framework performance evaluation to use YOLO in Nvidia Jetson platform, *Applied Sciences,* 2022, Vol. 12, No. 8, pp. 3734.
15. *Zhao X. et al.* A review of convolutional neural networks in computer vision, *Artificial Intelligence Review,* 2024, Vol. 57, No. 4, pp. 99.
16. *Redmon J.* You only look once: Unified, real-time object detection, *Proceedings of the IEEE conference on computer vision and pattern recognition,* 2016.
17. *Alif M.A.R., Hussain M.* YOLOv1 to YOLOv10: A comprehensive review of YOLO variants and their application in the agricultural domain, *arXiv preprint arXiv:2406.10139,* 2024.
18. *Joseph Redmon and Ali Farhadi.* Yolo9000: Better, faster, stronger. arxiv. arXiv preprint arXiv:1612.08242, 394, 2016.
19. *Wang C.Y., Bochkovskiy A., Liao H.Y.M.* YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors, *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition,* 2023, pp. 7464-7475.
20. *Glenn Jocher, Ayush Chaurasia, and Jing Qiu*. Ultralytics yolov8, 2023.
21. *Glenn Jocher and Jing Qiu*. Ultralytics yolo11, 2024.
22. *Ghosh A.* YOLO11: Faster Than You Can Imagine!, *LearnOpenC*V. Available at: https://learnopencv.com/yolo11, 2024.
23. *Derkachev V.A., Bakhchevnikov V.V, Bakumenko A.N.* Klassifikator BPLA mul'tirotornogo tipa [Classifier of multirotor UAVs], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2023, No. 2 (232), pp. 90-99.
24. *Sanchez S.A., Romero H.J., Morales A.D.* A review: comparison of performance metrics of pretrained models for object detection using the TensorFlow framework, *IOP Conf. Series: Materials Science and Engineering,* 2020, 15 p. DOI: 10.1088/1757-899X/844/1/012024.
25. *Sokolova M., Lapalme G.* A systematic analysis of performance measures for classification tasks, *Information processing & management,* 2009, Vol. 45, No. 4, pp. 427-437.
26. *Miao J., Zhu W.* Precision–recall curve (PRC) classification trees, *Evolutionary intelligence,* 2022, Vol. 15, No. 3, pp. 1545-1569.

Деркачев Владимир Александрович – Южный федеральный университет; e-mail: vderkachev@sfedu.ru; г. Таганрог, Россия; тел.: +79614154733; кафедра радиотехнических и телекоммуникационных систем; старший преподаватель.

Derkachev Vladimir Aleksandrovich – Southern Federal University; e-mail: vderkachev@sfedu.ru; Taganrog, Russia; phone +79614154733; the Department of Radio engineering & Telecommunication Systems; senior lecturer.

УДК 004.896:004.048 DOI 10.18522/2311-3103-2025-3-181-197

А.С. Игнатьева, В.В. Шадрина, В.В. Игнатьев, А.В. Максимов

МЕТОД АВТОМАТИЧЕСКОЙ ОПТИМИЗАЦИИ БАЗЫ НЕЧЕТКИХ ПРАВИЛ ИНТЕЛЛЕКТУАЛЬНЫХ РЕГУЛЯТОРОВ НА ОСНОВЕ СУБТРАКТИВНОЙ КЛАСТЕРИЗАЦИИ

Целью работы является разработка метода оптимизации базы нечетких правил интеллектуального регулятора для управления техническим объектом с использованием субтрактивной кластеризации. В статье приведен обзор и краткий анализ состояния дел в области оптимизации работы интеллектуальных систем управления. Для достижения цели исследования разработана гибридная модель, в которой управление техническим объектом реализуется с помощью классического ПИ-регулятора и нечеткого ПИ-регулятора с сгенерированной структурой системы нечеткого вывода типа Сугено и разработанной моделью адаптивной системы нейро-нечеткого вывода. Данная конфигурация модели позволяет формировать базу нечетких правил, которая не зависит от знаний эксперта в предметной области. В статье предложен новый метод оптимизации базы правил нечеткого регулятора на основе методов кластеризации, в частности субтрактивной кластеризации, позволяющий уменьшать количество правил нечеткого логического вывода и увеличить быстродействие системы управления техническим объектом. Сначала проведено моделирование гибридной модели, синтезированной на основе значений нечеткого и классического регуляторов до применения субтрактивной кластеризации. Применение субтрактивной кластеризации по разработанному в исследовании способу для значений классического регулятора и нечеткого, позволило добиться их количественного сокращения в 1,7 и 5,25 раз соответственно. Затем проведено моделирование гибридной модели, синтезированной на основе значений нечеткого и классического регуляторов после применения субтрактивной кластеризации. Результаты, полученные в процессе моделирования показали высокую эффективность предложенного метода оптимизации базы правил нечеткого регулятора. За счет применения субтрактивной кластеризации в гибридной модели для интеллектуального регулятора удалось значительно уменьшить количество функций принадлежности, требуемых для описания входных лингвистических переменных (с пяти до четырех) и уменьшить количество правил нечеткого логического вывода (с двадцати пяти до шестнадцати). Анализ полученных графиков переходных процессов, полученных для гибридных моделей до и после применения субтрактивной кластеризации, показал, что основные показатели качества процесса управления остаются неизменными при существенном сокращении проводимых вычислений.

Система управления; субтрактивная кластеризация; нечеткие правила; оптимизация; система нечеткого вывода; гибридная сеть; обучение.

A.S. Ignatyeva, V.V. Shadrina, V.V. Ignatyev, A.V. Maksimov

METHOD OF AUTOMATIC OPTIMIZATION OF THE FUZZY RULE BASE OF AN INTELLIGENT CONTROLLER BASED ON SUBTRACTIVE CLUSTERING

The aim of the work is to develop a method for optimizing the fuzzy rule base of an intelligent controller for controlling a technical object using subtractive clustering. The article provides an overview and a brief analysis of the state of affairs in the field of optimizing the operation of intelligent control systems. To achieve the goal of the study, a hybrid model has been developed in which the technical object is controlled using a classical PI controller and a fuzzy PI controller with a generated structure of a Cygeno-type fuzzy inference system and a developed model of an adaptive neuro-fuzzy inference system. This configuration of the model allows you to form a fuzzy rule base that does not depend on the expert's knowledge in the subject area. The article proposes a new method for optimizing the fuzzy controller rule base based on clustering methods, in particular subtractive clustering, which allows you to reduce the number of fuzzy logical inference rules and increase the performance of the technical object control system. First, a hybrid model synthesized on the basis of the values of the fuzzy and classical controllers before applying subtractive clustering was simulated. The application of subtractive clustering according to the method developed in the study for the values of the classical and fuzzy controllers allowed us to achieve their quantitative reduction by 1.7 and 5.25 times, respectively. Then, the hybrid model synthesized on the basis of the values of the fuzzy and classical controllers after applying subtractive clustering was simulated. The results obtained in the process of simulation showed high efficiency of the proposed

method for optimizing the fuzzy controller rule base. Due to the application of subtractive clustering in the hybrid model for the intelligent controller, it was possible to significantly reduce the number of membership functions required to describe the input linguistic variables (from five to four) and reduce the number of fuzzy logical inference rules (from twenty-five to sixteen). The analysis of the resulting graphs of transient processes obtained for the hybrid models before and after applying subtractive clustering showed that the main indicators of the quality of the control process remain unchanged with a significant reduction in the calculations performed.

Control system; subtractive clustering; fuzzy rules; optimization; fuzzy inference system; hybrid network; training.

Введение. Автоматизированные системы управления технологическими процессами и производствами сегодня проходят очередную ступень развития. В первую очередь это связано с непрерывным взаимодействием с другими областями науки и техники. Системы управления находятся под влиянием «глубокой» цифровизации, разрабатываются с учетом необходимости применения интеллектуальных технологий, которые позволяют оперативно и с требуемой точностью решать самые сложные задачи при управлении не только отдельными техническими объектами, но и целыми процессами. Высокая эффективность таких систем подтверждается в различных отраслях промышленности.

Внедрение интеллектуальных технологий в автоматизированные процессы имеет и свои сложности, которые, в первую очередь, заключаются в необходимости «интеллектуализации» практически всего технологического цикла, что не всегда возможно сделать, из-за конструктивных ограничений, большого количества связей между объектами регулирования, отсутствия полной автоматизации технологического процесса и т.д.

Передовым и широко распространенным решением в таких случаях является проектирование автоматизированных систем, сочетающих одновременно традиционные подходы к управлению и подходы на основе интеллектуальных технологий, т.е. гибридные системы, основанные на двух и более методах управления. Такие системы способны обеспечить требуемую эффективность, но разработчику необходимо правильно и оптимально выстраивать взаимодействие управляющих элементов внутри таких систем.

Эта задача является достаточно сложной, особенно когда речь идет об объекте, управление которым требуется обеспечить в условиях неопределенности. Требуется оптимальная настройка параметров применяемых регуляторов. Одной из ключевых трудностей, с которой сталкивается разработчик при проектировании интеллектуальных регуляторов, является формирование базы управляющих правил. База правил должна быть сформирована по принципу необходимости и достаточности для достижения требуемого качества управления. Должны исключаться избыточность правил, противоречивость, повторяемость, правила не должны зависеть от экспертной оценки разработчика.

Этому способствует, главным образом, неполнота исходных данных при синтезе регулятора. Например, избыточное количество термов функций принадлежности, установленное экспертом, в итоге приведет к избыточному количеству управляющих правил, что потребует дополнительное время на их обработку, задействует вычислительные ресурсы и т.д.

В рамках выполнения исследований, результаты которых представлены в настоящей статье, авторами приводится описание разработанного метода автоматической оптимизации базы нечетких правил интеллектуального регулятора для управления техническим объектом с использованием субтрактивной кластеризации.

В общем виде основную идею разработки можно описать следующим образом. Выбрана гибридная модель управления техническим объектом, для которого ранее были рассчитаны параметры ПИ-регулятора и который является источником информации для второго нечеткого регулятора. Управляющие правила для нечеткого регулятора формируются автоматически без участия эксперта. Эффективность работы нечеткого регулятора достигается за счет обучения. Для сокращения исходных данных в ходе синтеза нечеткого регулятора применена субтрактивная кластеризация. Такой подход позволяет значительно сократить время и трудозатраты на проектирование базы управляющих правил нечеткого регулятора (сокращается количество функций принадлежности каждой из входных лингвистических переменных и выходной) без потери качества управления.

Анализ существующих подходов к оптимизации интеллектуальных регуляторов. Рост количества вычислений в современных системах неизбежен и обусловлен, в первую очередь, большим количеством информации, требующей анализа и обработки для принятия эффективных решений при реализации управления. Основным управляющим звеном в системах автоматизации по-прежнему остаются регуляторы. В ходе проектирования регуляторов применяются технологии искусственного интеллекта, которые способны обеспечить требуемую оперативность в ходе принятия решений. Однако и эти регуляторы нуждаются в оптимизации как с целью сокращения времени их синтеза, так и для минимизации времени выдачи эффективных управляющих воздействий на объект. Подходам к оптимизации интеллектуальных регуляторов посвящены разные исследования.

Например, в работе [1] авторы предлагают интервальный нечеткий дробный PD-PI-контроллер второго типа для стабилизации частоты изолированных микросетей, оптимизированный с помощью алгоритма гепарда. Управление частотой в микросетях во время изолированной работы сталкивается со значительными проблемами из-за колебаний нагрузки и прерывистого характера возобновляемых источников энергии. Для решения этой проблемы в этом исследовании предлагается интервальный нечеткий дробный PD-PI-контроллер второго типа с возможностью уменьшения отклонений частоты. Кроме того, оптимизация параметров контроллера в динамических системах является еще одной важной проблемой, где традиционные алгоритмы, такие как генетический алгоритм, оптимизация роем частиц и синусно-косинусный алгоритм, часто сталкиваются с преждевременной сходимостью и неоптимальными решениями. Чтобы преодолеть эти ограничения, авторы предлагают используется оптимизатор на основании алгоритма гепардов за его поисковую способность, способность избегать локальных оптимумов и простоту, поскольку он не полагается на сложные математические формулы. Рассматриваются различные сценарии, в которых влияние предлагаемого контроллера на изменения частоты сети сравнивается с двумя другими контроллерами, в основе которых лежит использование нескольких методов оптимизации. Результаты моделирования демонстрируют приблизительно 58,6% и 54,3% улучшение интегральной временной абсолютной ошибки по сравнению с двумя другими контроллерами соответственно в комбинированном сценарии. Алгоритм гепарда также достигает оптимального целевого значения 0,0001092, превосходя другие методы оптимизации.

Интерес представляет работа [2], в которой для минимизации ошибок обнаружения и снижения влияния внешнего шума и помех авторами разработан регулятор для использования в нелинейной системе. В основе работы интервального нечеткого пропорционально-интегрально-дифференциального регулятора дробного порядка второго тип используется алгоритм оптимизации на основе биогеографии (BBO) Предлагаемый метод имеет несколько преимуществ. Во-первых, предлагаемый регулятор оптимизирован для достижения надежности и минимизации ошибок отслеживания. Во-вторых, он эффективно обрабатывает внешний шум и помехи, что делает его пригодным для реального использования. В-третьих, использование алгоритма биогеографии повышает производительность регулятора за счет динамической настройки его параметров на основе системных требований. Производительность предлагаемого регулятора подтверждается путем его применения для управления роботизированным манипулятором, что представляет собой проблему из-за его нелинейных характеристик и динамики взаимодействия нескольких входов и нескольких выходов. Кроме того, проводится оценка предлагаемого регулятора в реальном времени путем его применения для управления скоростью машины постоянного тока. Эффективность предлагаемого регулятора проверена с помощью моделирования, практических экспериментов и сравнений с другими оптимизированными регуляторами. Результаты моделирования и практического применения демонстрируют превосходную производительность регулятора при наличии системных неопределенностей и различных типов возмущений.

В работе [3] энергоэффективный масштабируемый алгоритм маршрутизации на основе иерархической агломеративной кластеризации используется в беспроводных сенсорных сетях. В иерархических беспроводных сенсорных сетях несбалансированное по-

требление энергии, вызванное многоадресной маршрутизацией, предъявляет требования к выбору и распределению кластеров головным устройством кластера. Стремясь улучшить срок службы сети и достичь баланса потребления энергии между сенсорными узлами, авторами предлагается энергоэффективный масштабируемый алгоритм маршрутизации на основе иерархической агломеративной кластеризации для беспроводных сенсорных сетей путем совместной оптимизации формирования кластера и энергоэффективности межкластерной связи. Во-первых, для снижения стоимости передачи и сложности времени/пространства в процессе кластеризации предлагается иерархический метод кластеризации для достижения оптимального распределения всех сенсоров (датчиков) в кластеры. Во-вторых, принимая во внимание несколько параметров, таких как диапазон покрытия, связь и оставшаяся энергия сенсорных узлов, определяется функция оценочного коэффициента для выбора головной части кластера, чтобы снизить дополнительные потери на связь между узлами-членами и головными частями кластера. Кроме того, для решения проблемы горячих точек, вызванной межкластерной пересылкой данных, вводится генетический алгоритм для получения оптимальной межкластерной маршрутизации для баланса энергопотребления сети. Экспериментальные результаты показывают, что представленный авторами алгоритм дает оптимальное взаимодействие всех датчиков, входящих в систему, а также позволяет передавать данных без дополнительных потерь энергии и продлевает срок службы сети.

Методы и алгоритмы кластеризации также используются в селекции. Для механического и химического прореживания цветов, когда обычно сохраняется только один или два самых сильных цветка в каждом кластере, авторы в своей работе [4] предлагают использовать алгоритм кластеризации DPC для обнаружения и определения местоположения цветков яблони. С помощью данного алгоритма автоматически определяется количество цветочных кластеров и точно определяется центральный цветок в этих кластерах. Обнаружение и позиционирование цветков яблони имеют решающее значение предлагается улучшенный метод, который использует модель YOLOv8n для точного обнаружения цветов. Алгоритм DPC улучшен для автоматического определения количества цветочных кластеров и точного определения центральных цветов в этих кластерах. Чтобы оценить производительность предложенного алгоритма, результаты кластеризации сравнили с результатами, полученными в результате других алгоритмов кластеризации, таких как, алгоритм ближайших соседей, о k-средних, о k –медоидах, модель гауссовской смеси, пространственную кластеризацию приложений на основе плотности с шумом, спектральную кластеризацию. Результаты показали, что предложенный метод превзошел самые высокие результаты, полученные другими методами. Кроме того, предложенный алгоритм уменьшил отклонение между центром и истинным центральным цветком. В целом алгоритм эффективно уменьшает отклонения центра кластеризации, демонстрируя свою способность точно обнаруживать и определять местоположение цветков яблони.

Алгоритм кластеризации нечетких c-средних (FCM) сильно зависит от выбора начальных значений центров кластеров, из чего следует низкая точность кластеризации. Чтобы минимизировать эту зависимость, авторами в своей работе [5] предложен улучшенный алгоритм о нечетких c-средних с использованием нечеткого роя частиц – для решения проблем кластеризации данных. В этом алгоритме ключевые усовершенствования включали инициализацию центров кластеризации с использованием расстояний Махаланобиса для снижения зависимости от начальных значений центров кластеров. Для решения проблемы преждевременной сходимости была предложена целевая функция, основанная как на межкластерных, так и на внутрикластерных оценках. Был разработан модифицированный алгоритм роя частиц для нахождения центров кластеризации. Предложенный алгоритм был применен для анализа наборов данных, а также для кластеризации и сегментации классических тестовых изображений. Результаты показали, что алгоритм улучшил стабильность результатов анализа, сохранив высокую точность кластеризации и скорость сходимости, достигнув превосходной производительности по сравнению с существующими методами. Более того, он продемонстрировал превосходную производительность при анализе нечетких многотеневых серых изображений.

Так как кластеризация зачастую применяется к неструктурированным и зашумленным данным, разработка алгоритма полуконтролируемой кластеризации, который будет устойчив к шуму, становится все более важной. С этой целью в данной статье [6] авторами предлагается структура обучения полуконтролируемой кластеризации с устойчивостью к шуму, учитывающая взвешенный коэффициент пересечения и парные сходства. Основанная на алгоритме иерархического обучения, в основе которого лежит использование взвешенного коэффициента пересечения, авторами предлагается алгоритм полуконтролируемой ансамблевой кластеризации, которая является высокоэффективной с точки зрения вычислений. Здесь взвешенный коэффициент пересечения применяется для принятия решений об объединении различных образцов в один кластер, что в свою очередь позволяет разрабатывать всеобъемлющую и надежную модель кластеризации. Предлагаемая структура оценивает значимость каждого образца данных в окончательном объединении с помощью оценки его влияния на кластер, тем самым эффективно минимизируя влияние шума. Между тем, парные сходства используются для отбора образцов, в котором обучающие образцы делятся на чистые и зашумленные наборы. Результаты показывают, что предлагаемая структура достигает превосходной точности кластеризации и надежности по сравнению с существующими методами, особенно в шумных средах. В частности, разработанный алгоритм показывает результат на 3,9% лучший при оценке средней точности по сравнению с существующими аналогичными алгоритмами.

В настоящее время наблюдается тенденция к непрекращающемуся росту и усложнению объема данных, хранящихся у пользователей. Методы кластеризации в машинном обучении становятся все более важными для извлечения ценности из больших данных. Однако одному пользователю сложно в полной мере использовать крупномасштабные данные для локальной кластеризации из-за ограниченных локальных вычислительных ресурсов и отсутствия необходимого объема данных. Для решения этой проблемы модель многопользовательской совместной кластеризации появилась как способ решения для многопользовательской совместной кластеризации путем размещения данных на облачной платформе. Тем не менее, аутсорсинговая кластеризация может привести к ряду проблем с конфиденциальностью. Для эффективного решения авторами [7] предлагается новая, безопасная и эффективная схему аутсорсинговой кластеризации k-средних. Эта схема использует частично гомоморфные методы шифрования для облачной кластеризации k-средних, что гарантирует, что облако не содержит никакой личной информации, одновременно защищая конфиденциальность базы данных, данных, участвующих в процессе кластеризации, результатов кластеризации и пользовательской информации. Кроме того, авторами проведен сравнительный анализ предложенной схемы, результаты которого демонстрируют безопасность и практичность использования разработанного метода.

В настоящее время лишь немногие исследования рассматривали кластерный анализ многомерных данных, собранных многими датчиками в потоковой среде в реальном времени. Существующие алгоритмы кластерного анализа для многомерных данных в первую очередь основаны на моделях пакетной обработки, и большинство из них не могут удовлетворить требованиям инкрементальных многомерных потоков данных, которые чрезвычайно распространены в практических приложениях. Для решения вышеупомянутых проблем авторы в своей статье [8] основное внимание уделяются изучению многомерной кластеризации данных на основе потоковой обработки и предлагается алгоритм кластеризации многомерного потока данных на основе системы управления с обратной связью, которая включает три этапа: анализ главных компонент окна, кластеризация потока обратной связи и контроллер обратной связи. Классическая экспоненциально взвешенная функция затухания используется в анализе главных компонент окна, а извлечение признаков выполняется через скользящее окно для повышения итеративной эффективности данных в окне. Чтобы минимизировать ошибки, вызванные изменчивостью углов проекции во время снижения размерности, разработан этап кластеризации потока обратной связи с чередующимися итерациями кластеризации окна и агрегации кластера. Нацелившись на проблемы, вызванные ручной настройкой гиперпараметров, используемых в кластеризации потоков данных высокой размерности, разработан кон-

троллер обратной связи для настройки гиперпараметров на двух других этапах путем анализа результатов кластеризации в реальном времени и использования дискриминантной оценки для принятия соответствующих стратегий обратной связи. Экспериментальные сравнения между предлагаемым методом и существующими алгоритмами на нескольких наборах данных демонстрируют эффективность первого.

Новая методология прогнозирования под названием SSOFC-Apriori-WRP, которая представляет прогнозирование энергии ветра и скорости на один день вперед, представлена в работе [9]. Задача вероятностного прогноза энергии ветра решается с помощью комбинированной интеллектуальной структуры и алгоритма нечеткой кластеризации. Проведены исследования характеристик эксплуатационного поведения ветроэнергетической системы с использованием метода нечеткой кластеризации для мониторинга состояния системы и для исключения ее неисправностей [10].

Исследование [11] посвящено разработке нового метода проектирования систем на основе входных данных для автоматического определения типов нечетких множеств (нечеткие множества типа 1 (T1-FS) или нечеткие множества интервального типа 2 (IT2-FS)) на основе нечеткости. В нечеткой системе гибридного типа (HTFS) тип нечеткого множества определяется нечеткостью для повышения производительности системы, а интерпретируемость данной системы определяется целостностью, различимостью и избыточностью нечетких множеств. Во-первых, нечеткая кластеризация используется для инициализации базы правил и типов нечетких множеств. Во-вторых, метод роя частиц используется для оптимизации параметров HTFS, а типы нечетких множеств определяются нечеткостью, что означает, что типы нечетких множеств будут динамически меняться в процессе оптимизации. Таким образом, в статье предлагается метод проектирования нечетких систем управления данными, которые могут автоматически определять типы нечетких множеств за счет введения нечеткости.

Многоуровневая нечеткая модель, основанная на кластеризации нечетких правил для задач прогнозирования, предложена в [12]. Такой подход может быть полезен к применению в системах мониторинга эксплуатации и прогноза технического состояния оборудования. В работе [13] для диагностики и предсказания сбоев ветряной турбины применяется нечеткая кластеризация.

В работе [14] для повышения точности стандартного алгоритма FCM применен лесной алгоритм оптимизации (FOA). Нечеткая кластеризация в данном случае представляет собой комбинацию лесного алгоритма оптимизации с градиентным методом, что позволяет получить оптимизированные кластерные центры. Задача декомпозиции больших электросетей на малые и слабосвязанные с целью упрощения процесса управления системами передачи электроэнергии рассматривается в [15]. В экспертной системе управления на основе правил применена нечеткая кластеризация для проектирования локальных управляющих действий во время перегрузки, недогрузки и разделении.

Адаптивный метод нейро-нечеткого вывода с использованием алгоритма субтрактивной кластеризации используется в медицине [16]. Так в статье на основе адаптивного метода нейро-нечеткого вывода решается проблема обнаружения аномальных разрядов – режим разряда в энцефалограмме (ЭЭГ) с четкими контурами. Авторами предлагается подход, основанный на, во-первых, использовании плотности вероятности для извлечения логнормальных амплитудных признаков из огибающих ЭЭГ, во-вторых, метод субтрактивной кластеризации модифицируется таким образом, чтобы радиусы кластеризации могли адаптироваться к формам кластеров для каждого измерения вместо использования идентичных радиусов для каждого кластера. Результаты сравнительных экспериментов показали, что предложенный метод показал конкурентоспособные результаты по точности и полноте обнаружения аномального разряда с более низкими вычислительными затратами по сравнению с лучшими результатами, получаемыми в этой области ранее.

Авторы в своей работе [17] используют алгоритмы машинного обучения для прогнозирования теплофизических свойств наножидкостей, таких как плотность, вязкость, теплопроводность и удельная теплоемкость, для сокращения затрат и увеличения скорости обработки информации. Исследование было направлено на точное прогнозирование

теплофизических свойств гибридных наножидкостей оксид-MWCNT на водной основе путем принятия целой стратегии поиска для оптимизации моделей ANFIS с различными типами методов кластеризации, включая разбиение сетки, субтрактивную кластеризацию и нечеткую кластеризацию с-средних. Для оценки оптимизированных моделей ANFIS использовались различные статистические критерии. Результаты показали, что оптимальная модель, в основе которой было использование субтрактивной кластеризации, показала лучшие результаты, чем другие подходы ANFIS при моделировании удельной теплоемкости наножидкости.

В работе [18] система адаптивного нейро-нечеткого вывода (ANFIS) применяется для оценки качества воды, в частности, для прогнозирования уровня содержания тяжелых металлов в подземных водах, как городских, так и сельских. Для сравнения авторы используют в своей работе два типа моделей, в основе первой использовался алгоритм кластеризации о с-средних, во второй – субтрактивная кластеризация. Результаты показали, что данные, полученные с ANFIS, в сравнении с фактическими данными показали, что ANFIS обладают большим потенциалом для оценки содержания тяжелых металлов в грунтовых водах с высокой степенью точности. В свою очередь, данные, полученные с ANFIS, основанной на алгоритме кластеризации о с-средних, обеспечивают немного более высокую точность, чем данные, полученные с ANFIS, основанной на субтрактивной кластеризации.

В исследовании [19] авторами разработан каскадный нечеткий ПИД-регулятор, оптимизированный с помощью применения алгоритма серых волков, с треугольными функциями принадлежности для управления частотой нагрузки во взаимосвязанных энергосистемах. Эффективность регулятора продемонстрирована на тепловых и гибридных тепловых, гидрогазовых энергосистемах. Параметры регулятора были настроены с использованием целевой функции интегральной временной абсолютной погрешности, которая также оценивалась вместе с другими целевыми функциями для обеспечения высокой точности стабилизации частоты. Для проверки эффективности треугольной функции принадлежности были проведены сравнения с нечеткими ПИД-регуляторами, использующими трапециевидные и гауссовские функции принадлежности. Сравнения проводились с регуляторами, оптимизированными с использованием алгоритмов медоеда, модифицированного алгоритма кузнечиков, алгоритма роя частиц и алгоритма паукообразных обезьян. Результаты показывают, что нечеткий ПИД-регулятор на основе оптимизации с помощью алгоритма серых волков превосходит альтернативы, демонстрируя превосходную производительность по всем оцениваемым показателям.

Проведенный анализ выполняемых исследований доказывает интерес со стороны научного сообщества к кластеризации как одному из методов оптимизации, применяемых в различных системах. Одновременно можно сказать, что использование нечеткой кластеризации носит точечный характер ввиду отсутствия понятных и распространенных механизмов ее реализации.

Это подтверждает актуальность проведенных исследований в настоящей статье, результаты которых являются развитием существующих методов оптимизации интеллектуальных регуляторов для обеспечения эффективного управления техническим объектом.

Разработка метода автоматической оптимизации базы нечетких правил интеллектуальных регуляторов технических объектов с использованием субтрактивной кластеризации. Научная новизна данной работы заключается в разработке нового метода автоматической оптимизации базы правил интеллектуального регулятора на основе субтрактивного кластерного анализа для систем управления техническими объектами, что позволит повысить быстродействие модели управления, оптимизировать базу правил регулятора (сократить количество исходной информации для его синтеза, количество функций принадлежности и количество правил), сократить время разработки нечеткого регулятора [20].

Для доказательства эффективности разработанного метода выбрана гибридная модель управления техническим объектом. Синтез модели выполнен на основе совместной работы ПИ-регулятора и нечеткого регулятора. В основу взаимодействия двух регуляторов положена идея синтеза нечеткого регулятора на основе значений сигналов отклонения, интеграла отклонения и управляющего воздействия, полученных с ПИ-регулятора.

Рассмотрим пошагово процесс синтеза интеллектуально регулятора.

1. Выполняется запуск модели, в которой для управления техническим объектом используется ПИ-регулятор.

2. Выполняется запись значений сигналов отклонения, интеграла отклонения и управляющего воздействия, полученных с ПИ-регулятора вне зависимости от качества полученного управления.

3. Полученные значения формируются в виде матриц.

4. По специально разработанному алгоритму на основе данных значений формируются автоматически термы лингвистических переменных для синтеза нечеткого регулятора. Значения сигналов отклонения ПИ-регулятора используются для формирования термов первой входной лингвистической переменной, значения сигналов интеграла отклонения и управляющего воздействия – для второй лингвистической переменной и управляющего воздействия нечеткого регулятора, соответственно.

5. Выполняется запуск модели, в которой для управления техническим объектом используется нечеткий регулятор.

6. Выполняется запись значений сигналов отклонения, интеграла отклонения и управляющего воздействия, полученных с нечеткого регулятора (управление, как правило, получается требуемого качества за счет разработанного алгоритма в п. 4).

7. Разрабатывается адаптивная система нейро-нечеткого вывода для обучения нечеткого регулятора (для обучения используются значения сигналов отклонения, интеграла отклонения и управляющего воздействия, полученные с нечеткого регулятора, для проверки такие же сигналы, полученные с ПИ-регулятора).

8. Проверяется качество управления.

9. Для значений сигналов отклонения, интеграла отклонения и управляющего воздействия, полученных с нечеткого регулятора применяется субтрактивная кластеризация по специально разработанной методике.

10. Для значений сигналов отклонения, интеграла отклонения и управляющего воздействия, полученных с ПИ-регулятора также применяется субтрактивная кластеризация.

11. Разрабатывается адаптивная система нейро-нечеткого вывода для обучения нечеткого регулятора (для обучения используются кластеризованные значения сигналов отклонения, интеграла отклонения и управляющего воздействия, полученные с нечеткого регулятора после выполнения п. 9, для проверки такие же сигналы, полученные с ПИ-регулятора после выполнения п. 10).

12. Проверяется качество управления.

13. Метод считается успешно реализованным, если результаты п. 12 совпадают с результатами п. 8 (или отличаются в лучшую сторону).

Основной отличительной особенностью разработанного метода является то, что после выполнения субтрактивного кластерного анализа количество термов входных и выходной лингвистической переменных нечеткого регулятора значительно уменьшается, также значительно уменьшается количество правил нечетких продукций.

Это позволяет генерировать базу правил нечеткого регулятора с меньшими трудозатратами, пользуясь только нужными термами. То есть желаемое управление техническим объектом, в том числе в условиях неопределенности, достигается при значительно меньшем количестве вычислений.

Реализация разработанного метода. Для реализации предложенного метода и доказательства его эффективности выбрана гибридная модель, разработанная и рассчитанная в более ранних публикациях авторов [21, 22]. Также для этой модели ранее была разработана адаптивная система нейро-нечеткого вывода. Вид модели управления представлен на рис. 1.

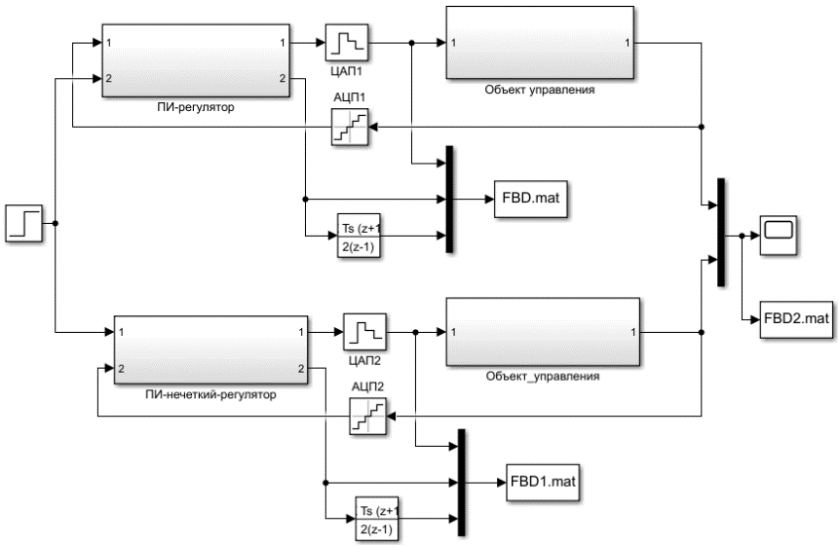


Рис. 1. Гибридная модель управления

После запуска модели получены значения сигналов управления, отклонения и интеграла отклонения в дискретные моменты времени. В результате работы ПИ-регулятора получены значения и объединены в матрицу размером 3×63, частично представленную в табл. 1.

Таблица 1

Значения сигналов управления, отклонения и интеграла отклонения, полученные с ПИ-регулятора, до кластеризации

№ п/п	Управление	Отклонение	Интеграл отклонения
1	1	0	0,221000000000000
2	0,983449900000000	0,0079545191750000	0,226132171588375
3	0,939550600000000	0,0156617773000000	0,224946946516500
4	0,876065950000000	0,0229348509000000	0,218953585194500
5	0,799561675000000	0,0296440149875000	0,209459766736188
6	0,715485250000000	0,0357075973750000	0,197579135349375
. . .	. . .	. . .	. . .
62	0,000396325000000086	0,0587470134125002	0,0650030376458125
63	0,000316450000000135	0,0587498884750002	0,0649885622148750

В результате работы нечеткого регулятора получены значения и объединены в матрицу размером 3×126, частично представленную в табл. 2.

Таблица 2

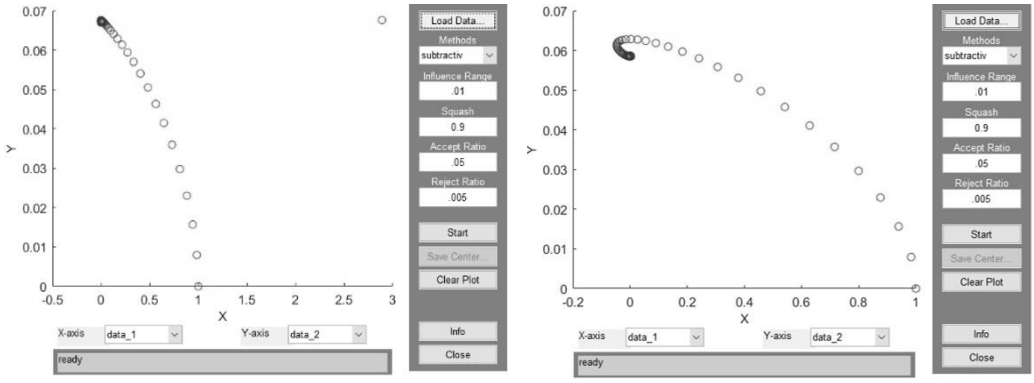
Значения сигналов управления, отклонения и интеграла отклонения, полученные с нечеткого регулятора, до кластеризации

№ п/п	Управление	Отклонение	Интеграл отклонения
1	1	0	0,141650000000000
2	0,985239100000000	0,0079608452750000	0,217140643063296
3	0,943927750000000	0,0156924013750000	0,218195494066133
4	0,883590175000000	0,0230124175125000	0,206025352327971

Окончание табл. 2

№ п/п	Управление	Отклонение	Интеграл отклонения
5	0,811031725000000	0,0297973270625000	0,203076247396287
6	0,730757350000000	0,0359682774250000	0,192916997768288
. . .	. . .	. . .	. . .
125	–0,000306574999999976	0,0669835760375009	0,0649854973871797
126	–0,000290599999999808	0,0669812113000008	0,0649856498426884

В графическом виде полученные значения сигналов с ПИ-регулятора и нечеткого регулятора, представлены на рис. 2.



а б

Рис. 2. Данные для кластеризации: а – обучающие данные; б – проверочные данные

В соответствии с пунктами разработанного метода на следующем этапе применяется субтрактивная кластеризация для всех значений сигналов отклонения, интеграла отклонения и управляющего воздействия, полученных как с ПИ-регулятора, так и с нечеткого регулятора. Основная цель этого решения – уменьшить количество значений в матрицах. После выполнения субтрактивной кластеризации получаем значения, представленные в табл. 3 и 4.

Таблица 3

Значения сигналов управления, отклонения и интеграла отклонения, полученные с ПИ-регулятора, после кластеризации

№ п/п	Управление	Отклонение	Интеграл отклонения
1	1,850049999999992	5,8674219275000203	6,5243873348874895
2	7,1582500000000326	5,8448425887500197	6,47437079306874
3	–3,3577999999900021	5,8474738025000202	6,3872511717624897
4	–7,7030000000000015	5,8561275475000202	6,3007846399874903
5	–1,3517899999990000	5,8729173600000101	6,47437079306874
6	–2,0706649999990001	5,9001340550000198	6,3872511717624897
. . .	. . .	. . .	. . .
36	5,4743275000000001	6,24275936625001	8,1080754772062502
37	2,5748650000000005	6,2745415850000097	7,5024136164249994

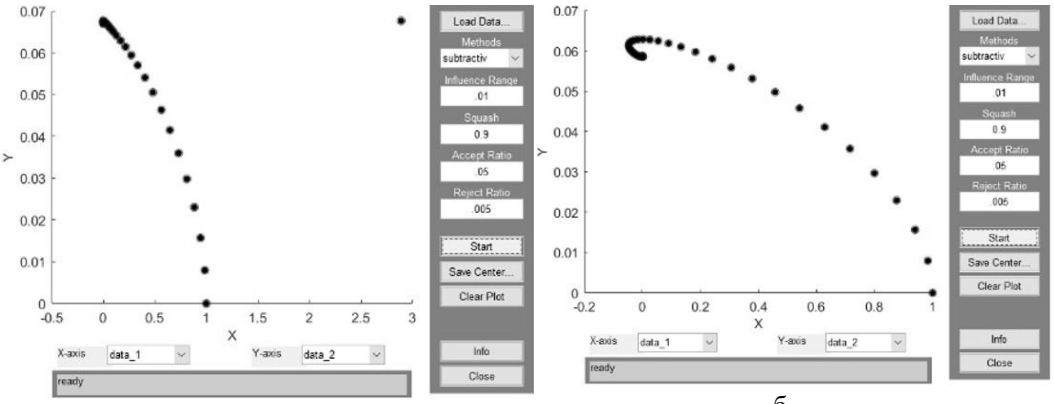
Таблица 4

Значения сигналов управления, отклонения и интеграла отклонения, полученные с нечеткого регулятора, после кластеризации

№ п/п	Управление	Отклонение	Интеграл отклонения
1	–6,5802499998999999	6,7152605862500200	6,4981688475955507
2	–2,0638250000000000	6,7552924037500003	6,4968773702567997
3	–2,9059999998999977	6,6981211300000801	6,4985649842688398
4	1,2489399999999999	6,7412477525000097	6,5116869704048994
5	3,201085	6,6909210425000101	6,5355397839653995
6	5,6835999999999991	6,6215592775000096	6,5711874474852994
. . .	. . .	. . .	. . .
23	2,1680965000000002	6,1371104325000002	1,01395307646861
24	2,8900000000109398	6,76330097750001	6,4988700554897

Полученная матрица после кластеризации для ПИ-регулятора имеет размером 3×37, для нечеткого регулятора 3×24. То есть в первом случае матрица уменьшилась в 1,7 раза, во втором в 5,25 раза.

В графическом виде полученные значения сигналов с ПИ-регулятора и нечеткого регулятора после кластеризации, представлены на рис. 3.



а б

Рис. 3. Результаты кластеризации с помощью субтрактивного алгоритма: а – обучающие данные; б – проверочные данные

Результаты сформированных правил сгенерированного нечеткого регулятора до обучения [20–22] представлены на рис. 4.

Из рисунка видно (выделено пунктиром), что база правил состоит из 25 правил – на основе пяти функций принадлежности для первой входной лингвистической переменной и пяти для второй.

Рассмотрим результаты полученные после запуска модели с выполненной нечеткой субтрактивной кластеризацией.

На рис. 5 представлен этап обучения нечеткого регулятора (обучение гибридной сети, метод – гибридный).

Обучение заканчивается на втором шаге после двух циклов, что подтверждается данными из командной строки пакета MATLAB:

```
ANFIS info:
        Number of nodes: 53
        Number of linear parameters: 48
        Number of nonlinear parameters: 24
        Total number of parameters: 72
        Number of training data pairs: 24
        Number of checking data pairs: 37
        Number of fuzzy rules: 16
Start training ANFIS ...
1    0.00222368        0.0165961
2    0.00227145        0.0169721
Designated epoch number reached. ANFIS training completed at epoch 2.
```

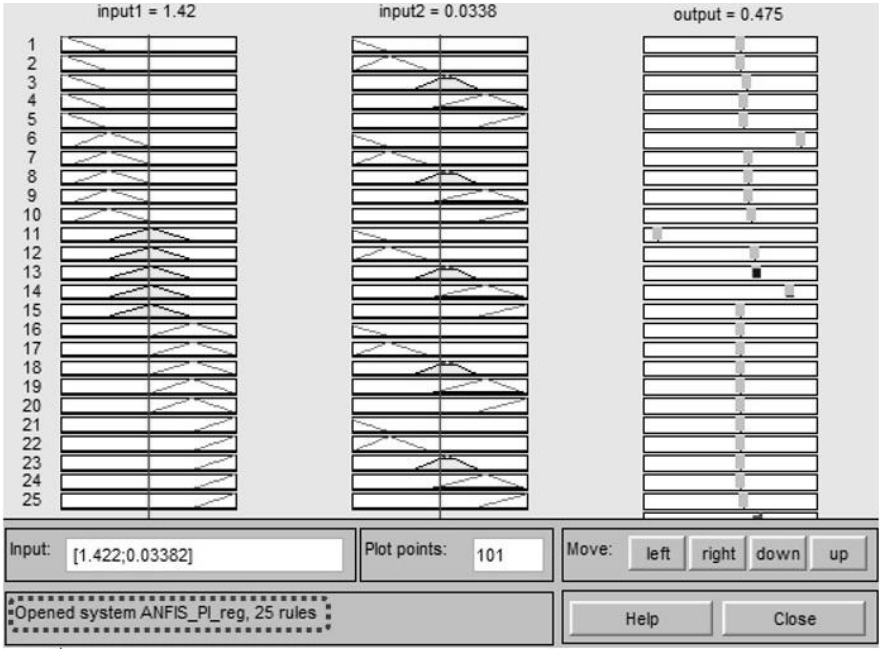


Рис. 4. База правил нечеткого регулятора

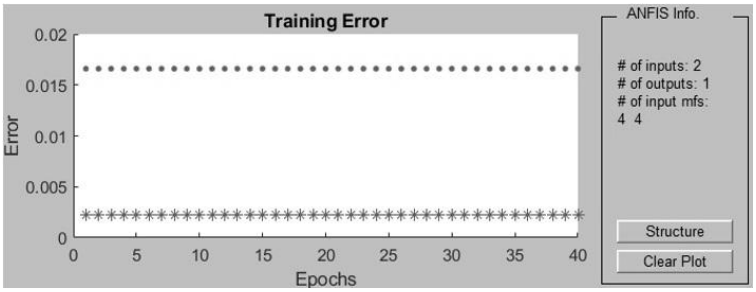


Рис. 5. Обучение гибридной сети

Следует обратить внимание, на строку «Number of fuzzy rules: 16», которая подтверждает уменьшение количества управляющих правил с 25 до 16 за счет сокращения функций принадлежности с пяти до четырех каждой входной лингвистической переменной. Это также подтверждается визуально представленной базой правил на рис. 6 и сгенерированной структурой системы нечеткого вывода FIS типа Сугено, представленной на рис. 7.

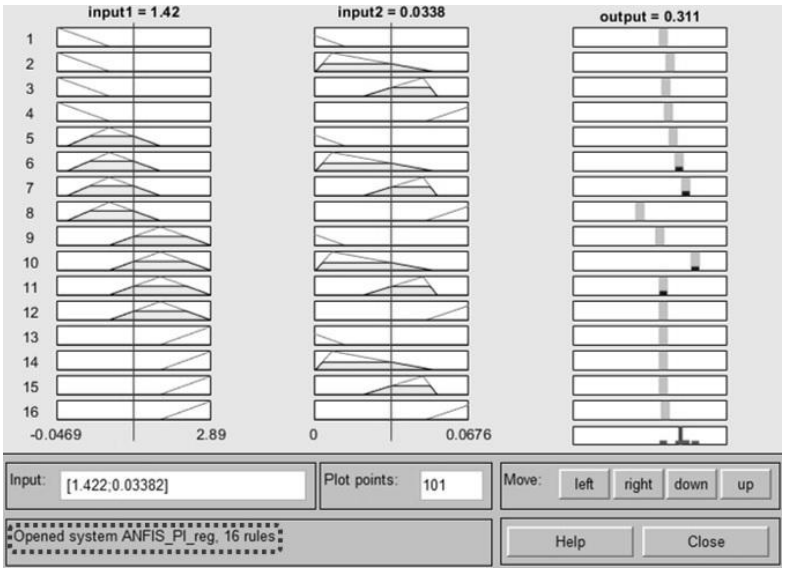


Рис. 6. База правил нечеткого регулятора после кластеризации

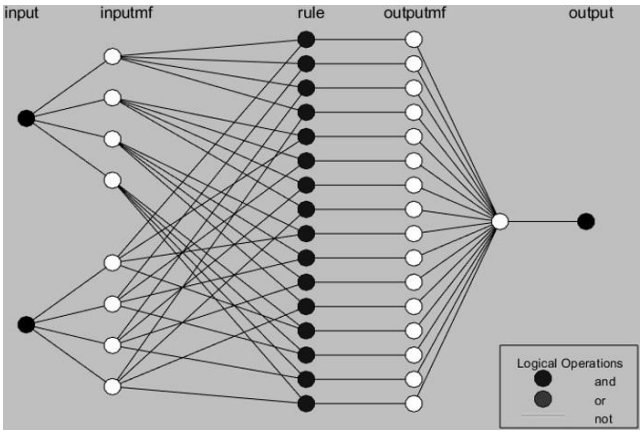


Рис. 7. Сгенерированная структура системы нечеткого вывода

Результаты работы метода. Для доказательства эффективности предложенного метода рассмотрим результаты моделирования работы интеллектуального регулятора до выполнения субтрактивной кластеризации и после, представленные на рис. 8.

Из графиков переходных процессов и поверхностей нечеткого вывода, полученных в ходе моделирования для случаев управления техническим объектов до и после применения субтрактивной кластеризации однозначно видно, что качество управления не поменялось.

Видно, что, во-первых, нечеткий регулятор и до кластеризации и после показывает лучшие результаты по сравнению с классическим регулятором с учетом оценки качества регулирования по таким критериям как перерегулирование, количество колебаний, время регулирования.

Во-вторых, применение предложенного метода позволило сократить количество исходных данных для синтеза интеллектуального регулятора, количество функций принадлежности каждой из входных лингвистических переменных и количество управляющих правил, тем самым выполнена значительная оптимизация базы правил регулятора без потери качества управления.

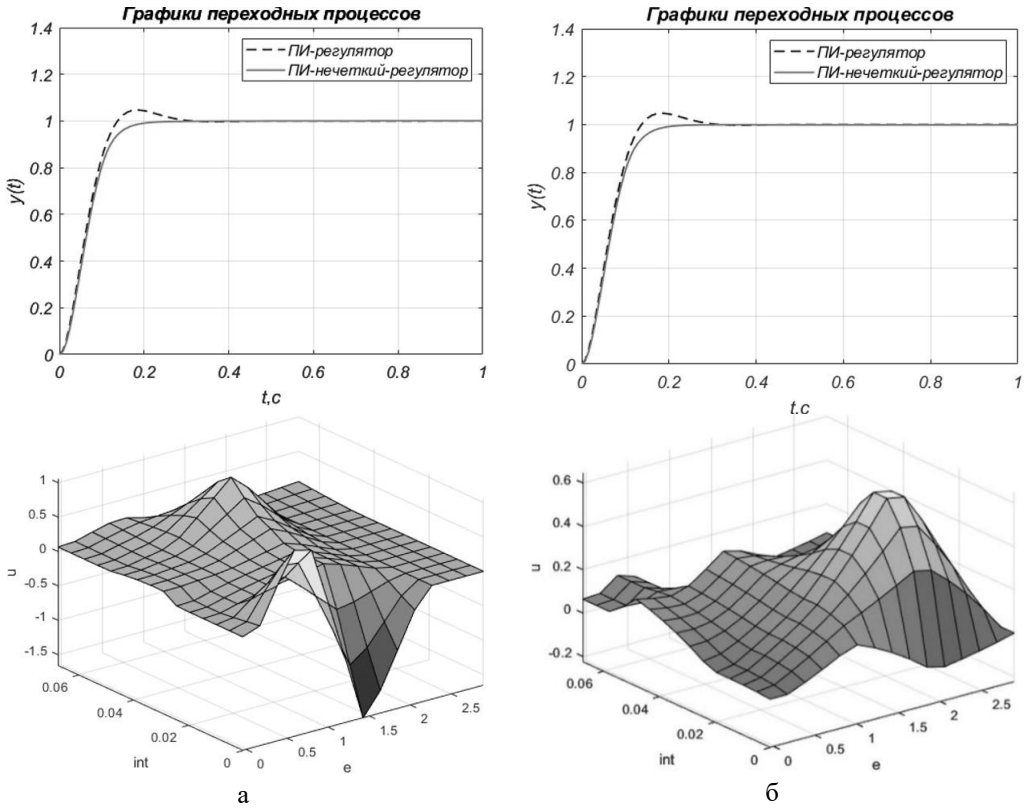


Рис. 8. Графики переходных процессов и поверхности нечеткого вывода: а – до кластеризации; б – после кластеризации

Заключение. Проведенные исследования и полученные результаты, представленные в настоящей статье, позволяют говорить о перспективности применения механизмов нечеткой кластеризации в системах управления, реализованных с применением интеллектуальных регуляторов. Научная новизна исследования заключается в разработке нового метода автоматической оптимизации базы правил интеллектуального регулятора. Основная идея метода основана на применении субтрактивного кластерного анализа в гибридных моделях управления техническими объектами с использованием интеллектуального регулятора, что позволяет повысить быстродействие модели управления за счет оптимизации базы правил регулятора, а также сократить время его разработки. Показатели качества управления, полученные в ходе моделирования, полностью подтвердили работоспособность разработанного метода. Это свидетельствует о перспективности применения полученных результатов на практике при проектировании современных автоматизированных систем управления. Дальнейшие исследования авторов будут направлены на обобщение результатов, полученных в ходе моделирования различных систем управления с применением интеллектуальных регуляторов, синтезированных с помощью субтрактивной кластеризации и алгоритма FCM (алгоритма нечетких с-средних).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Siavash Shirali, Saeed Zolfaghari Moghaddam, Mortaza Aliasghary.* An interval Type-2 fuzzy Fractional-Order PD-PI controller for frequency stabilization of islanded microgrids optimized with CO algorithm // International Journal of Electrical Power & Energy Systems. – March 2025. – Vol. 164. – 110422. – https://doi.org/10.1016/j.ijepes.2024.110422.
2. *Mohamed I. Abdo, Emad A. Elsheikh.* Optimization of a fractional-order interval type-2 fuzzy PID controller based on BBO for real-time applications // Franklin Open. – September 2024. – Vol. 8. – 100121. – https://doi.org/10.1016/j.fraope.2024.100121.

3. *Xuguang Chai, Yalin Wu, Lei Feng.* Energy-efficient scalable routing algorithm based on hierarchical agglomerative clustering for Wireless Sensor Networks // Alexandria Engineering Journal. – May 2025. – Vol. 120. – P. 95-105. – https://doi.org/10.1016/j.aej.2025.02.018.
4. *Mingyang Geng, Yuying Shang, Shiyu Xiang, Jiachen Wang, Lei Wang, Huaibo Song.* Using improved density peak clustering algorithm for flower cluster identification and apple central and peripheral flower detection // Computers and Electronics in Agriculture. – May 2025. – Vol. 232. – 110095. – https://doi.org/10.1016/j.compag.2025.110095.
5. *Hongkang Zhang, Shao-Lun Huang.* Improved fuzzy C-means clustering algorithm based on fuzzy particle swarm optimization for solving data clustering problems // Mathematics and Computers in Simulation. – July 2025. – Vol. 233. – P. 311-329. – https://doi.org/10.1016/j.matcom.2025.02.012.
6. *Guangchuan Hu, Amin Rezaeipanah.* Noise-robust semi-supervised clustering learning framework considering weighted consensus and pairwise similarities // Neurocomputing. Available online 16 February 2025, 129700. – https://doi.org/10.1016/j.neucom.2025.129700.
7. *Jun Ye, Zhaowang Hu, Zhengqi Zhang.* General-purpose multi-user privacy-preserving outsourced k-means clustering // Journal of Information Security and Applications. – March 2025. – Vol. 89, 103976. – https://doi.org/10.1016/j.jisa.2025.103976.
8. *Guohui Ding, Yankai Wang, Chenyang Li, Haohan Sun, Cailong Li, Lei Wang, Haijun Yin, Tiantian Huang.* HSCFC: High-dimensional streaming data clustering algorithm based on feedback control system // Future Generation Computer Systems. – September 2023. – Vol. 146. – P. 156-165. – https://doi.org/10.1016/j.future.2023.04.008.
9. *Lei Li, Xiao-Li Yin, Xin-Chun Jia, Behrooz Sobhani.* Day ahead powerful probabilistic wind power forecast usingcombined intelligent structure and fuzzy clustering algorithm // Energy. – 2020. – Vol. 192. – 116498. – https://doi.org/10.1016/j.energy.2019.116498.
10. *Mao Yang, Chaoyu Shi, Huiyu Liu.* Day-ahead wind power forecasting based on the clustering of equivalent power curves // Energy. – 1 March 2021. – Vol. 218. – 119515. – https://doi.org/10.1016/j.energy.2020.119515.
11. *Tao Tan, Tao Zhao.* A data-driven fuzzy system for the automatic determination of fuzzy set type based on fuzziness // Information Sciences. – September 2023. – Vol. 642. – 119173. – https://doi.org/10.1016/j.ins.2023.119173.
12. *Fan Z., Chiong R., Hu Z., Lin Y.* A multi-layer fuzzy model based on fuzzy-rule clustering for prediction tasks // Neurocomputing. – 2020. – https://doi.org/10.1016/j.neucom.2020.04.031.
13. *Raul Ruiz de la Hermosa Gonzalez-Carrato.* Wind farm monitoring using Mahalanobis distance and fuzzy clustering // Renewable Energy. – 2018. – 123. – P. 526-540.
14. *Arash Chaghari, Mohammad-Reza Feizi-Derakhshi, Mohammad-Ali Balafar.* Fuzzy clustering based on Forest optimization algorithm // Journal of King Saud University – Computer and Information Sciences. – 2018. – 30. – P. 25-32.
15. *Mayank Baranwal and Srinivasa Salapaka.* Clustering and supervisory voltage control in power systems // International Journal of Electrical Power & Energy Systems. – July 2019. – Vol. 109. – P. 641-651. – https://doi.org/10.1016/j.ijepes.2019.02.025.
16. *Guanhao Liang, Haotian Liao, Zhaoyang Huang, Xiaoli Li.* Abnormal discharge detection using adaptive neuro-fuzzy inference method with probability density-based feature and modified subtractive clustering // Neurocomputing. – September 2023. – Vol. 551, 28. – https://doi.org/10.1016/j.neucom.2023.126513.
17. *Zhongwei Zhang, Mohammed Al-Bahrani, Behrooz Ruhani, Hossein Heybatian Ghalehsalimi, Nastaran Zandy Ilghani, Hamid Maleki, Nafis Ahmad, Navid Nasajpour-Esfahani, Davood Toghraie.* Optimized ANFIS models based on grid partitioning, subtractive clustering, and fuzzy C-means to precise prediction of thermophysical properties of hybrid nanofluids // Chemical Engineering Journal. – September 2023. – Vol. 471, 1. – https://doi.org/10.1016/j.cej.2023.144362.
18. *Naghmeh Jafarzade, Ozgur Kisi, Mahmood Yousefi, Mansour Baziar, Vahide Oskoei, Nilufar Marufi, Ali Akbar Mohammadi.* Viability of two adaptive fuzzy systems based on fuzzy c means and subtractive clustering methods for modeling Cadmium in groundwater resources // Heliyon. – August 2023. – Vol. 9, Issue 8. – https://doi.org/10.1016/j.heliyon.2023.e18415.
19. *Md. Faiyaj Ahmed Limon, Rhydita Shahrin Upoma, Nomita Sinha, Shristi Roy Swarna, Bidyut Kanti Nath, Kulsuma Khanum, Md Jubaer Rahman, Md. Shahid Iqbal.* Grey wolf optimization-based fuzzy-PID controller for load frequency control in multi-area power systems // Journal of Automation and Intelligence. Available online 8 January 2025. – https://doi.org/10.1016/j.jai.2025.01.002.
20. *Игнатьева А.С.* Нечеткая кластеризация как способ повышения эффективности управления в автоматических системах // Программные продукты и системы. – 2024. – Т. 37, № 4. – С. 566-575. – DOI: 10.15827/0236-235X.148.566-575.

21. *Игнатьев В.В.* Методы управления техническими объектами с помощью интеллектуальных регуляторов на основе самоорганизации баз знаний: монография. – Ростов-на-Дону; Таганрог: Изд-во ЮФУ, 2020. – 142 с. – ISBN 978-5-9275-3562-0. – DOI: 10.18522/801273622.
22. *Игнатьева А.А., Спиридонов О.Б., Игнатьев В.В., Шаповалов И.О., Соловьев В.В*. Оптимизация базы правил нечеткого регулятора на основе методов кластеризации // Тр. конгресса по интеллектуальным системам и информационным технологиям «IS&IT'18». Научное издание в 3-х т. Т. 2. – Таганрог: Изд-во Ступина С.А., 2018. – 418 с. – ISBN 978-5-6041321-4-2, ISBN 978-5-6041321-6-6 (Т. 2). – С. 35-44.

REFERENCES

1. *Siavash Shirali, Saeed Zolfaghari Moghaddam, Mortaza Aliasghary.* An interval Type-2 fuzzy Fractional-Order PD-PI controller for frequency stabilization of islanded microgrids optimized with CO algorithm, *International Journal of Electrical Power & Energy Systems,* March 2025, Vol. 164, 110422. Available at: https://doi.org/10.1016/j.ijepes.2024.110422.
2. *Mohamed I. Abdo, Emad A. Elsheikh.* Optimization of a fractional-order interval type-2 fuzzy PID controller based on BBO for real-time applications, *Franklin Open,* September 2024, Vol. 8, 100121. Available at: https://doi.org/10.1016/j.fraope.2024.100121.
3. *Xuguang Chai, Yalin Wu, Lei Feng.* Energy-efficient scalable routing algorithm based on hierarchical agglomerative clustering for Wireless Sensor Networks, *Alexandria Engineering Journal,* May 2025, Vol. 120, pp. 95-105. Available at: https://doi.org/10.1016/j.aej.2025.02.018.
4. *Mingyang Geng, Yuying Shang, Shiyu Xiang, Jiachen Wang, Lei Wang, Huaibo Song.* Using improved density peak clustering algorithm for flower cluster identification and apple central and peripheral flower detection, *Computers and Electronics in Agriculture,* May 2025, Vol. 232, 110095. Available at: https://doi.org/10.1016/j.compag.2025.110095.
5. *Hongkang Zhang, Shao-Lun Huang.* Improved fuzzy C-means clustering algorithm based on fuzzy particle swarm optimization for solving data clustering problems, *Mathematics and Computers in Simulation,* July 2025, Vol. 233, pp. 311-329. Available at: https://doi.org/10.1016/j.matcom.2025.02.012.
6. *Guangchuan Hu, Amin Rezaeipanah.* Noise-robust semi-supervised clustering learning framework considering weighted consensus and pairwise similarities, *Neurocomputing*. Available online 16 February 2025, 129700. Available at: https://doi.org/10.1016/j.neucom.2025.129700.
7. *Jun Ye, Zhaowang Hu, Zhengqi Zhang.* General-purpose multi-user privacy-preserving outsourced k-means clustering, *Journal of Information Security and Applications,* March 2025, Vol. 89, 103976. Available at: https://doi.org/10.1016/j.jisa.2025.103976.
8. *Guohui Ding, Yankai Wang, Chenyang Li, Haohan Sun, Cailong Li, Lei Wang, Haijun Yin, Tiantian Huang.* HSCFC: High-dimensional streaming data clustering algorithm based on feedback control system, *Future Generation Computer Systems,* September 2023, Vol. 146, pp. 156-165. Available at: https://doi.org/10.1016/j.future.2023.04.008.
9. *Lei Li, Xiao-Li Yin, Xin-Chun Jia, Behrooz Sobhani.* Day ahead powerful probabilistic wind power forecast usingcombined intelligent structure and fuzzy clustering algorithm, *Energy,* 2020, Vol. 192, 116498. Available at: https://doi.org/10.1016/j.energy.2019.116498.
10. *Mao Yang, Chaoyu Shi, Huiyu Liu.* Day-ahead wind power forecasting based on the clustering of equivalent power curves, *Energy,* 1 March 2021, Vol. 218, 119515. Available at: https://doi.org/10.1016/j.energy.2020.119515.
11. *Tao Tan, Tao Zhao.* A data-driven fuzzy system for the automatic determination of fuzzy set type based on fuzziness, *Information Sciences,* September 2023, Vol. 642, 119173. Available at: https://doi.org/10.1016/j.ins.2023.119173.
12. *Fan Z., Chiong R., Hu Z., Lin Y.* A multi-layer fuzzy model based on fuzzy-rule clustering for prediction tasks, *Neurocomputing,* 2020. Available at: https://doi.org/10.1016/j.neucom.2020.04.031.
13. *Raul Ruiz de la Hermosa Gonzalez-Carrato.* Wind farm monitoring using Mahalanobis distance and fuzzy clustering, *Renewable Energy,* 2018, 123, pp. 526-540.
14. *Arash Chaghari, Mohammad-Reza Feizi-Derakhshi, Mohammad-Ali Balafar.* Fuzzy clustering based on Forest optimization algorithm, *Journal of King Saud University – Computer and Information Sciences,* 2018, 30, pp. 25-32.
15. *Mayank Baranwal and Srinivasa Salapaka.* Clustering and supervisory voltage control in power systems, *International Journal of Electrical Power & Energy Systems,* July 2019, Vol. 109, pp. 641-651. Available at: https://doi.org/10.1016/j.ijepes.2019.02.025.
16. *Guanhao Liang, Haotian Liao, Zhaoyang Huang, Xiaoli Li.* Abnormal discharge detection using adaptive neuro-fuzzy inference method with probability density-based feature and modified subtractive clustering, *Neurocomputing,* September 2023, Vol. 551, 28. Available at: https://doi.org/10.1016/j.neucom.2023.126513.

17. *Zhongwei Zhang, Mohammed Al-Bahrani, Behrooz Ruhani, Hossein Heybatian Ghalehsalimi, Nastaran Zandy Ilghani, Hamid Maleki, Nafis Ahmad, Navid Nasajpour-Esfahani, Davood Toghraie.* Optimized ANFIS models based on grid partitioning, subtractive clustering, and fuzzy C-means to precise prediction of thermophysical properties of hybrid nanofluids, *Chemical Engineering Journal,* September 2023, Vol. 471, 1. Available at: https://doi.org/10.1016/j.cej.2023.144362.
18. *Naghmeh Jafarzade, Ozgur Kisi, Mahmood Yousefi, Mansour Baziar, Vahide Oskoei, Nilufar Marufi, Ali Akbar Mohammadi.* Viability of two adaptive fuzzy systems based on fuzzy c means and subtractive clustering methods for modeling Cadmium in groundwater resources, *Heliyon,* August 2023, Vol. 9, Issue 8. Available at: https://doi.org/10.1016/j.heliyon.2023.e18415.
19. *Md. Faiyaj Ahmed Limon, Rhydita Shahrin Upoma, Nomita Sinha, Shristi Roy Swarna, Bidyut Kanti Nath, Kulsuma Khanum, Md Jubaer Rahman, Md. Shahid Iqbal.* Grey wolf optimization-based fuzzy-PID controller for load frequency control in multi-area power systems, *Journal of Automation and Intelligence*. Available online 8 January 2025. Available at: https://doi.org/10.1016/j.jai.2025.01.002.
20. *Ignat'eva A.S.* Nechetkaya klasterizatsiya kak sposob povysheniya effektivnosti upravleniya v avtomaticheskikh sistemakh [Fuzzy clustering as a way to improve control efficiency in automatic systems], *Programmnye produkty i sistemy* [Software Products and Systems], 2024, Vol. 37, No. 4, pp. 566-575. DOI: 10.15827/0236-235X.148.566-575.
21. *Ignat'ev V.V.* Metody upravleniya tekhnicheskimi ob"ektami s pomoshch'yu intellektual'nykh regulyatorov na osnove samoorganizatsii baz znaniy: monografiya [Methods of controlling technical objects using intelligent controllers based on self-organization of knowledge bases: monograph]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2020, 142 p. ISBN 978-5-9275-3562-0. DOI: 10.18522/801273622.
22. *Ignat'eva A.A., Spiridonov O.B., Ignat'ev V.V., Shapovalov I.O., Solov'ev V.V.* Optimizatsiya bazy pravil nechetkogo regulyatora na osnove metodov klasterizatsii [Optimization of the rule base of a fuzzy controller based on clustering methods], *Tr. kongressa po intellektual'nym sistemam i informatsionnym tekhnologiyam «IS&IT'18». Nauchnoe izdanie v 3-kh t. T. 2* [Proceedings of the Congress on Intelligent Systems and Information Technologies "IS&IT'18". Scientific publication in 3 vol. Vol. 2]. Taganrog: Izd-vo Stupina S.A., 2018, 418 p. ISBN 978-5-6041321-4-2, ISBN 978-5-6041321-6-6 (Vol. 2). S. 35-44.

Игнатьева Александра Сергеевна – Южный федеральный университет; e-mail: alexandra_25@mail.ru; г. Таганрог, Россия; кафедра систем автоматизированного управления; соискатель.

Шадрина Валентина Вячеславовна – Южный федеральный университет; e-mail: vvshadrina@sfedu.ru; г. Таганрог, Россия; кафедра систем автоматического управления; к.т.н., зав. кафедрой.

Игнатьев Владимир Владимирович – Южный федеральный университет; e-mail: vvignatev@sfedu.ru; г. Таганрог, Россия; к.т.н.; в.н.с.

Максимов Александр Викторович – Южный федеральный университет; e-mail: avmaksimov@sfedu.ru; кафедра встраиваемых и радиоприемных систем; к.т.н.; доцент.

Ignatyeva Alexandra Sergeevna – Southern Federal University; e-mail: alexandra_25@mail.ru; Taganrog, Russia; the Department of Automated Control Systems; applicant.

Shadrina Valentina Vyacheslavovna – Southern Federal University; e-mail: vvshadrina@sfedu.ru; Taganrog, Russia; the Department of Automatic Control Systems; cand. of eng. sc.; head of the department.

Ignatyev Vladimir Vladimirovich – Southern Federal University; e-mail: vvignatev@sfedu.ru; Taganrog, Russia; cand. of eng. sc.; leading researcher.

Maksimov Aleksandr Victorovich – Southern Federal University, e-mail: avmaksimov@sfedu.ru; Taganrog, Russia; the Department of Embedded and Radio Receiving Systems; cand. of eng. sc.; associate professor.

УДК 629.07.017 DOI 10.18522/2311-3103-2025-3-198-212

А.Л. Веревкин, И.Э. Джозефс, В.В. Мисюра, Л.С. Веревкина

МУЛЬТИАГЕНТНАЯ СИСТЕМА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБРАБОТКИ ИЗОБРАЖЕНИЙ С КАМЕР ТЕХНИЧЕСКОГО ЗРЕНИЯ ДРОНА

Мультиагентная технология с дронами, современными сенсорами, точным GPS и искусственном интеллекте, привели к прорыву в области киберфизических систем. В этой статье представлена мультиагентная система с использованием искусственного интеллекта для обработки изображений с камер технического зрения установленных на дроне. Разработана структурная схема мультиагентной системы на дроне на базе эффективной и простой платформе взятой с октокоптера ARRISE 410 – сельскохозяйственного дрона опрыскивателя с: интеллектуальной системой управления; всенаправленным цифровым микроволновым радаром; 6-ти осевым акселерометром высокой точности; электронным ватерпасом измерения наклона; оптической камерой реального времени с видом от первого лица; панелью управления, оснащенной новейшей системой передачи сигналов Light Bridge 2; пультом дистанционного управления, защищенного от попадания пыли и воды. Комплект необходимо дополнить: гиперспектральной HS – камерой для сканирования, ее модулем питания и возможностью сопряжения с системами дрона ARRISE 410, модулем сжатия информауции. Макет для исследования пропускной способности на DJI Agras T20 гексакоптере DJI Agras T20, сетевая карта MikrotikRB411 5G, микрокомпьютер Raspberry Pi 3, RGB-камера 1 Mpix , встроенный бортовой компьютер Raspberry Pi OV5647 v1.3 и гиперспектральная HS – камера 2 Resonon Pika L снимает гиперспектральные данные с 281 спектральными полосами со спектральными длинами волн от 400 до 1000нм и пространственным разрешением 900 гиперспектральных пикселей на строку изображения. В статье решена задача экспериментальным и расчетным путем определить требуемое сжатие информации получаемой с камер гиперспектрального и оптического диапазона с передачей через оператор связи и интернет для обработки изображений искусственным интернетом

Мультиагентная система; искусственный интеллект; обработка изображнений; гиперспектральная камера; камера оптического диапазона; дрон.

A.L. Verevkin, I.E. Josephs, V.V. Misyura, L.S. Verevkina

MULTI-AGENT SYSTEM USING ARTIFICIAL INTELLIGENCE TO PROCESS IMAGES FROM THE DRONE'S TECHNICAL VISION CAMERAS

Multi-agent technology with drones, modern sensors, precise GPS and artificial intelligence, have led to a breakthrough in the field of cyber-physical systems. This article presents a multi-agent system using artificial intelligence to process images from technical vision cameras installed on a drone. A block diagram of a multi-agent system on a drone was developed based on an effective and simple platform taken from the ARRISE 410 octocopter – an agricultural sprayer drone with: intelligent control system; omnidirectional digital microwave radar; 6-axis high-precision accelerometer; electronic level for measuring tilt; real-time optical camera 1 with a first-person view; control panel equipped with the latest Light Bridge 2 signal transmission system; remote control has a design protected from dust and water. The kit must be supplemented with: hyperspectral HS - camera for scanning, its power module and the ability to interface with the ARRISE 410 drone systems, an information compression module. Model for studying the throughput on the DJI Agras T20 hexacopter DJI Agras T20, MikrotikRB411 5G network card, Raspberry Pi 3 microcomputer, 1 Mpix RGB camera, built-in on-board computer Raspberry Pi OV5647 v1.3 and hyperspectral HS - camera 2 Resonon Pika L shoots hyperspectral data with 281 spectral bands with spectral wavelengths from 400 to 1000 nm and a spatial resolution of 900 hyperspectral pixels per image line. The article solves the problem of experimentally and computationally determining the required compression of information obtained from hyperspectral and optical range cameras with transmission through a telecom operator and the Internet for image processing by an artificial Internet.

Multi-agent system; artificial intelligence; image processing; hyperspectral camera; optical range camera; drone.

Введение. В настоящее время растет интерес к использованию дронов для сбора данных, наблюдения и мониторинга в областях обороны, безопасности, охраны окружающей среды и гражданских объектов. Прикладные решения, основанные на мультиагентных технологиях взаимодействия дрона, сенсоров, точного GPS, серверов интернета и сотовой связи, камер технического зрения привели к прорыву в области киберфизических систем. Дроны по отношению к спутникам или пилотируемые самолетам, имеют ряд преимуществ они дешевле, с более гибким временем повторного полета и лучшим пространственным и спектральным разрешением, что позволяет проводить более глубокий и точный анализ данных [1]. В научной литературе есть исследовательские публикации в разных областях, которые подтверждают большой спрос на дроны, рассмотрим некоторые из них: в работе [2] дрон используются для обнаружения, автоматического наблюдения и контроля состояния линий электропередач; в работе [3] рассмотрены миссии испытаний обеспечения безопасности, защиты и спасения с использованием дронов; в работе [4] приведено использование малогабаритных дронов в полицейских управлениях, пожарных бригадах и других организациях безопасности и охраны. Однако в области сельского хозяйства дистанционное использование дронов прочно закрепилось, как их новая область применения [5]. В Японии на 20% сельхозугодий используются дроны для посева, обработки, и наблюдения за растениями. По оценкам аналитического агентства Fact.MR, рынок агродронов к 2033 году вырастет в 4 раза до 14 млрд долларов [6].

Сельское хозяйство и природоохранная отрасли могут получить огромную выгоду от мультиагентных технологий с точки зрения экономии времени, ресурсов и человеческого труда, не говоря уже об аспектах, связанных с защитой окружающей среды. Новое направление точное земледелие (или точное фермерство), основано на наблюдении и измерении роста сельскохозяйственных культур. Ключевой технологией в точном земледелии является гиперспектральная визуализация, сначала использованной на спутниках и пилотируемых самолетах, состоящей из сотен спектральных диапазонов, что облегчает преобразование скрытых данных в нужную информацию. Поэтому разработка и исследование мультиагентной системы с использованием искусственного интеллекта для обработки изображений с камер технического зрения дрона (далее по тексту МСИИ дрона) актуальна.

Постановка задачи. В статье поставлены и решены задачи:

- рассмотреть особенности современных камер предназначенных для сбора данных;
- определить структуру и разработать структурную схему МСИИ дрона и ее реализацию;
- определить состав макета МСИИ дрона для исследования пропускной способности модулей связи посредством сотового оператора МТС и интернет;
- выполнить расчет требуемых параметров сжатия информации с гиперспектральной камеры для передачи через сотовый оператор связи МТС и интернет для обработки искусственным интеллектом.

Особенности современных камер технического зрения. Дистанционное наблюдение оптического диапазона RGB-камерами используются населением в повседневной жизни, например Google Earth или навигационные системы.

С 1972 году хорошо зарекомендовало себя систематическое наблюдение за поверхностью Земли многоспектральными камерами. Применение многоспектральных камер многочисленны, начиная от наблюдения за океаном до мониторинга растительного покрова и биомассы.

С 1980-х годов началось использование данных дистанционного наблюдения гиперспектральными камерами с самолетов, затем со спутников, запущенных в начале 21-го века. Благодаря более высокому спектральному разрешению данных гиперспектральных камер, это открыло возможность для нового применения. Гиперспектральное картографирование с помощью дронов стало вызывать повышенный интерес в научном сообществе примерно 10 лет назад и с тех пор получило дальнейшее развитие.

Спектры различных камер технического зрения, показаны на рис. 1. Типичная RGB-камера оптического диапазона имеет три широких спектральных канала (рис. 1,а).

Мультиспектральная камера обычно имеет больше каналов, которые более узкие дают данные (рис. 1,б).

Гиперспектральная HS-камера обычно имеет более 100 смежных спектральных полос (рис. 1,в).

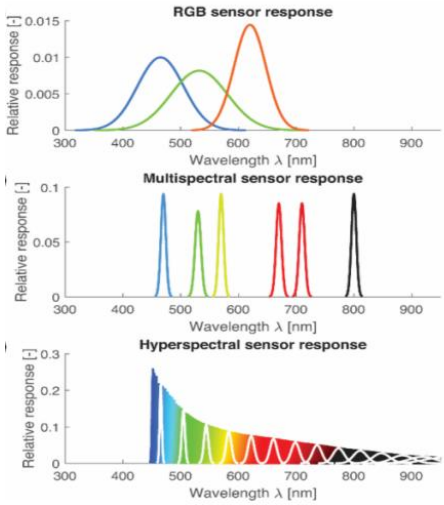


Рис. 1. Спектральные характеристики оптического диапазана RGB-камеры, мультиспектральной камеры и гиперспектральной HS-камеры

Полосы гиперспектральной HS-камеры расположены близко друг к другу и перекрываются, поэтому каждая десятая полоса отображается белым цветом для видимости функций отклика полос. На рис. 2 приведен моделируемый отклик a) трех типов датчиков, измеряющих отражательную способность поля риса и b) измеряющих нисходящую облученность [7].

Для обработки изображений искусственным интеллектом необходим учет отражательной способности рисовых культур и нисходящей освещенности от облаков (a+b) спектров. RGB-камера показывает только общие тенденции, но не может разрешить какие-либо спектральные детали. Мультиспектральная камера хорошо представляет спектральную форму отражательной способности ростков риса, поскольку местоположения спектральных полос были выбраны для мониторинга растительности, но особенности атмосферного поглощения нисходящей освещенности остаются необнаруженными. Спектр (рис. 2) гиперспектральной HS-камеры точно следует форме отражательной способности растений риса и нисходящей освещенности, в то время, как особенности освещенности в ближней инфракрасной области (NIR) менее резкие из-за увеличенной полосы пропускания камеры.

Хотя дистанционное наблюдение гиперспектральной HS-камеры с дрона может обеспечить беспрецедентный уровень спектральной детализации благодаря сверхвысокому пространственному и спектральному разрешению и дает возможность сбора данных под облаками. Установка гиперспектральной HS-камеры на дрон требует легких и миниатюрных сенсоров из-за ограничений по весу и размеру полезной нагрузки дрона. Миниатюризация сенсоров приводит к снижению точности и снижению отношения сигнал/шум по сравнению с более крупными, размещенными на самолетах или спутниках, однако при изменяющемся облачном покрове, затрудняет картирование отражательной способности поверхности земли, поскольку не только отражательная способность поверхности, но и изменяющаяся освещенность влияет на измеренную восходящую освещенность.

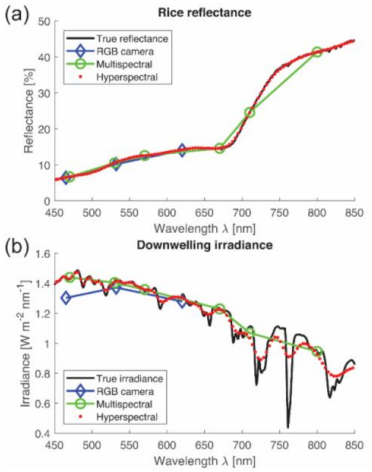


Рис. 2. Спектральные характеристики оптического диапазана RGB-камеры, мультиспектральной камеры и гиперспектральной HS-камеры растительности рисового поля

В солнечных условиях отражательную способность можно картировать с помощью радиометрических опорных точек, методом эмпирических линий или нисходящую освещенность измерять с помощью моделей переноса излучения. Эти методы не работают при изменяющейся освещенности, в условиях изменяющейся облачности. Поэтому необходимо измерять нисходящую освещенность в то же время и в том месте, где измеряется восходящая освещенность и требуется ориентация по отношению к солнцу. Значения измеренной нисходящей радиации распространяются на картирование отражения. Нисходящая радиация имеет две составляющие: прямая радиация, которая достигает поверхности земли по прямому пути от солнца, и непрямая радиация, которая достигает поверхности земли со всего неба после рассеяния, например, аэрозолями, облаками и рэлеевским рассеянием. Предполагается, что непрямая радиация изотропна по полусфере, изменения в ориентации датчика ILS не влияет на измеренную непрямую радиацию. Эффект прямой радиации рассчитывается с помощью закона косинуса Ламберта, по геометрии солнечного датчика. Это было использовано Лонгом 2010, который измерил вклад прямой и непрямой радиации с помощью специально разработанного датчика ILS, чтобы скорректировать измеренную нисходящую радиацию с учетом эффектов наклона, достигая ошибок менее 10 Вт/м^2 для 90 % данных. В 2018г. была скорректирована нисходящая освещенность с учетом наклона датчика, путем измерений несколькими датчиками ILS с разными углами обзора, интегрированных в один датчик, и была определена нисходящая освещенность, соответствующая датчику с горизонтальной поверхностью, путем интерполяции, с точностью стабильности 2,5 % во время полета [8–11].

Из рассмотренных методов следует вывод, что для обучения искусственного интеллекта необходимо при изменяющейся освещенности, в условиях облачности измерять нисходящую освещенность в то же время и в том месте, где измеряется восходящая освещенность и требуется ориентация по отношению к солнцу, что возможно с двумя камерами технического зрения и специально разработанным подвесом для ориентации камер.

Обзор гиперспектральных HS-камер. Гиперспектральные HS-камеры имеют до сотен смежных спектральных полос, что позволяет измерять яркость, как непрерывную функцию длин волн. Независимо от воздушной платформы авиационной, спутниковой, дрона камеры технического зрения играют важную роль в получении данных. Есть четыре основных метода для измерений: гиперспектральная съемка, мультиспектральная съемка, спектрометрия и RGB-снимки. Сравнения методов отображено в табл. 1, в которой учитываются (1) пространственные и (2) спектральные различия. Классификация, основанная, на условной оценке (1–3), использовалась для определения возможностей получения спектральной и пространственной информации

Таблица 1

Основные различия между гиперспектральной и мультиспектральной съемкой, спектроскометрией и RGB-снимками

Камеры технического зрения	Спектральная информация	Пространственная информация
Гиперспектральная	○ ○ ○	○ ○ ○
Мультиспектральная	○ ○	○ ○ ○
Спектрометрии	○ ○ ○	○
RGB-снимков	○	○ ○ ○

По сравнению с другими, гиперспектральные сенсоры наиболее эффективно работают и в спектральном и в пространственном отношении. RGB-изображения не дают спектральной информации за пределами видимого спектра, что имеет большое значение для характеристики химических и физических свойств объектов. С другой стороны, спектрометрия является технологией, в основном используемой для обнаружения крошечных областей (например, пятнистости листьев) с целью получения спектральных образцов без пространственного определения. Относительно мультиспектральной съемки, то она уступает гиперспектральной именно в получении детальной спектральной информации. Таким образом, гиперспектральная технология зондирования должна быть предпочтительной, когда дело доходит до получения информации о химических и физических свойствах.

Гиперспектральные камеры бывают двух типов: с зарядовой связью (CCD) и металл-оксид-полупроводниковые сенсоры (CMOS). Оба включают массивы фотодиодов, которые могут быть созданы с использованием на разных частотах материалов гиперспектральных камер, как показано на рис. 3. Материалы, используемые при изготовлении гиперспектральных камер: кремний (Si) – для получения информации в ультрафиолетовой, видимой и коротковолновой NIR полосах; арсенид индия (InAs) и арсенид галлия (GaAs) имеет спектральный отклик в полосе от 900 до 1700 нм; арсенид индия-галлия (InGaAs) расширяет предыдущий диапазон до 2600 нм; и ртутно-кадмиевый теллурид (MCT или HgCdTe) характеризуется большим спектральным диапазоном с высокой квантовой эффективностью, что позволяет достичь полос инфракрасных каналов (около 2500-25000 нм) и области NIR (около 800-2500) [12].

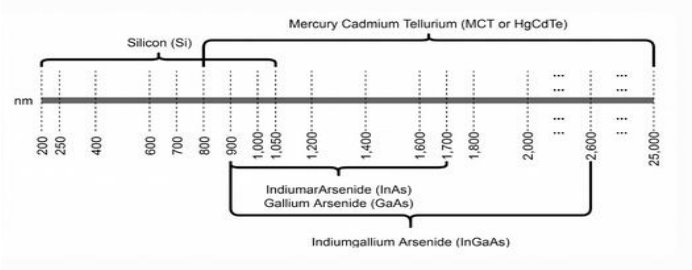


Рис. 3. Использование на разных частотах материалов гиперспектральных камер

Что касается режимов получения данных, то их выделяют четыре: точечное сканирование (или whiskbroom), линейное сканирование (или pushbroom), плоское сканирование и одиночный кадр (singleshot) (рис. 4). В то время как режим whiskbroom получает все полосы попиксельно, перемещая детектор в пространстве x - y, для хранения данных в форме массива попиксельной записи спектральных каналов (BIP), режим pushbroom работает аналогично, но вместо пиксельного сканирования формируется линия, которая, в конечном счете, записывается массив полинейной записи спектральных каналов (BIL). Несколько других характеристики режима pushbroom включают компактный размер, малый вес, более простое управление и более высокий уровень сигнала. В режиме плоского сканирования создается массив поканальной записи (BSQ), состоящий из нескольких изображений, снятых за один раз, каждое из которых содержит спектральные данные относительно всего данного пространства x - y.

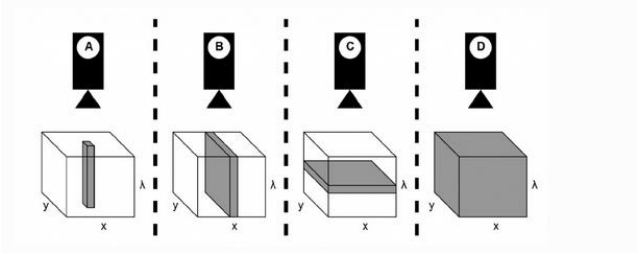


Рис. 4. Гиперспектральные режимы получения данных: A – точечное сканирование; B – линейное сканирование; C – плоское сканирование; D – объемное сканирование, C и D относится к одиночному кадру

Наконец, есть еще режим, который получает все пространственные и спектральные данные одновременно, известен он как одиночный кадр (singleshot).

Список доступных коммерческих гиперспектральных сенсоров представлен в табл. 2 [13].

Таблица 2

Manuf.	Sensor	Spectral Range (nm)	No. Bands	Spectral Resol. (nm)	Spatial Resol. (px)	Acquis. Mode	Weight (g)
BaySpec	OCI-UAV-1000	600–1000	100	<5 [b]	2048 [d]	P	272
Brandywine Photonics	CHAI S-640	825–2125	260	5 [c]	640 × 512	P	5000
	CHAI V-640	350–1080	256	2.5 [c] 5 [c] 10 [c]	640 × 512	P	480
Cubert GmbH	S 185—FIREFLEYE SE	450–950 355–750	125	4 [c]	50 × 50	S	490
	S 485—FIREFLEYE XL	450–950 550–1000	125	4.5 [c]	70 × 70	S	1200
	Q 285—FIREFLEYE QE	450–950	125	4 [c]	50 × 50	S	3000
Headwall Photonics Inc., Fitchburg, MA, USA	Nano HyperSpec	400–1000	270	6 [b]	640 [d]	P	1200 [e]
	Micro Hyperspec VNIR	380–1000	775 837 923	2.5 [b]	1004 [d] 1600 [d]	P	≤3900
HySpex	VNIR-1024	400–1000	108	5.4 [c]	1024 [d]	P	4000
	Mjolnir V-1240	400–1000	200	3 [c]	1240 [d]	P	4200
	HySpex SWIR-384	1000–2500	288	5.45 [c]	384 [d]	P	5700
MosaicMill	Rikola	500–900	50 [a]	10 [b]	1010 × 1010	S	720
NovaSol	vis-NIR microHSI	400–800 400–1000 380–880	120 180 150	3.3 [c]	680 [d]	P	<450
	Alpha-vis micro HSI	400–800 350–1000	40 60	10 [c]	1280 [d]	P	<2100
	SWIR 640 microHSI	850–1700 600–1700	170 200	5 [c]	640 [d]	P	3500
	Alpha-SWIR microHSI	900–1700	160	5 [c]	640 [d]	P	1200
	Extra-SWIR microHSI	964–2500	256	6 [c]	320 [d]	P	2600
PhotonFocus	MV1-D2048x1088-HS05-96-G2	470–900	150	10-12 [b]	2048 × 1088	P	265
Quest Innovations	Hyperea 660 C1	400–1000	660	-	1024 [d]	P	1440
Resonon	Pika L	400–1000	281	2.1 [c]	900 [d]	P	600
	Pika XC2	400–1000	447	1.3 [c]	1600 [d]	P	2200
	Pika NIR	900–1700	164	4.9 [c]	320 [d]	P	2700
	Pika NUV	350–800	196	2.3 [c]	1600 [d]	P	2100
SENOP	VIS-VNIR Snapshot	400–900	380	10 [b]	1010 × 1010	S	720
SPECIM	SPECIM FX10	400–1000	224	5.5 [b]	1024 [d]	P	1260
	SPECIM FX17	900–1700	224	8 [b]	640 [d]	P	1700
Surface Optics Corp., San Diego, CA, USA	SOC710-GX	400–1000	120	4.2 [c]	640 [d]	P	1250
XIMEA	MQ022HG-IM-LS100-NIR	600–975	100+	4 [c]	2048 × 8	P	32
	MQ022HG-IM-LS150-VISNIR	470–900	150+	3 [c]	2048 × 5	P	300

Note: [a] 380 in laboratory; [b] at FWHM; [c] by sampling; [d] Pushbroom length line (the other dimension depends on sensor's sweep distance); [e] without lens and global positioning system (GPS); P—Pushbroom; S—Snapshot.

Кроме того, укажем некоторые проблемы присущие для каждого режима.

Точечная съемка – это режим медленной съемки, а линейная съемка должна выполняться за короткое время, чтобы избежать риска несоответствий в спектральном уровне полосы (насыщенность или недоэкспонирование). Плоское сканирование не подходит для движущихся сред, в то время как одиночный кадр (singleshot) – технологии в стадии разработки, которая не поддерживает высокое пространственное разрешение.

Установка гиперспектральных камер на дрон создает готовые системы, которые требуют взаимодействия как минимум с тремя производителями: камер технического зрения, дронов и искусственного интеллекта.

Структурная схема МСИИ дрона и ее реализация. Спектры, получаемые МСИИ дроном сначала калибруются затем анализируются с использованием нормализованного индекса неоднородности растительности (NDVI), модифицированного индекса коэффициента поглощения хлорофилла (MCARI) и модифицированного индекса растительности, скорректированного по почве (MSAVI) и другими способами обработки результатов, простым классификатором, применяемым к части одного из захваченных изображений. Сжатие в реальном времени, полученных данных, демонстрирует преимущества использования бортового вычислительного устройства с относительно высокой вычислительной мощностью.

В этой статье рассмотрена мультиагентная система искусственного интеллекта обработки изображений с камер технического зрения дрона и подробно описана устройство системы. Предлагаемое решение основано на дроне и гиперспектральной камерой и камерой оптического диапазона. В статье решена задача разработки МСИИ дрона с использованием искусственного интеллекта обработки изображений с камер технического зрения дрона, в которой вес, энергетический бюджет и подключение камер имеют первостепенное значение. На дроне установлена встроенная плата с расширенными возможностями обработки, чтобы контролировать его траекторию, управлять сбором данных и обеспечивать бортовую обработку, и передачу данных посредством мобильного сотового оператора МТС и сжатия информации, что имеет решающее значение из-за огромных объемов полученных данных для последующей обработки искусственным интеллектом (ИИ). ИИ используется ля обработки изображений и расчета различных индексов растительности: нормализованного индекса неоднородности растительности NDVI, модифицированного индекса коэффициента поглощения хлорофилла MCARI, модифицированного индекса растительности на почве MSAVI, которые являются численными и/или графическими или атрибутивными показателями свойств растительности. Дрон был успешно испытан в реальных условиях городской застройки г. Ростова на Дону России, и в пригороде на территории виноградника.

Использование дронов позволяет периодически контролировать растения во время их роста, а также контролировать внешние условия, которые повлияют на их состояние. Многоспектральные датчики широко используются на дронах для сбора спектральной информации, которая позволяет создать карты состояний растений [9–12]. Один из показателей это нормализованный разностный индекс вегетации NDVI, который указывает на жизнеспособность растений рассчитываемый по информации двух спектральных каналов, расположенных в красной и ближней инфракрасной полосах электромагнитного спектра [7, 9].

Существуют и другие индексы, кроме индекса NDVI, которые дают полезную информацию в интеллектуальном земледелии [8, 10]. Эти индексы рассчитываются по спектральной информации различных частей электромагнитного спектра. В данной статье рассмотрена разработка МСИИ дрона, способной нести гиперспектральную и оптическую камеры для сбора информации в широком диапазоне спектральных каналов, предоставляя информацию, которая может быть чрезвычайно полезна не только для приложений интеллектуального земледелия, но и для других приложений, таких как обнаружение загрязнений мазутом, обнаружение аномалий и классификации загрязнений углеводородными соединениями и других исследований. Однако использование гиперспектральных камер МСИИ дрона вместо мультиспектральных датчиков не лишено недостатков. Мультиспектральные датчики, специально разработанные для установки на дрон и управления ими с помощью встроенных устройств, а найти гиперспектральную камеру, которую можно напрямую установить на дрон проблемно.

Структурная схема СМИИ дрона, показана на рис. 5.

Рис. 5. Структурная схема СМИИ дрона

На базе сельскохозяйственного дрона опрыскивателя с грузоподъемностью до 25 кг. реализована структура МСИИ дрона и следующих компонентов на базе эффективной и простой платформы взятой с октокоптера ARRISE 410:

- интеллектуальная система управления;
- всенаправленный цифровой микроволновый радар;
- 6-ти осевой акселерометр высокой точности;
- электронный ватерпас измерения наклона;
- оптическая камера 1 реального времени с видом от первого лица;
- панель управления, оснащенная новейшей системой передачи сигналов Light Bridge 2;
- пульт дистанционного управления имеет конструкцию, защищенную от попадания пыли и воды;

В ARRISE 410 включены интеллектуальные запоминающие устройства, которые регистрируют прошлые и текущие точки полетного задания. В случае прерывания полета по различным причинам (упал заряд батареи), дрон автоматически возобновит работу с последней зарегистрированной точки.

Комплект необходимо дополнить: гиперспектральной HS – камерой для сканирования, ее модулем питания и возможностью сопряжения с системами дрона ARRISE 410, модулем сжатия информации модулем связи через оператор мегафон и сервером интернета и компьютером.

Реализация СМИИ дрона приведена на рис. 6. и выполнена на DJI Agras T20 гексакоптере [14], сетевая карта MikrotikRB411 5G, микрокомпьютер Raspberry Pi 3, RGB-камера 1 Mpix, встроенный бортовой компьютер Raspberry Pi OV5647 v1.3 [15] и гиперспектральная HS – камера 2 Resonon Pika L [16] снимает гиперспектральные данные с 281 спектральными полосами со спектральными длинами волн от 400 до 1000нм и пространственным разрешением 900 гиперспектральных пикселей на строку изображения.

Гиперспектральная камера видимого и ближнего инфракрасного диапазонов. RGB-камера с целью получения информации для верификации полученных гиперспектральных данных. Эти две камеры размещаются на подвесе для снижения влияния на изображения вибраций дрона. Система включает в себя встроенный бортовой компьютер Raspberry Pi 3 [17], для автономного управления полетом дрона и управления сбором данных. Плата проведения бортовой обработки данных, что значительно увеличивает применимость этой системы сбора данных.

Рис. 6. Реализация СМИИ дрона

Перезаряжаемая литиевая батарея, долгосрочной работы, емкость аккумулятора позволяет лететь 9-15минут.

Гиперспектральная камера видимого и ближнего инфракрасного диапазонов. Характеристики гипоспектральной камеры Resonon Pika L даны в табл. 3.

Таблица 3

Характеристики гипоспектральной камеры Resonon Pika L

Характеристика	Значение
Количество спектральных каналов	281
Спектральный диапазон, нм	400-1000
Возможность установки на дрон	Да
Объектив	6 / 8 / 12 / 17 / 23 / 50 / 70
Разрешение, нм	2.1
Частота кадров, Гц	249
Вес, кг	0.6
Размер, м	0.1 x 0.125 x 0.053
Подключение	USB 3.0
Питание, В	3.4
Размер пикселя, µm	5.86
Ширина спектрального канала, нм	1,07
Спектральное разрешение, нм	2,1
Гарантия, месяцев	12

Камере Resonon Pika L соответствуют гиперспектральные данные с 281 спектральными полосами со спектральными длинами волн от 400 до 1000нм и пространственным разрешением 1080 гиперспектральных пикселей на строку изображения.

Пульт управления:

- дальность связи (на открытом пространстве, при отсутствии препятствий): 1 км;
- мощность передающего модуля 100 мВт при 2,4 ГГц;
- встроенная батарея 6000 мА/ч, 2S LiPo;
- зарядное устройство DJI;

- мощность 9 Вт;
- рабочая температура от -10° до +40°C;

Зарядное устройство пульта управления:

- модель A14-057N1A;
- напряжение 17,4 В;
- номинальная мощность 57 Вт;
- сервер NUC7i7DNHE;
- 4 аккумулятора;
- модуль питания 5В;
- зарядное устройство для аккумуляторов (возможность одновременной зарядки двух аккумуляторов за 60 минут).

Экспериментальные исследования пропускной способности СМИИ дрона. В рааботе [18] рассмотрены особенности передачи данных, посредством использования различных средств в том числе и сотового оперетора связи Мегафон. Структурная схема макета для испытаний СМИИ дрона представлена на рис. 7. Также была установлена промышленная камера для Raspberry Pi 1.3 5мп с целью предоставления дополнительной информации для оценки пропускной способности. Эта камера размещена в подвесе для снижения вибраций дрона и повышения качества полученных изображений.

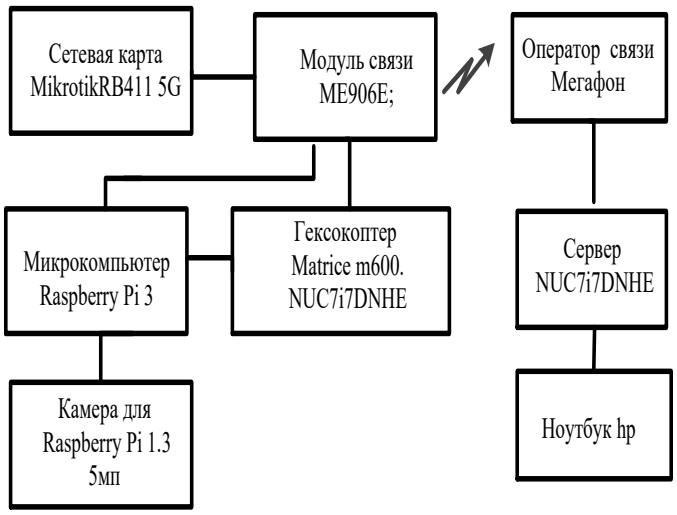


Рис. 7. Структурная схема макета для испытаний СМИИ дрона

В дополнение к устройствам, перевозимым дроном, была установлена наземная станция, состоящая из сервера и ноутбука hp, который взаимодействует с бортовым компьютером дрона через сотовый оператор МТС. Данные можно легко передавать с помощью сетевой карты и модуля связи. Система сбора данных была протестирована в разных сценариях подъема и спуска дрона в городской застройке, и над виноградником в пригороде Ростова на Дону. Полученные графики пропускной способности от высоты полета при подъеме и спуске дрона необходимы для определения бортового сжатия гиперспектральных данных в реальном времени таким образом, чтобы их можно было эффективно передавать на наземную станцию управления для дальнейшей обработки. Для выбора компрессора HyperLCA [19, 21] с использованием NVIDIA CUDA (архитектура унифицированных вычислительных устройств) и использования преимуществ параллелизма маломощного графического процессора (GPU). Полученные результаты позволяют определить производительность сжатия в реальном времени, а также установки такого рода бортовых вычислительных устройств на дрон.

Проведено исследование пропускной способности макета модуля передачи информации с камеры и оопределена возможность установки двух камер с разрешением Full-HD и HD (количество рядов и столбцов – это и есть разрешение экрана, при разрешении Full HD экран состоит из 1080 рядов и 1920 столбцов пикселей и HD; из 1280 рядов и 720 столбцов пикселей) на дрон. Сенсор OV5647 имеет встроенный процессор, отвечающий за функции управления экспозицией, баланса белого цвета, автокалибровки уровня чёрного цвета, коррекции дефективных пикселей, регулировки частоты кадров, автофокусировки, обработки изображения: зеркального переворота, обрезки, наклона, и т.д. Данные изображения выводятся в формате 8-/10-бит RGB RAW. Максимальное разрешение снимка/кадра составляет 2592 x 1944 графических точек (пикселей). Видеосъёмка в стандарте FullHD осуществляется с частотой 30 к/с. Зависимость частоты кадров относительно выбранного разрешения съёмки [19]: QSXGA (2592x1944) – 15 кадр/с; 1080p – 30 кадр/с [20], и потверждена возможность в реальном времени смотреть передаваемое изображение до 30 минут.

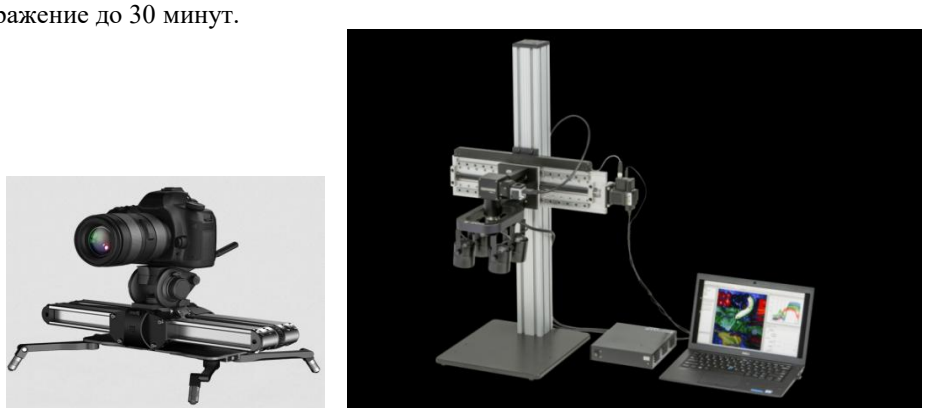


Рис. 8. Вид макета гипоспектральной камеры Resonon Pika L

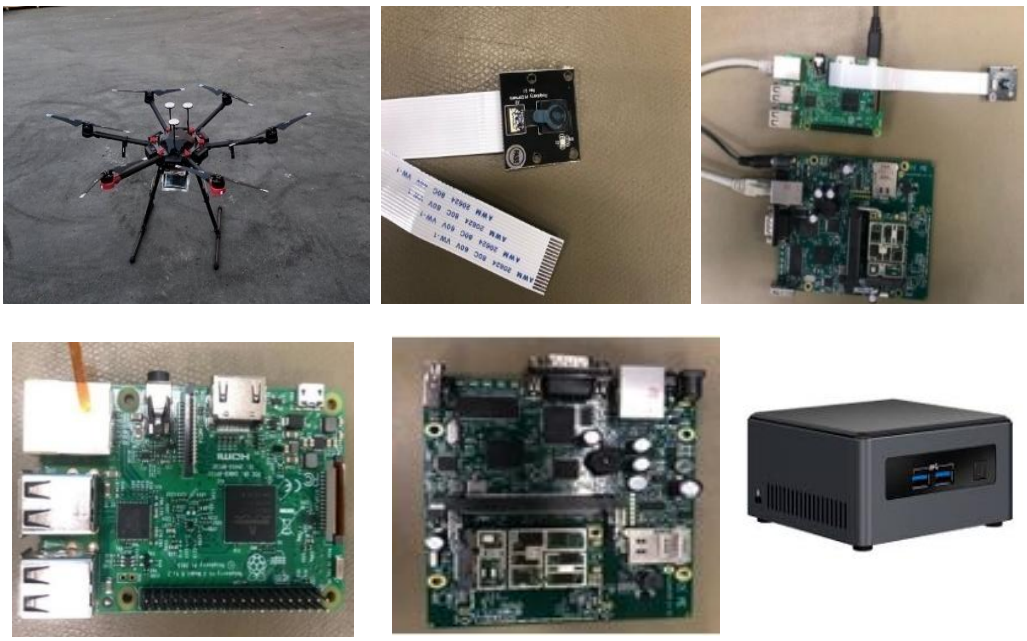


Рис. 9. Гексакоптер Matrice m600. NUC7i7DNHE и макет в составе: камера для Raspberry Pi 1.3 5мп; модуль связи ME906E; сетевая карта MikrotikRB411 5G; микрокомпьютер Raspberry Pi 3; сервер NUC7i7DNHE

Приведены графики измерения пропускной способности – скорости обмена данными от высоты полета (рис. 10) при подъеме и спуске дрона (указано стрелками) в городской застройке.

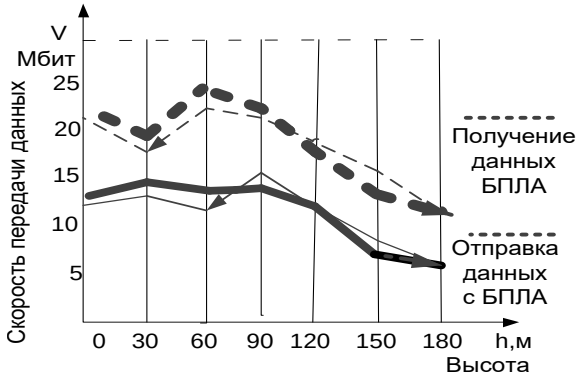


Рис. 10. Пропускная способности от высоты полета

Максимально время задержки управляющего сигнала не более 0,4 секунды по экспериментальным данным**.**

Расчет сжатия в реальном времени. Мегабайт в секунду (MB/s) – это единица измерения скорости передачи данных, которая указывает, сколько миллионов байт передаётся каждую секунду, при этом 1 мегабайт равен 8 мегабитам и когда 2 мегабайт в секунду равно 16 мегабитам в секунду будет соответствовать среднему значению пропускной способности полученной зависимости, пропускной способности на рис. 10. Рассмотренная система передачи информации через сотовый оператор может выступать каналом управления и/или передачи данных между дроном и оборудованием с базой данных ИИ, и позволяет формировать более эффективные с дешевым и высокого качества информационным каналом.

В СМИИ дрона входит наземное оборудование сервер NUC7i7DNHE с приложением adhoc, для передачи изображений посредством использования интернета и сотового оператора связи Мегафон.

Сервер взаимодействует с бортовым компьютером через сотовый оператор связи Мегафон, таким образом сбора данных может быть легко настроен. Получаемые изображения позволяют создавать наборы различных карт растительности и рельефа, экспереиментом потверждена возможность в реальном времени смотреть передаваемое изображение в течение 30минут на экране компьютера.

Сжатие получаемых гиперспектральных данных в реальном времени. Была также изучена возможность бортового сжатия получаемых гиперспектральных данных в реальном времени таким образом, чтобы их можно было СМИИ дрона использовать для дальнейшей обработки ИИ. Для этого можно использовать компрессор HyperLCA [21] на основе преобразования за счёт функции адаптивного искажения во время зондирования, которая обеспечивает несколько коэффициентов сжатия в одном сценарии. Новая версия компрессор Hyper LCA способна обрабатывать гиперспектральные изображения размером 1024x1024 и 180 спектральных диапазонов (377,5 Мб) за 0,935 секунды при энергопотреблении 1,145 Вт. А архитектура отличается высокой пропускной способностью (в миллионах выборок в секунду) и значительной энергоэффективностью (в мегабайтах в секунду на ватт) [13]. Полученные результаты в работе [7] подтверждают достижение производительности сжатия в реальном времени, а также демонстрируют преимущества переноса такого рода бортовых вычислительных устройств на таких дронах, как в макете.

При сборе получаемых с гиперспектральной камеры информации для последующего анализа объём данных получается большим – это гигабайты данных и передача такого большого объема данных потребует заметной траты времени, поэтому сжатие переда-

ваемой камерой информации представляется единственно верной опцией. Таким образом, на борту дрона должен использоваться алгоритм сжатия для передачи последующей передачи.

Скорость сбора данных гиперспектральной камеры Resonon Pika L составляет до 60 Мбайт в секунду. А скорость передачи данных макета 2 Мбайт в секунду**.** По этой причине размер полученных данных должен быть радикально уменьшен для возможности быстрой передачи, особенно если требуется передача в реальном времени. Для сжатия гиперспектральных изображений с потерями можно использовать алгоритм, основанный на методе главных компонент (PCA). Основная формула, связывающая количество гиперспектральных пикселей, количество бит на пиксель и степень сжатия, может быть представлена следующим образом:

$$C=(N*B)/R, \quad \text{отсюда} \quad Rp=(N*B)/C = 56 / 2 = 28,$$

где C – общее количество бит после сжатия , 2Мбит/с;

N – количество гиперспектральных пикселей на кадр;

B – количество бит, используемых для представления каждого пикселя, (N bits);

Rp – расчетная степень сжатия.

Для гиперспектральной камеры Resonon Pika L N*B=56 Мбит/с. Для использования гипоспектральной камеры Resonon Pika L СМИИ дрона необходима степень сжатия Rp = 28 компрессор HyperLCA позволяет обеспечить сжатие R=20, при определенных условиях работы часть информации можно распределить для хранения на плате дрона, а определенную часть передавать одновременно с зондированием.

Заключение. В настоящее время нет никаких сомнений относительно использования гипоспектральных камер в сочетании с дронами и мультиагентными технологиями, расширяющих возможности агентов при их взаимодействии в миссии. Задача адаптации промышленных камер технического зрения к дронам актуальна и требует уменьшения характеристик таких, как вес, размер, бюджет мощности и стоимости. В этой работе решена проблема разработки и исследования мультиагентной системы с использованием искусственного интеллекта для обработки изображений с камер технического зрения дрона.

Дрон включает в себя гиперспектральную камеру, точный GPS, контроллер и встроенную плату для взаимодействия с модульным приложением управления полетом. В результате предлагается решение для конкретного варианта использования точного зондирования, основанное на захвате 281 спектральных полос со скоростью до 249 кадров в секунду в диапазоне VNIR что позволит выполнить обработку различных индексов растительности, таких как известные NDVI, MSAVI и MCARI, для выявления особенностей виноградниковых зон в Ростовской области и юга России, открывая инновационные возможности в распознавании загрязнений мазутом береговой зоны, дистанционном зондировании влажности почвы, загрязнение окружающей среды пластиком и другие.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Berni J.A.J., Zarco-Tejada P.J., Suarez L. и Fereres E.* Thermal and Narrowband Multispectral Remote Sensing for Vegetation Monitoring from an Unmanned Aerial Vehicle // IEEE Transactions on Geoscience and Remote Sensing. – 2009. – Vol. 47. – P. 722-738.
2. *Li Z., Liu Y., Walker R., Hayward R. и Zhang J.* Towards automatic power line detection for a UAV surveillance system using pulse coupled neural filter and an improved Hough transform // Machine Vision and Applications. – 2010. – Vol. 21, No. 5. – P. 677-686.
3. *Бирк А., Виггерих Б., Бюлов Х., Пфингсторн М. и Швертфегер С.* Безопасность, защита и спасательные операции с использованием беспилотных летательных аппаратов (БПЛА) // J. Intel. Роботизированные системы. – 2011. – Т. 64, № 1. – С. 57-76.
4. *Дэниел К. и Витфельд К.* Использование инфраструктур общедоступных сетей для дистанционного зондирования с помощью БПЛА в гражданских операциях по обеспечению безопасности. – 2011.
5. *Faial B.S., Freitas H., Гомес Р.Н., Мано Л.Я., Пессин Г., де Карвалью А.С., Кришнамачари Б., Дж. Ueyama.* Адаптивный подход к распылению пестицидов на основе беспилотных летательных аппаратов в динамических средах // Вычисл. Электрон. Agric. – 2017. – 138 с.
6. https://docs.yandex.ru/docs/view?tm=1728206370&tld=ru&lang=ru&name=215085.pdf&text.

7. *Пабло Хорстранд, Рааль Герра, Айтами Родригес, Мария Диас, Себастьян Лопес, Хозе Фко Лопес*. Платформа БПЛА на основе гиперспектрального датчика для захвата изображений и бортовой обработки. – https://innoter.com/articles/giperspektralnaya-semka/.
8. *Адаои Т. и др*. Гиперспектральная съемка: обзор датчиков на базе БПЛА, обработки данных и приложений для сельского и лесного хозяйства // Удалённая чувствительность. – 2017. – Т. 9, 11. – 1110 с.
9. *Хант-младший Э.Р. и Дотри К.С.Т.* Какая польза от беспилотных летательных аппаратов для дистанционного зондирования сельского хозяйства и точного земледелия? // Int. J. Remote Sens. – 2018. – Т. 39. – С. 15-16.
10. *Huang J., Wang H., Dai Q. и Han D.* Анализ данных NDVI для идентификации сельскохозяйственных культур и оценки урожайности // IEEE J. Sel. Темы Прикладное наблюдение за Землей Дистанционное зондирование. – 2014. – Т. 7. – С. 4374-4384.
11. *Rey-Caramés C., Diago M.P., Martín M.P., Lobo A. и Tardaguila J.* Использование многоспектральных изображений RPAS для характеристики мощности, развития листьев, компонентов урожайности и изменчивости состава ягод в пределах виноградника // Удалённая чувствительность. – 2015. – Т. 7, № 11. – С. 14458-14481. – http://www.mdpi.com/2072-4292/7/11/14458.
12. Гиперспектральные камеры серии Specim FX1. Доступно: 4 мая 2019 г. – http://www.specim.fi/fx/.
13. https://sovzond.ru/press-center/articles/bpla/5601/.
14. https://geon.ru/product/dji-agras-t20-s-4-dop-akb-i-zu- geksakopter/?ysclid=m7aoja559 g30884089
15. https://compacttool.ru/camera-5-mpix-dlya-raspberry-pi?ysclid=m7apxj7qdy527308006.
16. https://resonon.com/Pika-L.
17. https://tixer.ru/catalog/raspberrypi/raspberry_pi_3_model_b_v1_2/?ysclid=m7aq4e66hj615743840.
18. *Веревкин А.Л., Сиренко Е.А.* Символы их предназначение и направление научного исследования Всемирный технологический университет ЮНЕСКО. Московский технологический институт // Матер. Международного форума. Вып. 1. «Инновации в сфере жизнедеятельности человека XXI века». – Ростов-на-Дону: Гинго, 2015. – С. 249-251.
19. https://compacttool.ru/camera-5-mpix-dlya-raspberry-pi?ysclid=m7aiz70xdw920542036.
20. https://compacttool.ru/camera-5-mpix-dlya-raspberry-pi?ysclid=m7aiz70xdw920542036.
21. https://www.researchgate.net/publication/372604327_FPGA-based_Hyperspectral_Lossy_Compressor_with_Adaptive_Distortion_Feature_for_Unexpected_Scenarios#pf3.

REFERENCES

1. *Berni J.A.J., Zarco-Tejada P.J., Suarez L. u Fereres E.* Thermal and Narrowband Multispectral Remote Sensing for Vegetation Monitoring from an Unmanned Aerial Vehicle, *IEEE Transactions on Geoscience and Remote Sensing,* 2009, Vol. 47, pp. 722-738.
2. *Li Z., Liu Y., Walker R., Hayward R. u Zhang J.* Towards automatic power line detection for a UAV surveillance system using pulse coupled neural filter and an improved Hough transform, *Machine Vision and Applications,* 2010, Vol. 21, No. 5, pp. 677-686.
3. *Birk A., Viggerikh B., Byulov Kh., Pfingstorn M. i Shvertfeger S.* Bezopasnost', zashchita i spasatel'nye operatsii s ispol'zovaniem bespilotnykh letatel'nykh apparatov (BPLA) [Security, Defense, and Rescue Operations Using Unmanned Aerial Vehicles (UAVs)], *J. Intel. Robotizirovannye sistemy* [J. Intel. Robotic Systems], 2011, Vol. 64, No. 1, pp. 57-76.
4. *Deniel K. i Vitfel'd K.* Ispol'zovanie infrastruktur obshchedostupnykh setey dlya distantsionnogo zondirovaniya s pomoshch'yu BPLA v grazhdanskikh operatsiyakh po obespecheniyu bezopasnosti [Using public network infrastructures for UAV remote sensing in civil security operations], 2011.
5. *Faial B.S., Freitas H., Gomes P.H., Mano L.Ya., Pessin G., de Karval'yu A.S., Krishnamachari B., Dzh. Ueyama.* Adaptivnyy podkhod k raspyleniyu pestitsidov na osnove bespilotnykh letatel'nykh apparatov v dinamicheskikh sredakh [Adaptive approach to pesticide spraying based on unmanned aerial vehicles in dynamic environments], *Vychisl. Elektron. Agric.* [Calculation. The electron. Agric], 2017, 138 p.
6. Available at: https://docs.yandex.ru/docs/view?tm=1728206370&tld=ru&lang=ru&name=215085.pdf&text.
7. *Pablo Khorstrand, Raal' Gerra, Aytami Rodriges, Mariya Dias, Sebast'yan Lopes, Khoze Fko Lopes.* Platforma BPLA na osnove giperspektral'nogo datchika dlya zakhvata izobrazheniy i bortovoy obrabotki [A UAV platform based on a hyperspectral sensor for image capture and on-board processing]. Available at: https://innoter.com/articles/giperspektralnaya-semka/.
8. *Adaoi T. et al.* Giperspektral'naya s"emka: obzor datchikov na baze BPLA, obrabotki dannykh i prilozheniy dlya sel'skogo i lesnogo khozyaystva [Hyperspectral imaging: An overview of UAV-based sensors, data processing, and applications for agriculture and forestry], *Udalennaya chuvstvitel'nost'* [Remote Sensitivity], 2017, Vol. 9, 11, 1110 p.

9. *Khant-mladshiy E.R. i Dotri K.S.T.* Kakaya pol'za ot bespilotnykh letatel'nykh apparatov dlya distantsionnogo zondirovaniya sel'skogo khozyaystva i tochnogo zemledeliya? [What is the use of unmanned aerial vehicles for remote sensing of agriculture and precision farming?], *Int. J. Remote Sens.,* 2018, Vol. 39, pp. 15-16.
10. *Huang J., Wang H., Dai Q. i Han D.* Analiz dannykh NDVI dlya identifikatsii sel'skokhozyaystvennykh kul'tur i otsenki urozhaynosti [NDVI data analysis for crop identification and yield estimation], *IEEE J. Sel. Temy Prikladnoe nablyudenie za Zemley Distantsionnoe zondirovanie* [IEEE J. Sel. Topics Applied Earth Observation and Remote Sensing], 2014, Vol. 7, pp. 4374-4384.
11. *Rey-Caramés C., Diago M.P., Martín M.P., Lobo A. i Tardaguila J.* Ispol'zovanie mnogospektral'nykh izobrazheniy RPAS dlya kharakteristiki moshchnosti, razvitiya list'ev, komponentov urozhaynosti i izmenchivosti sostava yagod v predelakh vinogradnika [Using multispectral RPAS images to characterize power, leaf development, yield components, and berry composition variability within a vineyard], *Udalennaya chuvstvitel'nost'* [Remote Sensitivity], 2015, Vol. 7, No. 11, pp. 14458-14481. Available at: http://www.mdpi.com/2072-4292/7/11/14458.
12. Giperspektral'nye kamery serii Specim FX1 [Specim FX1 series hyperspectral cameras]. Available: May 4, 2019. Available at: http://www.specim.fi/fx/.
13. Available at: https://sovzond.ru/press-center/articles/bpla/5601/.
14. Available at: https://geon.ru/product/dji-agras-t20-s-4-dop-akb-i-zu- geksakopter/?ysclid=m7aoja559g30884089
15. Available at: https://compacttool.ru/camera-5-mpix-dlya-raspberry-pi?ysclid=m7apxj7qdy527308006.
16. Available at: https://resonon.com/Pika-L.
17. Available at: https://tixer.ru/catalog/raspberrypi/raspberry_pi_3_model_b_v1_2/?ysclid=m7aq4e66hj615743840.
18. *Verevkin A.L., Sirenko E.A. Simvoly* ikh prednaznachenie i napravlenie nauchnogo issledovaniya. Vsemirnyy tekhnologicheskiy universitet YuNESKO. Moskovskiy tekhnologicheskiy institut [Symbols, their purpose and the direction of scientific research UNESCO World Technological University. Moscow Institute of Technology], *Mater. mezhdunarodnogo foruma. Vyp. 1. «Innovatsii v sfere zhiznedeyatel'nosti cheloveka XXI veka»* [Materials of the international forum. Issue 1. "Innovations in the sphere of human activity of the 21st century]. Rostov-on-Don: Gingo, 2015, pp. 249-251.
19. Available at: https://compacttool.ru/camera-5-mpix-dlya-raspberry-pi?ysclid=m7aiz70xdw920542036.
20. Available at: https://compacttool.ru/camera-5-mpix-dlya-raspberry-pi?ysclid=m7aiz70xdw920542036.
21. Available at: https://www.researchgate.net/publication/372604327_FPGA-based_Hyperspectral_Lossy_Compressor_with_Adaptive_Distortion_Feature_for_Unexpected_Scenarios#pf3.

Веревкин Александр Леонидович – Южный федеральный университет; e-mail: verevkin.a@mail.ru; г. Таганрог, Россия; тел. +78634371634; аспирант.

Джозефс Исаак Эхимен – Южный федеральный университет; e-mail: ijosephs@sfedu.ru; г. Таганрог, Россия; тел.: +78634371634; аспирант.

Мисюра Вадим Вадимович – Южный федеральный университет; e-mail: vmisyura@sfedu.ru; г. Таганрог, Россия; тел.: +78634371634; магистрант.

Веревкина Лина Станиславовна – Южный федеральный университет e-mail: lverevkina@sfedu.ru; г. Таганрог, Россия; тел. +78634371634; к.т.н.; доцент.

Verevkin Alexander Leonidovich – Southern Federal University; e-mail: verevkin.a@mail.ru; Taganrog, Russia; phone: +78634371634; postgraduate student.

Josephs Isaac Ehimen – Southern Federal University; e-mail: ijosephs@sfedu.ru; Taganrog, Russia; phone: +78634371634; postgraduate student.

Misyura Vadim Vadimovich – Southern Federal University; e-mail: vmisyura@sfedu.ru; Taganrog, Russia; phone: +78634371634; master's student.

Verevkina Lina Stanislavovna – Southern Federal University e-mail: lverevkina@sfedu.ru; Taganrog, Russia; phone: +78634371634; cand. of eng. sc.; associate professor.

УДК 004.8 DOI 10.18522/2311-3103-2025-3-213-223

Е.С. Подоплелова

ПРОГНОЗИРОВАНИЕ ОТКАЗОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ФАКТОРНОГО АНАЛИЗА

Рассматривается применение метода оценки рисков, основанного на объединении методологии FMEA (failure mode and effect analysis) – анализ рисков и последствий отказа и методов многокритериального принятия решений MCDM (Multiple Criteria Decision Making). Такой подход позволяет учитывать как экспертные знания, так и исторические данные о работе оборудования. Методы MCDM обрабатывают оценку более гибко в сравнении со стандартным способом расчета приоритетного числа риска (ПЧР), что помогает качественнее оценить риски по трем критериям: вероятность возникновения, сложность обнаружения и тяжесть последствий. Один из критериев возможно получить не только через оценку экспертом, но и на основе данных, фиксирующих работу оборудования. На примере синтетических данных из открытого доступа о режимах работы производственного оборудования был опробован данный подход. Задача заключалась в прогнозировании как самого отказа, так и его вида, а также выявлении факторов, сильнее всех оказывающих влияние на отказ. Для этого проводилась предобработка данных, в ходе которой потребовалось устранить дисбаланс классов. Существует несколько подходов к решению этой проблемы, направленные на сокращение преобладающего класса, либо генерацию экземпляров слабо представленных классов. В этом примере использовалось сокращение количества записей не имеющих ошибок случайным образом. Далее, в качестве алгоритмов классификации сравнивались AdaBoost, Random Forest и LinearSVC. Так как требовалась многоклассовая классификация, было решено использовать стратегию «one-vs-the-rest» (один против всех). В итоге удалось добиться точности прогнозирования по F-мере в 86% алгоритмами AdaBoost и Random Forest. LinearSVC оказался неэффективным. Таким образом, полученная модель прогнозирования распознает разные виды ошибок, но существует перспектива к улучшению, для чего требуется более объемная выборка, включающая больше примеров с разными видами отказа. Исходя из этого, такой подход как альтернатива экспертной оценки является перспективным, улучшая объективность, а также давая возможность предвидеть риски и не допустить реального отказа или инцидента, связанного с риском.

Прогнозирование; многоклассовая классификация; машинное обучение; факторный анализ; оценка рисков.

E.S. Podoplelova

FAILURE PREDICTION USING FACTOR ANALYSIS METHODS

This article discusses the application of a risk assessment method based on the combination of the FMEA (failure mode and effect analysis) methodology and the MCDM (Multiple Criteria Decision Making) methods. This approach allows taking into account both expert knowledge and historical data on the operation of the equipment. MCDM methods process the assessment more flexibly in comparison with the standard method of calculating the priority number of risks (PRN), which helps to better assess the risks by three criteria: the probability of occurrence, the complexity of detection and the severity of the consequences. One of the criteria can be obtained not only through an expert assessment, but also on the basis of data recording the operation of the equipment. This approach was tested using the example of synthetic open-source data on the operating modes of production equipment. The task was to predict both the failure itself and its type, as well as to identify the factors that have the greatest impact on the failure. For this purpose, data preprocessing was carried out, during which it was necessary to eliminate the imbalance of classes. There are several approaches to solving this problem, aimed at reducing the dominant class or generating instances of poorly represented classes. In this example, random reduction of the number of records without errors was used. Then, AdaBoost, Random Forest and LinearSVC were compared as classification algorithms. Since multi-class classification was required, it was decided to use the one-vs-the-rest strategy. As a result, it was possible to achieve 86% forecasting accuracy by F-measure using the AdaBoost and Random Forest algorithms. LinearSVC turned out to be ineffective. Thus, the resulting forecasting model recognizes different types of errors, but there is room for improvement, which requires a larger sample, including more examples with different types of failure. Based on this, this approach as an alternative to expert assessment is promising, improving objectivity, and also making it possible to foresee risks and prevent a real failure or risk-related incident.

Forecasting; multi-class classification; machine learning; factor analysis; risk assessment.

Введение. Оценка рисков является неотъемлемой частью управления предприятием, особенно важна и разнообразна оценка на производстве ввиду большого количества оборудования. Всегда существует риск производственных травм, отказов, поломок дорогостоящего оборудования, которые могут привести к более серьезным последствиям. Для повышения безопасности на предприятиях разрабатываются меры по предупреждению негативных событий. Существуют разные подходы и методы к риск менеджменту, один из них – анализ рисков и последствий отказов (FMEA) [1]. Подробно данный подход описывается в ГОСТ Р 51814.2–2001 [2], а идея его модификации путем замены экспертной оценки по критерию «вероятность возникновения» исследована в работе [3].

В данном исследовании рассмотрим применение метода оценки рисков при наличии исторических данных с целью спрогнозировать не только отказ производственного оборудования, но и его вид в зависимости от рабочих параметров.

Анализ исследований. Как говорилось выше, подходы к оценке рисков существуют разные. Например, в работе [4] говорится о системе управления рисками усталости (FRM), которая представляет собой набор методов управления для выявления и управления рисками безопасности, связанных с усталостью. Этот подход учитывает время сна и длительность рабочей смены. Нацелен на постоянную оценку риска и мониторинг состояния рабочих. В этом исследовании рассматривается также эффективность FRM, а также барьеры и факторы в реализации FRM.

Работа [5] посвящена улучшению методики FMEA, где авторы выделяют следующие недостатки:

- сложность выражения и получения оценок;
- неточность в агрегировании оценок;
- и отсутствие взаимосвязей между факторами риска.

Для устранения этих недостатков авторами работы применяется теория нечетких множеств изображений (PFS), что позволяет экспертам выражать оценки более эффективно и получать высокую точность. Для улучшения ими были разработаны следующие шаги:

- для упрощения процесса экспертной оценки создается гибкая система приобретения знаний (FKAF), позволяющая экспертам выражать нечеткую информацию с помощью различных форм нечетких оценок;
- разрабатывается метод нечеткого преобразования изображений (PFC) для стандартизации нечетких значений для изображения нечетких чисел (PFN);
- для повышения точности агрегирования оценок в неопределенных условиях предлагается метод нечеткого доказательного рассуждения (PFER), который расширяет существующие методы нечеткого доказательного рассуждения (FER);
- для описания параллельных и причинно-следственных связей между факторами риска создаются четыре альтернативные модели с использованием нечетких сетей Петри (PFPN). Ранжирование приоритетов рисков определяется путем умозаключений.

Работа [6] также использует в своей основе FMEA, применяя методы глубокого обучения для интеллектуального анализа данных различных аспектов предметной области. На примере прогнозирования ремонта самолета рассматривается четыре области: физический мир, получение данных, кибер-мир и поддержка принятия решений. Авторы пишут об использовании глубокого обучения при наличии достаточного количества записей о работе оборудования, его сбоях и ремонтах, результаты которого можно использовать для прогнозирования возникновения.

Помимо описанных выше, работы [7–9] также описывают анализ рисков по методологии FMEA, используя их при разработке систем поддержки принятия решений в различных сферах. В работах [10, 11] описываются методы прогнозирования рисков в медицинских задачах.

В своем исследовании я использую идею прогнозирования отказа, но на примере синтетических данных о работе производственного оборудования.

Описание задачи и данных. Набор данных состоит из 10 000 строк, имеющих 14 признаков, 5 из которых – вид отказа:

1. UID: уникальный идентификатор в диапазоне от 1 до 10000.
2. Идентификатор продукта.
3. Тип продукта [L, M или H].
4. Температура воздуха [K].
5. Температура процесса [K].
6. Скорость вращения [об/мин].
7. Крутящий момент [Нм].
8. Износ инструмента [мин].
9. Целевая переменная «отказ машины» по любому из режимов.

Отказ машины включает 5 видов ошибок оборудования:

1. Отказ из-за износа комплектующих (TWF).
2. Нарушение отвода тепла (HDF).
3. Сбой мощности (PWF).
4. Перенапряжение (OSF).
5. Случайные ошибки (RNF).

В работе [12] приведено подробное описание этого датасета, для исследования я взяла только необходимую информацию.

Теперь опишем целевую переменную. В данном наборе при одном из вышеперечисленных режимов сбоя стоит единица, процесс завершается отказом, и в параметре «отказ машины» присваивается значение 1.

Исходя из всего вышеперечисленного, можно выделить 5 видов ошибок:

1. Отказ из-за износа.
2. Нарушение отвода тепла.
3. Сбой мощности.
4. Перегрузка.
5. Случайные сбои.

Возникновение каждого вила и будем прогнозировать. Также, добавим прогноз отказа оборудования в целом, по параметру «Machine Failure» (отказ оборудования).

В итоге, переходим к задаче бинарной классификации в случае, когда мы прогнозируем отказ в целом по параметру «отказ оборудования». При загрузке датасета в систему и определенной настройке модель способна спрогнозировать отказ на основании данных об оборудовании еще до его реализации, тем самым предотвратив реализацию угрозы. В контексте типов ошибок мы сводим все к задаче многоклассовой классификации с перекрестными классами (так как возможен вариант реализации нескольких ошибок сразу), чтобы определить, какой вид отказа наиболее вероятен при текущих значениях признаков системы.

Факторный анализ. Для того, чтобы определить наиболее значимые признаки была создана корреляционная матрица для количественных признаков, и по ней отрисована тепловая карта на рис. 1.

Фиксируется сильная корреляция температуры воздуха от температуры процесса, а также обратная связь между скоростью вращения и крутящим моментом. Однако, обычной матрицы корреляции недостаточно, потому используем факторный анализ. Факторный анализ позволяет решить две важные проблемы исследователя: описать объект измерения всесторонне и в то же время компактно. С помощью факторного анализа возможно выявление скрытых переменных факторов, отвечающих за наличие линейных статистических корреляций между наблюдаемыми переменными.

Две основных цели факторного анализа:

- определение взаимосвязей между переменными [13, 14];
- сокращение числа переменных необходимых для описания данных.

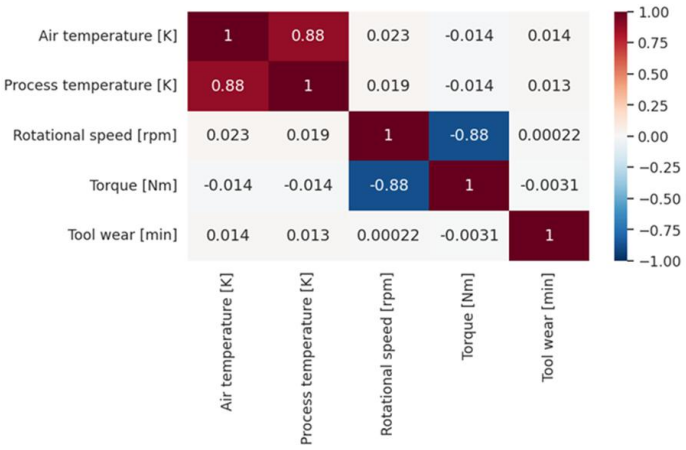


Рис. 1. Тепловая карта

Воспользуемся двумя методами: факторный анализ на основе метода главных компонент (PCA)[15] и метод feature_importances_ [16] в классификаторе Случайного леса библиотеки SckitLearn. На рис. 2 отображено влияние признаков.

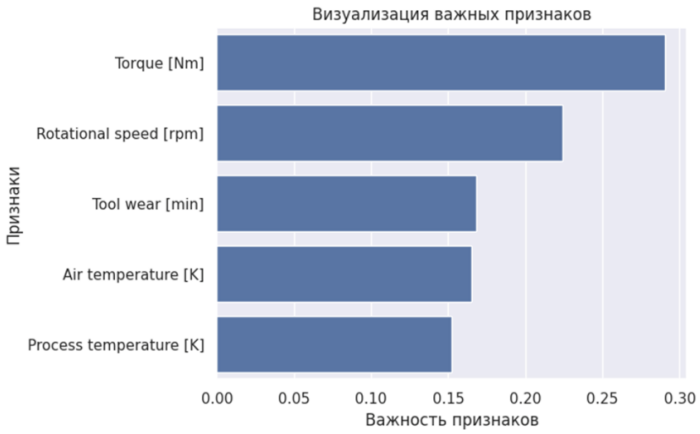


Рис. 2. Результаты влияния признаков методом Случайного леса

Ниже, в табл. 1 представлены результаты факторного анализа методом главных компонент и методом feature importances_.

Таблица 1

Результаты факторного анализа

	feature_importances_	PCA. Фактор 1	PCA. Фактор 2
Крутящий момент	0.290333	-0.693762	-0.628608
Скорость вращения	0.224212	0.705323	0.621208
Износ	0.167999	-0.011478	-0.020076
Температура воздуха	0.165356	0.642	-0.6804
Температура рабочего процесса	0.152099	0.643	-0.6802

Как видим из таблицы, методы показали, что наиболее влиятельными являются крутящий момент и скорость вращения по обоим подходам, факторный анализ методом главных компонент же выделил еще обе температуры, износ был определен самым слабым. Оба метода не противоречат друг другу, а скорее, дополняют.

Предобработка и обучение модели. Для лучшего понимания данных проведем разведочный анализ, чтобы лучше понять закономерности в датасете. На рис. 3 представлена визуализация распределения видов ошибок.

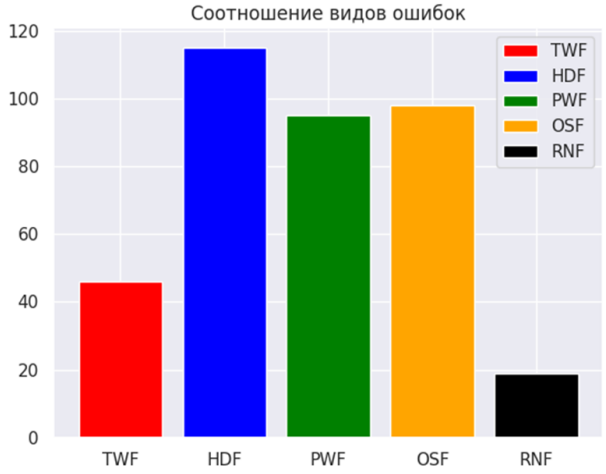


Рис. 3. Распределение видов ошибок

Исходя из этого, можно сделать вывод, что наибольшее количество ошибок более 100 это нарушение обмена тепла (HDF), процент случайных ошибок самый маленький.

Всего отказов в датасете зафиксировано 339 по параметру «Ошибка оборудования». Это меньше, чем ошибок по всем видам суммарно, т. к. есть записи, где возникали сразу две ошибки. В 23 записях ошибок две одновременно, в 1 записи три ошибки - суммарно 0,24% от всех записей или 7% от всех ошибок

Рис. 4 отражает распределение ошибок по качеству.

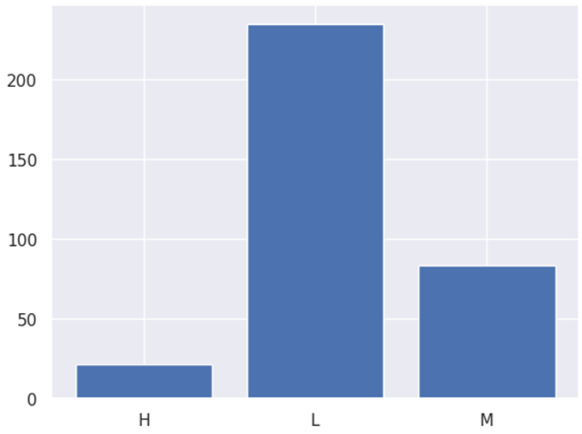


Рис. 4. Распределение ошибок по качеству

Распределение количества ошибок по типу показывает, что набольшей вероятности подвержены детали низкого качества, однако это объясняется еще и тем, что их больше остальных.

Из-за проблемы дисбаланса классов было принято решение сократить количество записей без ошибок, чтобы исключить превосходство одного класса, так как в разрезе определения вида ошибки это значительно влияет на точность. Так как данные генерировались на основе реальных настроек, в случае прогнозирования аномалий всегда будет присутствовать превосходство «рабочих» состояний над «рисковыми». Для многоклассо-

вой классификации были выбраны алгоритмы из библиотеки Scikit-learn: AdaBoost [17, 18] и Random Forest (RF) [19, 20], а также использовалась стратегия «Один против всех» [21, 22]. На рис. 5 представлены матрицы без изменения количества строк в датасете.

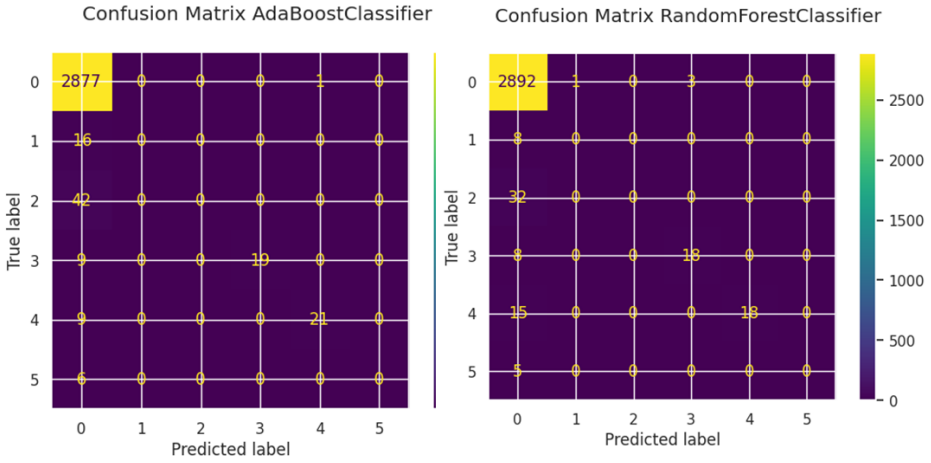


Рис. 5. Матрица ошибок

На рис. 6 приведены подробные описания моделей.

```
Classification report for classifier OneVsRestClassifier(estimator=AdaBoostClassifier(algorithm='SAMME',
                                                       n_estimators=200,
                                                       random_state=45)):
              precision    recall  f1-score   support

           0       0.98      1.00      0.99      2896
           1       0.00      0.00      0.00         8
           2       0.00      0.00      0.00        32
           3       0.87      0.50      0.63        26
           4       0.95      0.58      0.72        33
           5       0.00      0.00      0.00         5

    accuracy                           0.98      3000
   macro avg       0.47      0.35      0.39      3000
weighted avg       0.96      0.98      0.97      3000

Classification report for classifier OneVsRestClassifier(estimator=RandomForestClassifier(random_state=0)):
              precision    recall  f1-score   support

           0       0.98      1.00      0.99      2896
           1       0.00      0.00      0.00         8
           2       0.00      0.00      0.00        32
           3       0.86      0.69      0.77        26
           4       1.00      0.55      0.71        33
           5       0.00      0.00      0.00         5

    accuracy                           0.98      3000
   macro avg       0.47      0.37      0.41      3000
weighted avg       0.96      0.98      0.97      3000
```

Рис. 6. Подробное описание результата применения модели

Как видим, в разрезе классов модель сильно ошибается и не определяет вообще некоторые виды ошибок.

Чтобы улучшить качество, я случайным образом удаляю из датасета ~9200 значений, так как удаляемые всегда выбираются случайно, размер варьируется в пределах 20 строк.

Итоговый датасет содержит ~760 строк, где ошибки занимают около 45% от всего размера. Из-за сокращения наблюдений тестовую выборку сократили до 20%.

Далее, для получения наилучшего результата подберем показатель estimators для алгоритма AdaBoost так, чтобы точность модели на тестовой выборке была наилучшей. В качестве критерия качества я выбрала F1-меру (рис. 7).

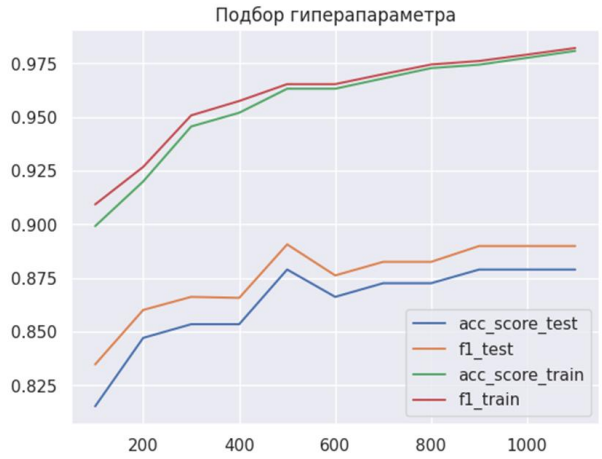


Рис. 7. Подбор гиперпараметров

Наилучшим вариантом оказался n_estimators равный 500. Видим в сравнении с тестовой и тренировочной выборками, что переобучения нет на этом этапе, а полученная точность по accuracy и F1 достигает 88%. Рассмотрим результат в разрезе классов на рис. 8.

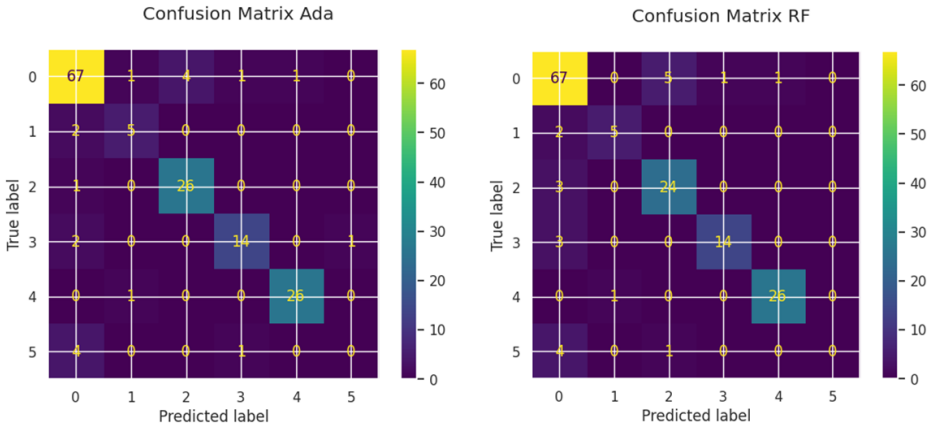


Рис. 8. Матрица ошибок по классам

Как видим, оба алгоритма неплохо справляются с классификациями ошибок, однако не определяется никак последний класс. Это можно объяснить следующим образом:

- количество этого вида очень маленькое;
- сам вид ошибки называется случайным и не маркируется как ошибка оборудования в исходном датасете, потому то, что наша модель этот вид ошибки определяет как ее отсутствие – наилучшее решение. 1-й вид ошибки определяется также не очень стабильно, потому как соответствующих наблюдений этой ошибки меньше всего.

В целом, модель имеет 85–88% точности, что достаточно неплохой показатель с учетом маленькой итоговой выборки. При наличии более качественных данных можно получить точность выше.

Полученная имитационная модель прогнозирования позволит определять вид отказа при входных параметрах оборудования до поломки, что позволит:

- определить диапазоны «рабочих» характеристик оборудования;
- протестировать сценарии и комбинации этих характеристик;
- заблаговременно принимать меры или сигнализировать о рисках.

В методологии указано, что критерий «вероятность возникновения» является относительным, а не абсолютным значением. Эксперт делает оценку на опыте, если не имеется иных указаний и шкал. В данном эксперименте была взята шкала преобразований из ГОСТ Р 51814.2-2001, описывающая соотношение количества возникновений с баллами от 1 до 10.

Итоговая оценка риска. Помимо этого, нам необходимо оценить еще два фактора: сложность обнаружения и тяжесть последствий. Для этого была привлечена экспертная оценка.

В табл. 2 представлен расчёт вероятности возникновения сходя из частоты появления каждого вида ошибки во всех 10000 значениях. Как видим, ранжирование сильно изменилось. Однако, мы здесь не учитываем важность критериев между собой.

Таблица 2

Расчет риска на основе прогноза

Ранг	Наименование ошибки	Вероятность возникновения	Сложность обнаружения	Тяжесть последствий	ПЧР
2	OSF. Отказ из-за перегрузки	5	6	9	270
3	PWF. Сбой мощности	5	6	6	180
1	RNF. Случайные сбои	4	10	7	280
5	HDF. Нарушение отвода тепла	5	1	5	25
4	TWF. Отказ из-за износа	5	3	8	120

Методы машинного обучения помогут обрабатывать и прогнозировать вид отказа методами многоклассовой классификации RandomForest, LinearSVC, AdaBoost, а также выявлять наиболее влияющие признаки методом главных компонент. Сравнение точности прогнозирования ошибок предоставлены в табл. 3.

Таблица 3

Точность прогнозирования разными методами

	LinearSVC	**RandomForestClassifier**	AdaBoost
Accuracy_Score	0.962	0.98175	0.973
F1_weighted	0.98	0.986	0.982
Accuracy_Score_сокращенный	0.53	0.88	0.84
F1_weighted_сокращенный	**0.67**	**0.86**	**0.86**

Как видим, Случайный лес показывает лучшую классификацию на нашей задаче. Это позволит применять систему для оценки рисков с учетом прогнозирования видов отказа.

Таким образом, пользователь получит следующие рекомендации, показанные в табл. 4.

Таблица 4

Итоговые рекомендации для ЛПР

Вид ошибки	Расшифровка	ПЧР Эксперта	ПЧР на основе прогноза
OSF	Отказ из-за перегрузки	1	2
PWF	Сбой мощности	2	3
RNF	Случайные сбои	3	1
HDF	Нарушение отвода тепла	4	5
TWF	Отказ из-за износа	5	4
Степень влияния признаков	Наиболее влиятельными признаками являются скорость вращения и крутящий момент, наименее – степень износа.		

Заключение. На текущем этапе исследования была протестирована часть гибридного подхода оценки рисков, включающая модель прогнозирования видов отказа, а также получение значения по критерию «вероятность возникновения» на основе данных о рабочих характеристиках оборудования и статистики появления. Помимо этого, были получены пояснения для ЛПР о влиянии признаков на возникновения отказа, выявленные при помощи факторного анализа. Для сравнения были использованы два метода: метол главных компонент и встроенный параметр алгоритма Random Forest. Метод главных компонент показал существенную разницу между влиянием признаков (разница в коэффициентах больше, чем у другого метода), потому в дальнейшем использовании в рамках разработки системы поддержки принятия решений планируется использовать именно его.

Результаты прогнозирования алгоритмами RF и AdaBoost показали приемлемые результаты в 85-88% распознавания по классам по F-мере. Если расширить выборку, можно улучшить показатели.

Использование модели прогнозирования для оценке рисков позволит меньше зависеть от эксперта, а в случае отсутствия достаточно квалифицированного эксперта заменить эту оценку, но при этом возникнет потребность в качественных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *McDermott R.E., Mikulak, Raymond J., Beauregard Michael R.* The Basics of FMEA. – Productivity Press, 1996. – 80 p. – ISBN 9780527763206.
2. ГОСТ Р 51814.2–2001. Системы качества в автомобилестроении. Метод анализа видов и последствий потенциальных дефектов.
3. *Подоплелова Е.С., Князев И.И.* Модификация метода FMEA при помощи алгоритмов машинного обучения // Известия ЮФУ. Технические науки. – 2024. – № 6 (2023). – С. 88-95.
4. *Sprajcer M., Matthew J.W. Thomas, Charli Sargent, Meagan E. Crowther, Diane B. Boivin, Imelda S. Wong, Alison Smiley, Drew Dawson*. How effective are Fatigue Risk Management Systems (FRMS)? A review // Accident Analysis & Prevention. – 2022. – No. 165. – P. 106398.
5. *Jin C., Ran Y., Zhang G.* An improving failure mode and effect analysis method for pallet exchange rack risk analysis // Soft Comput. – 2021. – 25. – P. 15221-15241. – https://doi.org/10.1007/s00500-021-06359-z.
6. *Filz M., Langner J.E*., *Herrmann C., Thiede S*. Data-driven failure mode and effect analysis (FMEA) to enhance maintenance planning // Comput. Ind. – 2021. – 129. – 103451.
7. *Aboozar Jamalnia, Yu Gong, Kannan Govindan, Michael Bourlakis, Sachin Kumar Mangla.* A decision support system for selection and risk management of sustainability governance approaches in multi-tier supply chain // International Journal of Production Economics. – 2023. – No. 264. – P. 108960.
8. *Wan Suzila Wan Husin, Yazriwati Yahya, Nurulhuda Firdaus Mohd Azmi, Nilam Nur Amir Sjarif, Suriayati Chuprat, Azri Azmi.* Risk Management Framework for Distributed Software Team: A Case Study of Telecommunication Company // Procedia Computer Science. – 2019. – 161. – P. 178-186.
9. *Nabil K., Dkhissi. P.B.* A decision support system for evaluating the logistical risks in Supply chains based on RPN factors and multi criteria decision making approach // 2022 IEEE 6th International Conference on Logistics Operations Management (GOL). – Strasbourg, France, 2022. – P. 1-6.
10. *Dent T.H.S. et al*. Risk prediction models: a framework for assessment // Public health genomics. – 2012. – Vol. 15 (2). – P. 98-105. – DOI: 10.1159/000334436.

11. *Cai Y., Cai YQ., Tang, LY. Et al.* Artificial intelligence in the risk prediction models of cardiovascular disease and development of an independent validation screening tool: a systematic review // BMC Med. – 2024. – 22. – 56. – https://doi.org/10.1186/s12916-024-03273-7.
12. *Matzka S.* AI4I 2020 Predictive Maintenance Dataset, submitted to UCI Machine Learning Repository. – 2020.
13. *Ким Дж.-О., Мьюллер Ч.У.* Факторный анализ: статистические методы и практические вопросы // Сб. работ «Факторный, дискриминантный и кластерный анализ»: пер. с англ. / под. ред. И.С. Енюкова. – М.: Финансы и статистика, 1989. – 215 с.
14. *Бююль А., Цёфель П.* SPSS: Искусство обработки информации. Анализ статистических данных и восстановление скрытых закономерностей. – СПб.: ООО «ДиаСофтЮП», 2002. – 603 с.
15. *Pearson K.* On lines and planes of closest fit to systems of points in space // Philosophical Magazine. – 1901. – Vol. 2. – P. 559-572.
16. Официальный сайт Scikit-learn. Feature importances with a forest of trees. – URL: https://scikit-learn.org/stable/auto_examples/ensemble/plot_forest_importances.html.
17. *Freund Y., Schapire R.* A Decision-Theoretic Generalization of on-Line Learning and an Application to Boosting. – 1995.
18. *Zhu J., Zou H., Rosset S., Hastie T*. Multi-class adaboost // Statistics and its Interface. – 2009. – Vol. 2. – P. 349-360.
19. *Prinzie A, Poel D*. Random Multiclass Classification: Generalizing Random Forests to Random MNL and Random NB // Database and Expert Systems Applications. Lecture Notes in Computer Science. – 2007. – Vol. 4653. – P. 349. – DOI: 10.1007/978-3-540-74469-6_35. ISBN 978-3-540-74467-2.
20. *Denisko D, Hoffman M.M*. Classification and interaction in random forests // Proceedings of the National Academy of Sciences of the United States of America. – 2018. – 115 (8). – P. 1690-1692. – Bibcode: 2018PNAS..115.1690D. – DOI: 10.1073/pnas.1800256115. PMC 5828645. – PMID 29440440.
21. *Bishop Christopher M*. Pattern Recognition and Machine Learning. – Springer, 2006.
22. Официальный сайт Scikit-learn. User Guide. OneVsRestClassifier. – URL: https://scikit-learn.org/stable/modules/multiclass.html#ovr-classification.

REFERENCES

1. *McDermott R.E., Mikulak, Raymond J., Beauregard Michael R.* The Basics of FMEA. Productivity Press, 1996, 80 p. ISBN 9780527763206.
2. GOST R 51814.2–2001. Sistemy kachestva v avtomobilestroenii. Metod analiza vidov I posledstviy potentsial'nykh defektov [GOST R 51814.2–2001. Quality systems in the automotive industry. Method for analyzing the types and consequences of potential defects].
3. *Podoplelova E.S., Knyazev I.I.* Modifikatsiya metoda FMEA pri pomoshchi algoritmov mashinnogo obucheniya [Modification of the FMEA method using machine learning algorithms], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SfedU. Engineering Sciences], 2024, No. 6 (2023), pp. 88-95.
4. *Sprajcer M., Matthew J.W. Thomas, Charli Sargent, Meagan E. Crowther, Diane B. Boivin, Imelda S. Wong, Alison Smiley, Drew Dawson*. How effective are Fatigue Risk Management Systems (FRMS)? A review, *Accident Analysis & Prevention,* 2022, No. 165, pp. 106398.
5. *Jin C., Ran Y., Zhang G.* An improving failure mode and effect analysis method for pallet exchange rack risk analysis, *Soft Comput,* 2021, 25, pp. 15221-15241. Available at: https://doi.org/10.1007/s00500-021-06359-z.
6. *Filz M., Langner J.E*., *Herrmann C., Thiede S*. Data-driven failure mode and effect analysis (FMEA) to enhance maintenance planning, *Comput. Ind*., 2021, 129, 103451.
7. *Aboozar Jamalnia, Yu Gong, Kannan Govindan, Michael Bourlakis, Sachin Kumar Mangla.* A decision support system for selection and risk management of sustainability governance approaches in multi-tier supply chain, *International Journal of Production Economics,* 2023, No. 264, pp. 108960.
8. *Wan Suzila Wan Husin, Yazriwati Yahya, Nurulhuda Firdaus Mohd Azmi, Nilam Nur Amir Sjarif, Suriayati Chuprat, Azri Azmi.* Risk Management Framework for Distributed Software Team: A Case Study of Telecommunication Company, *Procedia Computer Science,* 2019, 161, pp. 178-186.
9. *Nabil K., Dkhissi. P.B.* A decision support system for evaluating the logistical risks in Supply chains based on RPN factors and multi criteria decision making approach, *2022 IEEE 6th International Conference on Logistics Operations Management (GOL).* Strasbourg, France, 2022, pp. 1-6.
10. *Dent T.H.S. et al*. Risk prediction models: a framework for assessment, *Public health genomics,* 2012, Vol. 15 (2), pp. 98-105. DOI: 10.1159/000334436.

11. *Cai Y., Cai YQ., Tang, LY. et al.* Artificial intelligence in the risk prediction models of cardiovascular disease and development of an independent validation screening tool: a systematic review, *BMC Med.*, 2024, 22, 56. Available at: https://doi.org/10.1186/s12916-024-03273-7.
12. *Matzka S.* AI4I 2020 Predictive Maintenance Dataset, submitted to UCI Machine Learning Repository, 2020.
13. *Kim Dzh.-O., M'yuller Ch.U.* Faktornyy analiz: statisticheskie metody i prakticheskie voprosy [Factor analysis: statistical methods and practical issues], *Sb. rabot «Faktornyy, diskriminantnyy i klasternyy analiz»* [Collection of works "Factor, discriminant and cluster analysis"]: transl. from engl., ed. by I.S. Enyukova. Moscow: Finansy i statistika, 1989, 215 p.
14. *Byuyul' A., Tsefel' P.* SPSS: Iskusstvo obrabotki informatsii. Analiz statisticheskikh dannykh i vosstanovlenie skrytykh zakonomernostey [SPSS: The art of information processing. Analysis of statistical data and reconstruction of hidden patterns]. Saint Petersburg: OOO «DiaSoftYUP», 2002, 603 p.
15. *Pearson K.* On lines and planes of closest fit to systems of points in space, *Philosophical Magazine,* 1901, Vol. 2, pp. 559-572.
16. Scikit-learn. Feature importances with a forest of trees. Available at: https://scikit-learn.org/stable/auto_examples/ensemble/plot_forest_importances.html.
17. *Freund Y., Schapire R.* A Decision-Theoretic Generalization of on-Line Learning and an Application to Boosting, 1995.
18. *Zhu J., Zou H., Rosset S., Hastie T*. Multi-class adaboost, *Statistics and its Interface,* 2009, Vol. 2, pp. 349-360.
19. *Prinzie A, Poel D*. Random Multiclass Classification: Generalizing Random Forests to Random MNL and Random NB, *Database and Expert Systems Applications. Lecture Notes in Computer Science,* 2007, Vol. 4653, pp. 349. DOI: 10.1007/978-3-540-74469-6_35. ISBN 978-3-540-74467-2.
20. *Denisko D, Hoffman M.M*. Classification and interaction in random forests, *Proceedings of the National Academy of Sciences of the United States of America,* 2018, 115 (8), pp. 1690-1692. Bibcode: 2018PNAS..115.1690D. DOI: 10.1073/pnas.1800256115. PMC 5828645. PMID 29440440.
21. *Bishop Christopher M*. Pattern Recognition and Machine Learning. Springer, 2006.
22. Scikit-learn. User Guide. OneVsRestClassifier. Available at: https://scikit-learn.org/stable/modules/multiclass.html#ovr-classification.

Подоплелова Елизавета Сергеевна – Южный федеральный университет; e-mail: chuzhinova@sfedu.ru; г. Таганрог, Россия; тел.: +79525844188; кафедра информационно-аналитических систем безопасности им. Л.С. Берштейна; старший преподаватель.

Podoplelova Elizaveta Sergeevna – Southern Federal University; e-mail: chuzhinova@sfedu.ru; Taganrog, Russia; phone: +79525844188; Department of Information and Analytical Security Systems named after L.S. Bershtein; senior lecturer.

Раздел V. Моделирование и управление рисками

УДК 004.8 DOI 10.18522/2311-3103-2025-3-224-233

А.Н. Целых, В.С. Васильев, Л.А. Целых, Е.С. Подоплелова

ПОСТРОЕНИЕ ТРАЕКТОРИИ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ В ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ ПРИ ОТСУТСТВИИ НАБЛЮДАЕМЫХ ПЕРЕМЕННЫХ

Построение оптимального управления при полном отсутствии данных о динамике системы является актуальной проблемой. В данной статье предлагается решение линейной квадратичной задачи (ЛК) с конечным горизонтом для инвариантной ко времени системы с матрицей динамики графа. В отличие от задачи регулирования, устойчивость и полная управляемость системы не предполагаются. Построение траектории управления контролируется направлением нарастания изменения состояния переменных за малое число шагов, которое определяется условным главным собственным вектором матрицы смежности графовой модели. Решение классического оптимального управления осуществляется в автономном режиме и требует полного знания динамики системы. В условиях отсутствия полного знания динамики системы решение задач оптимального управления системами с неопределенностью, в том числе дискретными линейными системами, вызывают значительный интерес в последние годы. Основным подходом, когда полная информация о системе недоступна, является дизайн оптимального управления, при котором первоначально определяются параметры системы, а затем решается алгебраическое уравнение в двойственном пространстве. Важным отличием от стандартной задачи дискретного управления является то, что модель управления была модифицирована для оценки изменений состояния переменных при управлениях, передаваемых через матрицу динамики. Предложенный алгоритм с использованием графовой матрицы реализует рекуррентные вычисления динамических и сопряженных уравнений, а также метод Пауэлла для решения системы линейных алгебраических уравнений (СЛАУ). Авторами введена новая интерпретация математической конструкции матрицы динамики системы в стандартной задаче дискретного управления на конечном интервале времени, которая может быть использована для проектирования любой управляемой динамической системы с ненаблюдаемыми параметрами.

Стационарная дискретная система; квадратичная функция стоимости; линейная квадратичная задача; графовая матрица динамики.

A.N. Tselykh, V.S. Vasilev, L.A. Tselykh, E.S. Podoplelova

CONSTRUCTION OF AN OPTIMAL CONTROL TRAJECTORY IN AN INTELLIGENT SYSTEM IN THE ABSENCE OF OBSERVABLE VARIABLES

Constructing optimal control in the complete absence of data on the system dynamics is a pressing problem. In this paper, we propose a solution to a finite-horizon linear quadratic problem (LCP) for a time-invariant system with a graph dynamics matrix. Unlike the control problem, stability and complete controllability of the system are not assumed. The construction of the control trajectory is controlled by the direction of increase in the change in the state of variables over a small number of steps, which is determined by the conditional principal eigenvector of the adjacency matrix of the graph model. The solution of classical optimal control is carried out in an autonomous mode and requires complete knowledge of the system dynamics. In the absence of complete knowledge of the system dynamics, solving optimal control problems for systems with uncertainty, including discrete linear systems, has attracted considerable interest in recent years. The main approach when complete information about the system is unavailable is the design of optimal control, in which the system parameters are initially determined, and then an algebraic equation in the dual space is solved. An important difference from the standard discrete control problem is that the control model was modified to estimate changes in the state of variables under controls transmit-

ted through the dynamics matrix. The proposed algorithm using a graph matrix implements recurrent calculations of dynamic and adjoint equations, as well as the Powell method for solving a system of linear algebraic equations (SLAE). The authors introduced a new interpretation of the mathematical construction of the system dynamics matrix in a standard discrete control problem on a finite time interval, which can be used to design any controlled dynamic system with unobservable parameters.

Stationary discrete system; quadratic cost function; linear quadratic problem; graph matrix of dynamics.

Введение. Моделирование динамических систем, как для целей управления, так и для прогнозирования их поведения, широко распространено в науке и технике. Математические формализмы для построения моделей различаются в зависимости от области применения, и различия между ними обусловлены свойствами класса динамических систем, характерных для различных областей.

В этой статье нас интересует исключительно класс неизменяющихся во времени линейных детерминированных динамических систем с дискретным временем и нестохастическими параметрами. Этот класс включает в себя многие задачи, представляющие интерес для таких областей, как логические и графовые модели в искусственном интеллекте (ИИ), процессы последовательного принятия решений в задачах исследования операций (ИО). Рассматривается задача оптимального косвенного управления в моделях сложных систем с ненаблюдаемыми непосредственно параметрами состояний переменных. Такие системы учитывают социальные, экономические, экологические, культурные, политические и технологические факторы и причинно-следственные связи между ними.

Предполагается, что закон поведения управляемого объекта задается матрицей смежности направленного взвешенного знакового графа, который представляет когнитивную причинную модель (КМ) управляемой системы. Системная эффективность узлов, связанная с динамикой модели, в наибольшей степени выражается спектральными свойствами матрицы графа. Здесь мы опираемся на работы [1–9], которые доказывают, что спектральные свойства графовых матриц содержат всю информацию о динамике системы. Как отмечалось в [2], спектральный анализ дает представление о структурных и семантических свойствах, в то время как ориентированные графы обеспечивают естественный формализм моделирования. Тогда, в отсутствие наблюдаемых и измеряемых параметров управляемого объекта в качестве входных и выходных параметров (конечных наблюдений) для косвенного управления могут выступать компоненты главного собственного вектора в спектральном разложении матрицы смежности направленного графа.

В данной статье мы решаем ЛК задачу оптимального управления с конечным горизонтом для дискретной линейной системы, не зависящей от времени, с графовой матрицей динамики, квадратичным критерием стоимости и векторным входом.

Построение оптимальных управляющих воздействий для динамических систем является широко изученной областью теории управления. Существуют два общих метода решения задач оптимального управления – метод Понтрягина и метод динамического программирования, которые соответственно определяют необходимые и достаточные условия оптимальности [10]. Решение классического оптимального управления осуществляется в автономном режиме и требует полного знания динамики системы. В условиях отсутствия полного знания динамики системы решение задач оптимального управления системами с неопределенностью, в том числе дискретными линейными системами, вызывают значительный интерес в последние годы [11]. Однако используемые подходы требуют наличия хотя бы неполного набора данных. Методы оптимального управления в условиях полного отсутствия данных о состоянии переменных ранее предложены не были.

В этом исследовании мы пытаемся восполнить этот пробел для построения оптимального управления в условиях полного отсутствия данных о динамике системы. Основным подходом, когда полная информация о системе недоступна, является дизайн оптимального управления, при котором первоначально определяются параметры системы, а затем решается алгебраическое уравнение в двойственном пространстве. При этом матрица динамики выражает закон поведения управляемого объекта с помощью матрицы смежности, а параметры системы определяются направлением главного собственного вектора матрицы динамики.

Здесь мы представляем новую интерпретацию математической конструкции матрицы системной динамики ($\boldsymbol{A}$) в стандартной проблеме дискретного управления на конечном горизонте [12], которая может быть использована для описания любой управляемой динамической системы с ненаблюдаемыми параметрами. Учитывая дискретность задачи оптимизации, компоненты главного собственного вектора матрицы $\boldsymbol{A}$ интерпретируются, как приращение значения состояния переменных.

Входные значения принимаются, как неизвестные входные данные и определяются направлением главного собственного вектора матрицы динамики. Выходные значения определяются вектором оптимального изменения состояния, как воспроизводимого тренда для изменения состояний узлов модели управляемой системы с использованием метода MAEC, представленного в [13]. Поскольку могут быть измерены только выходные значения управляемой системы, оптимальное управление с обратной связью невозможно, и функции затрат выражаются квадратичными функциями управления.

Целью управления является перевод объекта в предписанное интегральное изменение состояния с максимальным значением критерия качества. Решение задачи является квадратичной по управлению с интегральным ограничением на переменные состояния. Оптимальным решением является распределение квадратичной энергии управляющих воздействий по шагам управления.

В отличие от задачи регулирования устойчивость и полная управляемость системы не предполагаются. При этом интерес представляет направление прироста изменения состояния переменных на коротком горизонте и оптимальное управление, обеспечивающее это направление. Направление определяется условным главным собственным вектором модели, собственное число которого не предполагается находящимся в границах единичного спектрального радиуса.

Наконец, мы приводим необходимые и достаточные условия существования и единственности оптимальных управлений. Теоремы доказывают стационарность функции Гамильтона в пространстве состояний и экстремальность функции Гамильтона в пространстве допустимых управлений для проблемы оптимального управления, то есть доказывается достаточность принципа максимума Понтрягина для рассматриваемой задачи.

Для задачи оптимального управления доказаны стационарность функции Гамильтона в пространстве состояний и ее экстремальность в пространстве допустимых управлений, т. е. достаточные условия оптимальности в форме принципа максимума Понтрягина (ПМП).

1. Описание метода. ***1.1. Постановка задачи.*** В этом разделе мы представляем модель управления, которая касается дискретных нестационарных детерминированных задач динамической оптимизации на конечном горизонте. Задачи динамической оптимизации также известны как задачи оптимального управления.

В настоящем исследовании рассматривается модель управления для системы с ненаблюдаемыми переменными. Специфическим свойством рассматриваемой системы является то, что переменные состояния системы ненаблюдаемы и не могут быть непосредственно измерены. Поэтому для описания поведения системы мы будем использовать относительное изменение этого состояния. С учетом специфического свойства рассматриваемой системы, указанного выше, введем следующие обозначения.

Пусть исследуемая система описывается моделью, представленной конечным графом $G = \langle V, E \rangle$, где V – множество n вершин $\{V_1, V_2, \dots, V_n\}$, $E \subset V \times V$ – множество дуг. Граф определяется матрицей смежности $\boldsymbol{F}^T$, транспонированной к матрице $\boldsymbol{F} = \left(f_{i,j}\right)_{n \times n}$, где $f_{i,j}$, $1 \leq i, j \leq n$ есть веса на дугах матрицы.

Пусть изменение состояния переменных системы есть вектор $\boldsymbol{z}$ и пусть это изменение состояния достигается последовательностью *векторов изменений* $\boldsymbol{x}_k$, $1 \leq k \leq m$ и записывается уравнением (1):

$$\boldsymbol{z} = \boldsymbol{x}_1 + \boldsymbol{x}_2 + \cdots + \boldsymbol{x}_m, \tag{1}$$

где $\boldsymbol{z} \in \mathbb{R}^n$ есть n-мерный и ограниченный вектор изменения состояния переменных системы на конечном горизонте m; $\mathbb{R}^n$ есть n-мерное вещественное Евклидово пространство векторов $\boldsymbol{x} = (x_i)_{i=1}^n$ с нормой $\|\boldsymbol{x}\| = \sqrt{\boldsymbol{x}^T\boldsymbol{x}}$; m есть натуральное число; далее m будет играть роль горизонта планирования или управления и будет фиксированным на всем протяжении. Число шагов предполагается малым $m \sim n$; $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_m$ есть последовательные изменения состояния переменных системы.

Эволюция системы определяется предыдущим вектором изменения состояния вершин (факторов) $\boldsymbol{x}_k$, $1 \le k \le m-1$, передающим эти изменения в систему через матрицу динамики $\boldsymbol{F}$, и прошлым вектором управляющего воздействия $\boldsymbol{u}_k$, $0 \le k \le m-1$. Будущий выход зависит от прошлого управления только через предыдущее состояние. Общее выходное изменение состояния суммирует эффект текущих управляющих воздействий на будущие результаты – подобно памяти системы.

Рассмотрим нашу задачу управления как стандартную проблему дискретного управления [12] с учетом введенных обозначений:

$$\boldsymbol{x}_{k+1} = \boldsymbol{A}_k\boldsymbol{x}_k + \boldsymbol{B}_k\boldsymbol{u}_k,\ 0 \le k \le m-1, \tag{2}$$

где $\boldsymbol{x}_k, \boldsymbol{x}_{k+1} \in R^n$ есть вектор изменений в состояниях переменных системы на шаге k, $1 \le k \le m-1$ and $k+1$, $0 \le k \le m$, соответственно; $\boldsymbol{A}_k = \boldsymbol{A} = \delta\boldsymbol{F}$ есть матрица динамики, независимая от k; $\boldsymbol{u}_k \in R^n$, $0 \le k \le m-1$ есть n-мерный и ограниченный вектор управляющего воздействия на переменные на шаге k на горизонте m, который необходимо спроектировать; $\boldsymbol{B}_k = \boldsymbol{I}$ есть константа, определенная как матрица управления; $\boldsymbol{I}$ – единичная матрица.

Пусть начальное изменение состояния системы определяется только вектором $\boldsymbol{u}_0$и пусть эволюция системы контролируется на горизонте m со значениями k, $1 \le k \le m-1$. Запишем траекторию оптимального управления, обеспечивающую условие (1) ценой минимизации суммы квадратов Евклидовых норм управляющих воздействий, в виде:

$$\|\boldsymbol{u}_0\|^2 + \|\boldsymbol{u}_1\|^2 + \cdots + \|\boldsymbol{u}_{m-1}\|^2 \to min. \tag{3}$$

Тогда задача дискретного оптимального управления с учетом введенных обозначений определяется следующим образом (4):

$$J(\boldsymbol{u},\boldsymbol{x}) := \|\boldsymbol{u}_0\|^2 + \|\boldsymbol{u}_1\|^2 + \cdots + \|\boldsymbol{u}_{m-1}\|^2 \to min, \tag{4}$$

при условии

$$\begin{cases} \boldsymbol{z} = \boldsymbol{x}_1 + \boldsymbol{x}_2 + \cdots + \boldsymbol{x}_m \\ \boldsymbol{x}_{k+1} = \delta\boldsymbol{F}\boldsymbol{x}_k + \boldsymbol{u}_k, 0 \le k \le m-1, \\ \boldsymbol{x}_0 = \boldsymbol{0} \end{cases} \tag{5}$$

где $J(\boldsymbol{u},\boldsymbol{x})$ есть квадратичный целевой функционал стоимости оптимального управления на конечном горизонте; $\boldsymbol{x}_0 = \boldsymbol{0}$ есть начальный вектор изменения состояния *переменных* системы; $\boldsymbol{u}_0$ – начальный вектор управляющего воздействия; δ, $0 < \delta \le 1$ – демпинг фактор для обозначения того факта, что мы ожидаем отклонения от номинала, ввиду субъективности оценки элементов матрицы смежности $\boldsymbol{F}^T$.

Целью оптимального управления является нахождение такой траектории изменения состояния $\boldsymbol{z}$ и управления $\boldsymbol{u}$, при которых $J(\boldsymbol{u},\boldsymbol{x})$ минимизируется на конечном горизонте m. Полная управляемость и устойчивость не предполагается.

Траектория $\{\boldsymbol{x}_{k+1}, \boldsymbol{u}_k | 0 \le k \le m-1\}$ называется *допустимой*, если $\boldsymbol{x}_{k+1}$ и $\boldsymbol{u}_k$ограничены и измеримы на конечном горизонте m и выполнены все ограничения (5) задачи (4). Допустимая траектория называется оптимальной, если среди всех допустимых траекторий она доставляет наименьшее значение функционалу $J(\boldsymbol{u},\boldsymbol{x})$.

Далее докажем теорему, дающую достаточные условия оптимальности ПМП в задаче (4)-(5). Необходимые условия оптимальности ПМП для общего случая доказаны в [14, 15].

1.2. Теорема

Теорема 1. Пусть имеется система управления

$$\boldsymbol{x}_{k+1} = \boldsymbol{u}_k + \delta \boldsymbol{F}\boldsymbol{x}_k,\ 0 \le k \le m-1,\ \boldsymbol{x}_0 = \boldsymbol{0}$$

тогда существует единственное решение $\{\boldsymbol{x}_{k+1}, \boldsymbol{u}_k | 0 \le k \le m-1\}$ *задачи*

$$\|\boldsymbol{u}_0\|^2 + \|\boldsymbol{u}_1\|^2 + \cdots + \|\boldsymbol{u}_{m-1}\|^2 \to min,$$

при условии

$$\boldsymbol{z} = \boldsymbol{x}_1 + \boldsymbol{x}_2 + \cdots + \boldsymbol{x}_m.$$

Доказательство. Запишем стандартную функцию Лагранжа [16] для задачи условной оптимизации (4)–(5):

$$L = -\tfrac{1}{2}\textstyle\sum_{k=0}^{m-1}\|\boldsymbol{u}_k\|^2 + \boldsymbol{v}_1^T(\boldsymbol{u}_0 - \boldsymbol{x}_1) + \sum_{k=2}^{m}\boldsymbol{v}_k^T(\boldsymbol{u}_{k-1} + \delta\boldsymbol{F}\boldsymbol{x}_{k-1} - \boldsymbol{x}_k) - \\ - \boldsymbol{w}^T(\boldsymbol{z} - \textstyle\sum_{k=1}^{m}\boldsymbol{x}_k) \to max, \qquad (6)$$

где вектор $\boldsymbol{v}_k$, $1 \le k \le m$ и вектор $\boldsymbol{w}$ есть векторы множителей Лагранжа.

Необходимые условия максимума имеют следующий вид. Производные функции (6) по компонентам векторов $\boldsymbol{x}_k$, $1 \le k \le m$; $\mathbf{u}_k$, $0 \le k \le m-1$; и $\boldsymbol{v}_k$, $1 \le k \le m$ представляют рекуррентные последовательности:

$$\boldsymbol{w} - \boldsymbol{v}_1 + \delta\boldsymbol{F}^T\boldsymbol{v}_2 = \boldsymbol{0}, \dots, \boldsymbol{w} - \boldsymbol{v}_{m-1} + \delta\boldsymbol{F}^T\boldsymbol{v}_m = \boldsymbol{0}, \boldsymbol{w} - \boldsymbol{v}_m = \boldsymbol{0}, \qquad (7)$$

$$\boldsymbol{v}_1 - \boldsymbol{u}_0 = \boldsymbol{0}, \dots, \boldsymbol{v}_{m-1} - \boldsymbol{u}_{m-2} = \boldsymbol{0}, \boldsymbol{v}_m - \boldsymbol{u}_{m-1} = \boldsymbol{0}, \qquad (8)$$

$$\boldsymbol{u}_0 - \boldsymbol{x}_1 = \boldsymbol{0}, \boldsymbol{u}_1 + \delta\boldsymbol{F}\boldsymbol{x}_1 - \boldsymbol{x}_2 = \boldsymbol{0}, \dots, \boldsymbol{u}_{m-1} + \delta\boldsymbol{F}\boldsymbol{x}_{m-1} - \boldsymbol{x}_m = \boldsymbol{0}. \qquad (9)$$

Уравнения (7) и (8) express выражает стационарность по состоянию и экстремальность по управлению ПМП, соответственно. Подставив (9) $\mathbf{x}$ в (1), мы получим:

$$\boldsymbol{z} = \boldsymbol{x}_1 + \boldsymbol{x}_2 + \cdots + \boldsymbol{x}_m = \boldsymbol{u}_{m-1} + (\boldsymbol{I} + \delta\boldsymbol{F})\boldsymbol{u}_{m-2} + (\boldsymbol{I} + \delta\boldsymbol{F} + (\delta\boldsymbol{F})^2)\boldsymbol{u}_{m-3} + \cdots \\ + (\boldsymbol{I} + \delta\boldsymbol{F} + (\delta\boldsymbol{F})^2 + \cdots + (\delta\boldsymbol{F})^{m-1})\boldsymbol{u}_0. \qquad (10)$$

Подставляя (8) $\mathbf{u}$ в (11), мы получим:

$$\boldsymbol{P}_m\boldsymbol{w} = \boldsymbol{z}, \qquad (11)$$

где $\boldsymbol{P}_m = \boldsymbol{I} + (\boldsymbol{I} + \delta\boldsymbol{F})(\boldsymbol{I} + \delta\boldsymbol{F})^T + \cdots + (\boldsymbol{I} + \delta\boldsymbol{F} + \cdots + (\delta\boldsymbol{F})^{m-1})(\boldsymbol{I} + \delta\boldsymbol{F} + \cdots + (\delta\boldsymbol{F})^{m-1})^T$.

Матрица $\boldsymbol{P}_m$ является положительно определённой, поскольку $\boldsymbol{w}^T\boldsymbol{P}_m\boldsymbol{w} \ge \boldsymbol{w}^T\boldsymbol{w} > \boldsymbol{0}$ для любого ненулевого вектора $\boldsymbol{w} \ne \boldsymbol{0}$. Следовательно, уравнение (12) однозначно разрешимо относительно $\boldsymbol{w}$ при любом $\boldsymbol{z}$. Далее, вектор $\boldsymbol{u}_k$, $m-1 \ge k \ge 0$ и вектор $\boldsymbol{x}_k$, $1 \le k \le m$ вычисляются, используя уравнения (7), (8), и (9), соответственно.

Таким образом, теорема 1 доказана.

1.3. Вычислительный алгоритм. Вычислительный алгоритм решения задачи (4)–(5) использует метод сопряженных направлений [17, 18] для решения СЛАУ с симметричной положительно определенной матрицей $\boldsymbol{P}$ и сводится к трем-шаговым последовательным вычислениям матриц $\boldsymbol{Q}$ и $\boldsymbol{P}$, векторов $\boldsymbol{u}_k$ и векторов $\boldsymbol{x}_k$.

Запишем рекуррентную последовательность для вычисления матрицы $\mathbf{P}_m$:

$$\boldsymbol{P}_1 = \boldsymbol{I},\ \boldsymbol{Q}_1 = \boldsymbol{I},\ \boldsymbol{Q}_k = \boldsymbol{I} + \delta\boldsymbol{F}\boldsymbol{Q}_{k-1}, \boldsymbol{P}_k = \boldsymbol{P}_{k-1} + \boldsymbol{Q}_k\boldsymbol{Q}_k^T, \quad 2 \le k \le m,$$

где n есть число вершин модели, $\boldsymbol{Q}_k$, $1 \le k \le m$ есть вспомогательные матрицы.

Вычислительная сложность матрицы $\boldsymbol{P}_m$ is $O(mn^3)$ операций, поскольку вычисление матрицы $\boldsymbol{P}_m$ требует n^3 операций для умножения двух матриц размерности $n \times n$ по этому полю и m дополнения для вычисления суммы произведений. Выход контролируется вектором изменения состояния с фиксированным концом $\boldsymbol{z}$ на конечном горизонте m. Вектор $\boldsymbol{z}$ вычисляется с использованием алгоритма MAEC, представленного в [13]. Алгоритм MAEC доступен для расчетов по адресу https://github.com/Simon1093/cognition. Выходные данные алгоритма представляют собой последовательность оптимальных управлений $\boldsymbol{u}_k$, $0 \le k \le m-1$ и последовательность изменений состояний $\boldsymbol{x}_k$, $1 \le k \le m$.

Алгоритм, использующий графовую матрицу динамики для решения линейной квадратичной задачи, обобщен в табл. 1. Алгоритм реализует рекуррентные вычисления уравнений динамики и сопряженных уравнений, а также метод сопряженных направлений для решения СЛАУ (12).

Таблица 1

Алгоритм, использующий графовую матрицу динамики

Input: $\mathbf{F}$, δ, $\mathbf{z}$, m;
$\mathbf{P} \leftarrow \mathbf{I}$; $\mathbf{Q} \leftarrow \mathbf{I}$;
for $k = 2$ to m do
$\mathbf{Q} \leftarrow \mathbf{I} + \delta\mathbf{FQ}$; $\mathbf{P} \leftarrow \mathbf{P} + \mathbf{QQ}^T$;
endfor;
$\mathbf{w} \leftarrow \mathbf{P}^{-1}\mathbf{z}$;
$\mathbf{u}_{m-1} \leftarrow \mathbf{w}$;
for $k = m-2$ downto 0 do
$\mathbf{u}_k \leftarrow \mathbf{w} + \delta\mathbf{F}^T\mathbf{u}_{k+1}$;
endfor;
$\mathbf{x}_1 \leftarrow \mathbf{u}_0$;
for $k = 2$ to m do
$\mathbf{x}_k \leftarrow \mathbf{u}_{k-1} + \delta\mathbf{F}\mathbf{x}_{k-1}$;
endfor;
Output: $\mathbf{u}_k$, $0 \le k \le m-1$; $\mathbf{x}_k$, $1 \le k \le m$.

2. Результаты моделирования. В этом разделе для моделирования предлагаемого метода, в уравнении (2) используется графовая матрица смежности $\boldsymbol{A_k} = \boldsymbol{A} = \delta\boldsymbol{F}$ (12), выражающая поведенческую модель системы «Преступление и наказание»:

$$\begin{pmatrix} 0 & 0.5 & 0.5 & 0 & 0.6 & 0 \\ 0 & 0 & 0.7 & 0 & 0 & 0 \\ 0 & -0.5 & 0 & 0.5 & 0 & 0.6 \\ 0 & 0 & -0.4 & 0 & 0.4 & 0.6 \\ 0 & 0 & 0.3 & 0 & 0 & 0 \\ 0.3 & 0 & 0 & -0.8 & 0 & 0 \\ 0.5 & 0 & -0.8 & 0 & 0 & 0 \end{pmatrix}. \quad (12)$$

Для моделирования оптимального управления предполагаются следующие исходные данные:

1. Матрица динамики $\boldsymbol{A_k} = \boldsymbol{A} = \delta\boldsymbol{F}$ (12) of dimension $n = 7$.
2. Значение демпинг фактора определяется с учетом теоремы из [17, 18]. Резонансная граница есть $\frac{\delta_{resonance=1}}{\lambda_{max\frac{1}{0.6024492=}}}$; тогда, δ=1.0.
3. $m = 10$ есть горизонт управления.

Выходные значения управляются вектором изменения состояния $\mathbf{z}$ на конечном горизонте $\mathrm{m} = 10$. был рассчитан с использованием алгоритма MAEC, представленного в [13]. Алгоритм MAEC доступен для расчета по адресу https://github.com/Simon1093/cognition . Вычисленные компоненты вектора $\mathbf{z}$ даны ниже:

$$\boldsymbol{z} = (0.610844 \quad 0.317196 \quad 0.283766 \quad 0.250364 \quad 0.367809 \quad 0.137910 \quad 0.478274)^T.$$

Результаты моделирования с использованием предложенного алгоритма следующие.

Оптимальным решением является распределение квадратичной энергии (стоимости) управлений по шагам. Рис. 1,а показывает, что квадратичная энергия управления в последовательностях норм векторов управлений $\mathbf{u}_1$ для разных горизонтов m резко уменьшается на последних шагах. Как показано на рис. 1,б, распределение значений норм векторов переменных отклика по шагам управления описывается полиномом второй степени, что характеризует динамику с равномерными приростами, положительными для одной ветви параболы и отрицательными для другой.

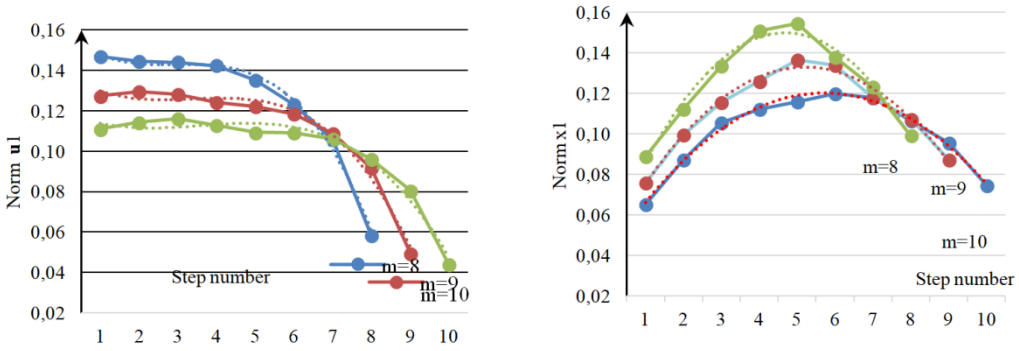


Рис. 1. Распределение нормы переменной управления $\mathbf{u}_1$ (a) и нормы переменной отклика $\mathbf{x}_1$ (b) на шагах управления m. Пояснение: линия тренда обозначена пунктиром; оптимальная траектория управления обозначена сплошной линией

Полученные последовательности управления оцениваются с использованием эффективности управления по базовому вектору управления (уравнение (15)) и эффективности управления по вектору отклика (уравнение (16)). Соответствующие определения приведены ниже.

Определение 1. *Эффективность управления по базовому вектору управления (CE_b) – есть соотношение многоступенчатого и одноступенчатого управлений*:

$$CE_b = \frac{\|\boldsymbol{u}_0+\boldsymbol{u}_1+\cdots+\boldsymbol{u}_{m-1}\|}{\|\boldsymbol{u}_k\|}, 0 \le k \le m-1, \quad (15)$$

где вектор $\|\boldsymbol{u}_k\|$ есть базовый вектор одноступенчатого управления, а вектор $\|\boldsymbol{u}_0+\boldsymbol{u}_1+\cdots+\boldsymbol{u}_{m-1}\|$ есть оцениваемый вектор многоступенчатого управления.

Определение 2. *Эффективность управления по вектору отклика (CE_r) – есть соотношение управление-отклик многоступенчатого управления*:

$$CE_r = \frac{\|\boldsymbol{u}_0+\boldsymbol{u}_1+\cdots+\boldsymbol{u}_{m-1}\|}{\|\boldsymbol{x}_0+\boldsymbol{x}_1+\cdots+\boldsymbol{x}_m\|}, 0 \le k \le m, \quad (16)$$

где вектор $\|\boldsymbol{u}_0+\boldsymbol{u}_1+\cdots+\boldsymbol{u}_{m-1}\|$ есть – соответствующий вектор отклика, а вектор $\|\boldsymbol{x}_0+\boldsymbol{x}_1+\cdots+\boldsymbol{x}_m\|$ есть оцениваемый вектор управления.

Как показано на рис. 2, CE_b стремится к единице, что означает приближение последовательности векторов многоступенчатого управления к оптимальному вектору многоступенчатого управления с увеличения количества шагов управления. В то же время, соотношение управление – отклик стремится к значению CE_r для одноступенчатого управления рассматриваемой модели, $CE_r = 1/\sqrt{\|\mathbf{u}_{k-1}\|/\|\mathbf{x}_k\|} \to 1/\sqrt{5.003556} = 0,447055$.

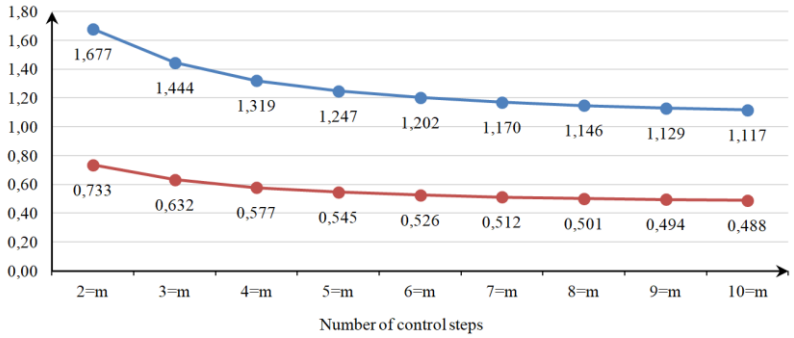


Рис. 2. Эффективность управления по базовому вектору управления и вектору отклика на шагах управления m

Траектории изменения состояний управляемой системы для разных горизонтов по предложенному алгоритму показаны на рис. 3.

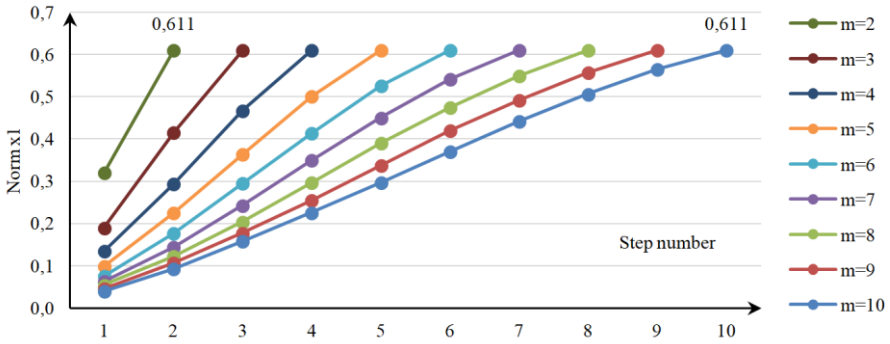


Рис. 3. Траектории изменения состояний $\boldsymbol{x}_1$ в зависимости от горизонта управления m

3. Анализ полученных результатов. Алгоритм, использующий графовую матрицу динамики, оценивался по нескольким параметрам и критериям оценки.

3.1. Время выполнения. На одном ядре процессора Intel Pentium время выполнения 4417U с частотой 2,3 ГГц обычно находится в диапазоне от нескольких микросекунд до нескольких миллисекунд для матриц размером до $n = 10^2$.

3.2. Устойчивость. Вычислительный процесс сводится к решению СЛАУ с положительно определенной матрицей, имеющей единственное решение. После решения СЛАУ двойственные и исходные переменные определяются в результате одной последовательности вычислений. Вычисление положительно определенной матрицы требует $O(mn^3)$ вычислительных затрат. Решение СЛАУ методом Пауэлла имеет сложность $O(n^3)$.

3.3. Надежность результатов. Надежность результатов основана на корректности математической постановки задачи, симметричной положительно определенной матрице СЛАУ, однократной последовательности вычислений, и малым горизонтом управления m.

3.4. Ограничения. Поскольку не требуются устойчивость и полная управляемость системы управления, то число шагов не может быть большим. Число шагов сравнимо с числом узлов и может составлять один или несколько десятков. Число узлов также составляет $n \sim 10^2$.

3.5. Качество результатов. Симметричная положительно определенная матрица СЛАУ определяется рекуррентной последовательностью вычислений, поддерживающей ее симметрию. Это обеспечивает минимальное накопление ошибок округления вычислений с плавающей точкой. Коэффициент совпадения траектории многоступенчатого управления с траекторией одноступенчатого управления находится в пределах 0,982863 – 0,999861.

Заключение. Мы представили оригинальный подход для решения линейной квадратичной задачи с конечным горизонтом для инвариантной во времени системы с дискретным временем и графовой матрицей динамики. Этот подход обеспечивает последовательность управления, которая минимизирует квадратичную функцию стоимости на векторном входе и векторном выходе.

Входной вектор генерируется алгоритмом из [13] в виде компонент главного собственного вектора матрицы динамики, являющейся матрицей смежности направленного графа. Этот граф представляет когнитивную причинную модель системы. Валидность генерируемых данных установлена в работах [13, 17].

Численный эксперимент показал, что алгоритм можно использовать для проектирования траектории управлений по изменению состояния управляемой системы для перевода ее в заданное направление развития. Это направление выражается условным главным собственным вектором графовой модели.

Важным отличием от стандартной проблемы дискретного управления [19, 20] является то, что модель управления интерпретирована таким образом, что оценивается изменение состояния переменных под действием управляющих воздействий, передающихся через матрицу динамики.

Важным преимуществом предложенного подхода является то, что траектория дискретного управления эффективно следует направлению условного главного собственного вектора матрицы динамики с фиксированной конечной точкой с точностью до 10^{-6} и суммарным отклонением вдоль траектории не более 1,714%. Для рассматриваемых систем получены достаточные условия в виде принципа максимума (Теорема 1).

Исследование выполнено за счет гранта Российского научного фонда № 25-21-00029, https://rscf.ru/project/25-21-00029/ в Южном федеральном университете.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *de Aguiar M.A.M., Bar-Yam Y.* Spectral analysis and the dynamic response of complex networks, *Phys. Rev. E,* 2005, 71, 016106. Available at: https://doi.org/10.1103/PhysRevE.71.016106.
2. *Butterworth J., Dunne P.E*. Spectral Techniques in Argumentation Framework Analysis, *Computational Models of Argumen*t, 2016, pp. 167-178. Available at: https://doi.org/10.3233/978-1-61499-686-6-167.
3. *Gadiyaram V., Ghosh S., Vishveshwara S.* A graph spectral-based scoring scheme for network comparison, *J. Complex Networks,* cnw016, 2016. Available at: https://doi.org/10.1093/comnet/cnw016.
4. *Pei S., Wang J., Morone F., Makse H.A*. Influencer identification in dynamical complex systems, *J. Complex Networks,* 2019. Available at: https://doi.org/10.1093/comnet/cnz029.
5. *Ritter F.E., Shadbolt N.R., Elliman D., Young R.M., Gobet F., Baxter G.D.* Techniques for Modeling Human Performance in Synthetic Environments: A Supplementary Review, 2003. Available at: https://doi.org/10.21236/ADA487721.
6. *Gray W.D. ed.* Integrated Models of Cognitive Systems. Oxford University Press, 2007. Available at: https://doi.org/10.1093/acprof:oso/9780195189193.001.0001.
7. *Langley P., Laird J.E., Rogers S.* Cognitive architectures: Research issues and challenges, *Cogn. Syst. Res*., 2009, 10, pp. 141-160. Available at: https://doi.org/10.1016/j.cogsys.2006.07.004.
8. *Kotseruba I., Tsotsos J.K*. 40 years of cognitive architectures: core cognitive abilities and practical applications, *Artif. Intell. Rev*., 2020, 53, pp. 17-94. Available at: https://doi.org/10.1007/s10462-018-9646-y.
9. *Sgaier S.K., Huang V., Charles G.* The Case for Causal AI, *Stanford Soc. Innov. Rev*., 2020, 18 (3), pp. 50-55. Available at: https://doi.org/10.48558/KT81-SN73.
10. *Razavi S.E., Moradi M.A., Shamaghdari S., Menhaj M.*B. Adaptive optimal control of unknown discrete-time linear systems with guaranteed prescribed degree of stability using reinforcement learning, *Int. J. Dyn. Control,* 2022, 10, pp. 870-878. Available at: https://doi.org/10.1007/s40435-021-00836-x.
11. *Moulton R.H., Rudie K.* Online control of discrete-event systems: A survey, *Annu. Rev. Control,* 2022, 54, pp. 24-48. Available at: https://doi.org/10.1016/j.arcontrol.2022.08.002.
12. *Katsuhiko O*. Discrete-time control systems. Prentice-Hall, Inc., USA, 1995.
13. *Tselykh A., Vasilev V., Tselykh L.* A Method for Modeling the Control Impact Strategy Based on the Mental Frame of References of the Decision-Maker. Presented at the 2023. Available at: https://doi.org/10.1007/978-3-031-43789-2_29.
14. *Pontryagin L.S.* Mathematical Theory of Optimal Processes. Routledge, 2018. Available at: https://doi.org/10.1201/9780203749319.
15. *Macki J., Strauss A*. Necessary Conditions for Optimal Controls — The Pontryagin Maximum Principle. Presented at the 1982. Available at: https://doi.org/10.1007/978-1-4612-5671-7_5.
16. *Bertsekas D.P.* Constrained Optimization and Lagrange Multiplier Methods. Athena Scientifi, Belmont, MA, 1996.
17. *Tselykh A., Vasilev V., Tselykh L., Ferreira F.A.F*. Influence control method on directed weighted signed graphs with deterministic causality, *Ann. Oper. Res*., 2022, 311, pp. 1281-1305. Available at: https://doi.org/10.1007/s10479-020-03587-8.
18. *Tselykh A., Vasilev V., Tselykh L*. Effect of Resonance in the Effective Control Model Based on the Spread of Influence on Directed Weighted Signed Graphs, *Advances in Intelligent Systems and Computting,* 2020, pp. 270-280. Available at: https://doi.org/10.1007/978-3-030-50097-9_28.
19. *Powell M.J.D.* An efficient method for finding the minimum of a function of several variables without calculating derivatives, *Comput. J.,* 1964, 7, pp. 155-162. Available at: https://doi.org/10.1093/comjnl/7.2.155.
20. *Carvalho J.P.* On the semantics and the use of fuzzy cognitive maps and dynamic cognitive maps in social sciences, *Fuzzy Sets Syst.*, 2013, 214, pp. 6-19. Available at: https://doi.org/10.1016/j.fss.2011.12.009.

Целых Александр Николаевич – Южный федеральный университет; e-mail: ant@sfedu.ru; г. Таганрог, Россия; тел.: +79185562047; кафедра ИАСБ; д.т.н.; зав. кафедрой.

Васильев Владислав Сергеевич – Южный федеральный университет; e-mail: vsvasilev@sfedu.ru; г. Таганрог, Россия; тел.: +79185983647; кафедра ИАСБ; к.ф.-м.н.; доцент.

Целых Лариса Анатольевна – Южный федеральный университет; e-mail: l.tselykh58@gmail.com; г. Таганрог, Россия; тел.: +79185562047; кафедра ИАСБ; к.э.н.; доцент.

Подоплелова Елизавета Сергеевна – Южный федеральный университет; e-mail: chuzhinova@sfedu.ru; г. Таганрог, Россия; тел.: +79525844188; кафедра ИАСБ; старший преподаватель.

Tselykh Alexander Nikolayevich – Southern Federal University; e-mail: ant@sfedu.ru; Taganrog, Russia; phone: +79185562047; the department IASB; dr. of eng. sc.; head of department.

Vasilev Vladislav Sergeevich – Southern Federal University; e-mail: vsvasilev@sfedu.ru; Taganrog, Russia; phone: +79185983647; the department IASB; cand. of phys. and math. sc.; associate professor.

Tselykh Larisa Anatolievna – Southern Federal University; e-mail: l.tselykh58@gmail.com; Taganrog, Russia; phone: +79185562047; the department IASB; cand. of ec. sc.; associate professor.

Podoplelova Elizaveta Sergeevna – Southern Federal University»; e-mail: chuzhinova@sfedu.ru; Taganrog, Russia; phone: +79525844188; the department IASB; senior lecturer.

УДК 004.056 DOI 10.18522/2311-3103-2025-3-233-245

А.В. Иванов, А.В. Царегородцев, М.В. Валеев

ТЕХНОЛОГИЧЕСКОЕ РЕШЕНИЕ ПО ФОРМИРОВАНИЮ ИНФРАСТРУКТУРЫ ДОВЕРИЯ В СИСТЕМЕ ЗАЩИЩЕННОСТИ ЦИФРОВОГО РУБЛЯ

Актуальность статьи обусловлена цифровой трансформацией российской экономики, важнейшим направлением которой является разработка и внедрение инструментов цифрового рубля в кредитно-финансовой сфере. В этой связи национальная система должна базироваться на информационно-технологической инфраструктуре доверия в системе защищенности цифрового рубля. Основными функциональными свойствами подобной инфраструктуры доверия относятся механизмы идентификация и аутентификация, безопасных финансовых транзакций на основе защиты целостности и конфиденциальности данных участников и пользователей платформы цифрового рубля. Кроме технологической готовности инфраструктуры доверия необходимо формирование доверия населения к цифровому рублю. Вышеназванные обстоятельства обусловили важность и необходимость разработки технологического решения по формированию инфраструктуры доверия в системе защищенности цифрового рубля. В процессе исследования решены следующие задачи: проведена теоретическая интерпретация и эмпирическая операционализация базовых понятий инфраструктуры доверия цифрового рубля; исследованы ее организационно-технологические предпосылки; уточнены структурные элементы базовой и ролевой модели инфраструктуры цифрового рубля; проведён анализ методов шифрования и токенизации API, а также сформулировано технологическое решение по обеспечению защищенности инфраструктуры доверия цифрового рубля. По результатам исследования предложен комплекс мер направленных на безопасность допуска к платформе цифрового рубля участников и пользователей по защищённым каналам; безопасность допуска кредитных организаций на основе двухфакторной аутентификации, а также безопасность конфиденциальности физических и юридических лиц на инфраструктуре доверия в системе защищенности цифрового рубля. Практическое значение имеет перечень работ, связанных с развёртыванием Удостоверяющих центров, средств защиты информации и СКЗИ, интеграцией с единой системой идентификации и аутентификации информационного и системой быстрых платежей и их внедрением в общей системе цифрового рубля.

Цифровой рубль; инфраструктура доверия; защищенность системы цифрового рубля; инфраструктура доверия в системе цифрового рубля; удостоверяющие центры; шифрование; кредитные организации; сертификаты; платформа цифрового рубля.

A.V. Ivanov, A.V. Tsaregorodtsev, M.V. Valeev

TECHNOLOGICAL SOLUTION FOR FORMING A TRUST INFRASTRUCTURE IN THE DIGITAL RUBLE SECURITY SYSTEM

The relevance of the article is due to the digital transformation of the Russian economy, the most important direction of which is the development and implementation of digital ruble instruments in the credit and financial sector. In this regard, the national system should be based on the information technology infrastructure of trust in the digital ruble security system. The main functional properties of such a trust infrastructure include identification and authentication mechanisms, secure financial transactions based on protecting the integrity and confidentiality of data of participants and users of the digital ruble platform. In addition to the technological readiness of the trust infrastructure, it is necessary to build public trust in the digital ruble. The above circumstances determined the importance and necessity of developing a technological solution for the formation of a trust infrastructure in the digital ruble security system. In the course of the study, the following tasks were solved: a theoretical interpretation and empirical operationalization of the basic concepts of the digital ruble trust infrastructure were carried out; its organizational and technological prerequisites were investigated; the structural elements of the basic and role models of the digital ruble infrastructure were clarified; the analysis of encryption and tokenization methods of API was carried out, and a technological solution was formulated to ensure the security of the digital ruble trust infrastructure. Based on the results of the study, a set of measures aimed at the security of access to the digital ruble platform for participants and users via secure channels is proposed; the security of access for credit institutions based on two-factor authentication, as well as the security of the privacy of individuals and legal entities on the trust infrastructure in the digital ruble security system. Of practical importance is the list of works related to the deployment of Certification Authorities, information security tools and cryptographic information protection tools, integration with a unified information identification and authentication system and a fast payment system and their implementation in the general digital ruble system.

Digital ruble; trust infrastructure; security of the digital ruble system; trust infrastructure in the digital ruble system; certification authorities; encryption; credit institutions; certificates; digital ruble platform.

Введение. Актуальность исследования процессов формирования инфраструктуры доверия в системе защищенности цифрового рубля обусловлена необходимостью научного (теоретическая интерпретация) и технологического (технологическая операционализация) определения таких понятий как: «цифровой рубль», «инфраструктура доверия», «защищенность цифрового рубля», а также формирования инфраструктуры доверия в системе цифрового рубля. Цифровой рубль (ЦР) – форма денег наряду с наличными и безналичными рублями, которую выпускает Банк России в виде цифрового кода (токена), который хранится в цифровых кошельках на его платформе. С помощью цифрового рубля можно платить за товары и услуги, а также осуществлять его перевод другим лицам. Особенности цифрового рубля «нельзя открыть вклад или получить кредит, можно создавать один цифровой кошелёк в любом удобном банке, пополнять его и снимать средства, отсутствие комиссий для граждан **(**для компаний она составит 0,3%) [1, 2]. Понятие «инфраструктура доверия» включает как технологические (методы, средства, технологии), так и регуляторные (законы, стандарты, нормы, правила, стандарты) меры по формированию инфраструктурной среды в которой его участники могут взаимодействовать на основе доверительных отношений. В общем плане можно утверждать, что инфраструктура доверия подразумевается нами как многоуровневая система, обеспечивающая доверие на основе сочетания технологических (технических) решений, правовых норм и механизмов функционирования технических систем. Понятие «защищенность цифрового рубля» понимается как комплекс мероприятий, связанных с конфиденциальностью и целостностью информации, а также организацией доступа, защитой персональных данных (платежей, транзакций), идентификацией пользователей по защите от несанкционированных действий в системе цифрового рубля. Поэтому построение многоуровневой системы защищенности, надёжности и безопасности будет способствовать формированию доверия к системе цифрового рубля.

Основная часть. Для анализа формирования инфраструктуры доверия в системе защищенности цифрового рубля важен научный подход по изучению предмета исследования. Например, ряд ученных акцентируют внимание на проблемах и перспективах

обеспечения безопасности цифрового рубля, основанной на «применении криптографических методов шифрования данных, подписей электронных транзакций и мультифакторной аутентификации, а также анализе преимуществ использования гражданами и бизнесом цифрового рубля» [3, 4]. В отдельных работах рассматривает связь между моделями доверия и архитектурой инфраструктуры открытых ключей, которая для криптографических преобразований использует ключевую пару: секретный ключ и открытый ключ. В этой связи рассматриваются две модели использования ключевых пар и сертификатов: децентрализованная модель сетей доверия, создаваемых на основе соглашений доверия удостоверяющих центров (УЦ), не прошедших аккредитацию; модель квалифицированного единого пространства доверия, в основу которой положена система аккредитованных УЦ и развёрнутая на их базе инфраструктуры открытых ключей (ИОК). В системе удостоверяющих центров традиционно принято классифицировать УЦ по доверительным признакам, например, удостоверяющие центры, которым по умолчанию доверяет все пользователи системы (корневые центры сертификации) и удостоверяющие центры, которым доверяют сами владельцы сертификатов, в связи с чем они формирую свои домены доверия (доверенные центры сертификации). Если бы утеряно доверие к исходному значению корневого центра сертификации, то и автоматически теряется доверие ко всем последующим звеньям цепочки сертификации.

Выделяются различные модели доверия, такие как: иерархическая, браузерная, сетевая и кросс-сертификационные модели доверия [5].

Мельников Д. А. на основе математического аппарата субъективной логики криптографических средств защиты информации в инфраструктуре открытых ключей предлагает «объединить все существующие удостоверяющие центры инфраструктуры открытых ключей в единую инфраструктуру открытых ключей Российской Федерации, а также сформировать технологическую основу доверия для различных прикладных автоматизированных информационно-технологических систем» [6]. Отдельные работы посвящены исследованию доверия при безопасной разработке программного обеспечения. «Безопасная разработка программного обеспечения является основой доверия к информационно-коммуникационным технологиям в условиях современных киберугроз на объектах критической информационной инфраструктуры [7].

Важное значение имеют практические рекомендации по формированию инфраструктуры доверия в системе цифрового рубля. Основными элементами такой модели являются: «репозитарий «движения» (активных) цифровых рублей (ЦР), которые выпущены Центральным Банком Российской Федерации (ЦБ); корневой удостоверяющий центр ЦБ; территориальные удостоверяющие центры (УЦ) ЦБ РФ; головной центр подтверждения подлинности ЦР и платёжных операций, принадлежащий ЦБ РФ; территориальные центры подтверждения подлинности ЦР и платёжных операций, принадлежащие ЦБ РФ, принадлежащие банкам; центры подтверждения подлинности ЦР и платёжных операций, принадлежащие банкам, обслуживающим организации (например, Интернет-магазины), которые принимают ЦР в качестве оплаты товаров и услуг; удостоверяющие центры банков, образующие второй уровень иерархии УЦ в ИОК ЦБ РФ; аккредитованные ЦБ РФ организации-продавцы (Интернет-магазины), которые принимают ЦР в качестве оплаты товаров и услуг, и которые подключены к территориальным центрам проверки подлинности ЦР соответствующих КФО (банков); физические и юридические лица, которые являются владельцами ЦР на основании соответствующих договоров с КФО (банками), аккредитованными ЦБ РФ и функционально-процедурная модель оплаты приобретённых товаров с помощью ЦР [8]» (рис. 1).

Для оценки состояния защищенности СЦР прикладное значение имеет исследование организационно – технологических предпосылок, включающие две группы: организационные (нормативные) и технологические (инфраструктурные), которые в целом способствовали формированию инфраструктуры доверия СЦР. Например, в ходе апробации пилотного проекта цифрового рубля (2022 г.) вводится понятие «платформа цифрового рубля» (далее ПЦР), предусматривающее [9]:

- ♦ организацию доступа пользователей к ПЦР;
- ♦ организацию доступа кредитной организации к ПЦР;

- организацию защиты данных на ПЦР;
- организацию защиты информационной безопасности;
- организацию защиты прав потребителей.

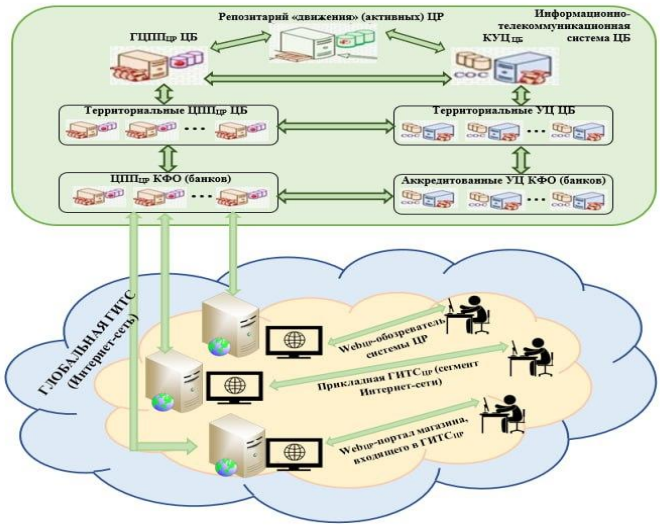


Рис. 1. Модель общей иерархической структуры инфраструктуры доверия Банка России [8]

Количественные характеристики соотношения наличных, безналичных и цифровых рублей представлено на рис. 2.

Рис. 2. Соотношение наличных, безналичных и цифровых рублей [Официальный сайт Банка России]

Организацию работ по противодействию финансовому мошенничеству среди различных категорий населения и формирования их доверия к системе цифрового рубля. Например, по результатам ежегодного опроса Банк России составил портрет пострадавшего от кибермошенников. В 2023 году 4 из 10 респондентов сталкивались с разными видами финансового мошенничества, при этом 10% лишились денег. Количество людей, которым звонили или писали злоумышленники, увеличилось. Например, чаще всего попадаются на уловки мошенников – это люди в возрасте от 25 лет до 64 лет, так как экономически более активны и часто пользуются банковскими онлайн-сервисами (рис. 3).

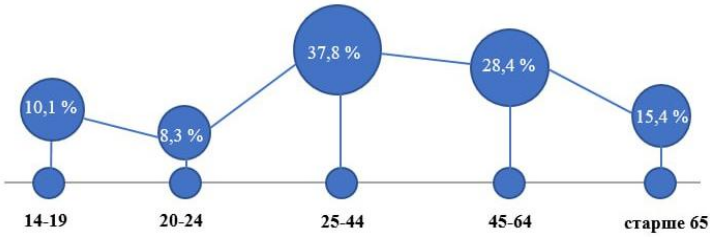


Рис. 3. Портрет пострадавших от кибермошенников по возрасту [https://cbr.ru/statistics/information_security/cyber_portrait/2024/]

С учётом сложившихся обстоятельств и в целях формирования инфраструктуры доверия в системе защищенности цифрового рубля Банком России сформулированы новые требования к участникам ПЦР [10] в соответствие с которыми разработана ролевая модель ее участников [11], включающей два уровня.

Первый уровень – **Банк России.** На первом уровне оператор платформы непосредственно создает и модифицирует саму «платформа цифрового рубля», а также подключает к ней Федеральное казначейство и иные финансовые организации (рис. 4).

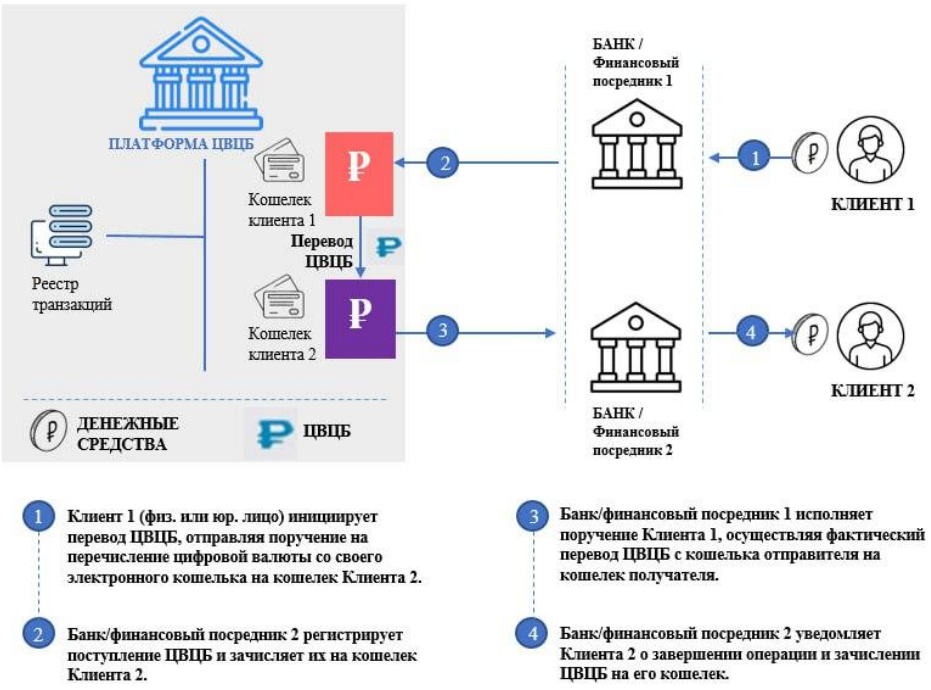


Рис. 4. Ролевая модель участников платформы цифрового рубля [Банк России. Концепция цифрового рубля. 2021]

Второй уровень – финансовые организации и Федеральное казначейство. На втором уровне уже финансовые организации взаимодействуют с клиентами по открытию и пополнению кошельков в рамках законодательства.

Архитектура прототипа ПЦР включает следующие ключевые компоненты: *Узлы Банка России, Удостоверяющий центр Банка России* и *Выделенный удостоверяющий центр Банка России*. *Удостоверяющие центры кредитных организаций* – компоненты, обеспечивающие регистрацию и сертификацию ключей клиентов; *API ПЦР* – программный интерфейс, через который кредитные организации будут подключаться к ПЦР; API *кредитных организаций (API КО)* – программный интерфейс для взаимодействия кредитных организаций и клиентов; *Устройства пользователей* – мобильные приложения, предоставляемые КО своим клиентам.

Функционально архитектурный анализ позволил разработать базовую модель инфраструктуры доверия цифрового рубля (рис. 5).

Предложенная базовая модель позволила разработать инфраструктуру доверия в системе цифрового рубля, структурными элементами которой являются:

1. *Платформа цифрового рубля Банка России* (ПЦРБР) на которую возложены функции оператора ПЦР [12, 13].

2. *Участники (кредитные организации) и пользователи (клиенты) ПЦР,* которым представляется доступ к платформе и обеспечивается возможности для совершения операций с цифровыми рублями. Участники ПЦР должны вести административное сопро-

вождение (вести документацию), а также применять технологические меры защиты информации, используемых для контроля целостности, подтверждения подлинности и обеспечения конфиденциальности электронных сообщений на этапах их подготовки, обработки, передачи и хранения, и правила их применения, в том числе порядок применения СКЗИ.

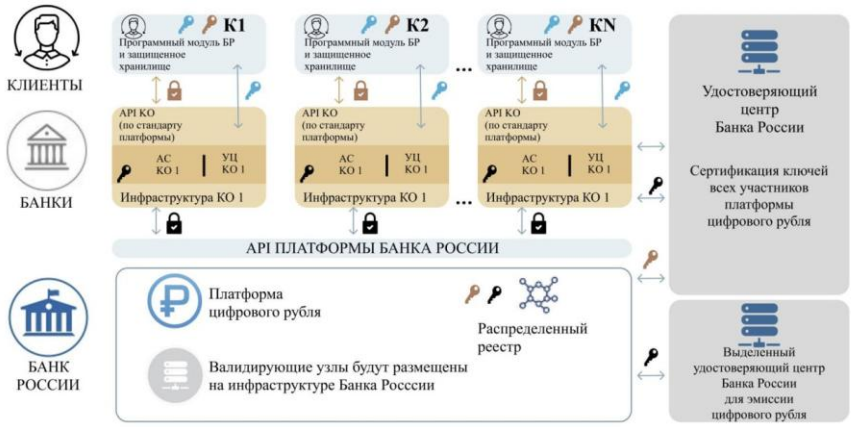


Рис. 5. Базовая модель инфраструктуры цифрового рубля [Банк России. Концепция цифрового рубля. С. 23]

3. *Инструменты,* обеспечивающие: открытие, ведение и закрытие счетов ЦР физических и юридических лиц; применение электронных денежных средств (ЭДС) и электронных средств платежа (ЭСП); перевод, пополнение счета и вывод средств со счета цифрового рубля.

4. *Механизмы контроля за соблюдением правил платформы*.

5. *Выполнение требований по инфраструктуре доверия к участникам ПЦР*, которые должны проводить оценку соответствия согласно следующим показателям: оценка соответствия должна проводиться в пределах выделенных сегментов (групп сегментов) вычислительных сетей в соответствии с требованиями Стандарта Российской Федерации ГОСТ Р 57580.2-2018, а также нормативных документов [14].

6. *Удостоверяющие центры кредитных организаций (УЦКО)* – обеспечивают регистрацию и сертификацию ключей клиентов. Например, в соответствие с Регламентом аккредитованного Удостоверяющего Центра АО «АЛЬФА-БАНК» определён порядок пользования такими ключами [15]. К их числу относятся: *ключ проверки электронной подписи* (предназначен для проверки подлинности электронной подписи); к*люч электронной подписи* (предназначен для создания электронной подписи); *сертификат ключа* проверки электронной подписи (Сертификат) – электронный документ, выданный УЦ для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа проверки электронной подписи; *список отозванных сертификатов* (СОС) – электронный документ с электронной подписью уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были аннулированы (отозваны); *средства УЦ* – сертифицированный ФСБ России программно-аппаратный комплекс «Удостоверяющий Центр «КриптоПро УЦ» версии 2.0 (ПАК «КриптоПро УЦ 2.0»), используемый для реализации функций удостоверяющего центра.

7. *API (прикладные программные приложения) Банка России и кредитных организаций.* Основу безопасности API составляет шифрование, под которым понимается преобразование исходных данных в зашифрованный вид, который должен быть расшифрован с помощью специального ключа. Выделяют два метода шифрования, а именно: симметричное и асимметричное. Например, симметричное шифрование предполагает использование одного ключа как для шифрования, так и для расшифрования. В этом случае, ис-

пользуется один ключ, этот метод отличается высокой скоростью работы и эффективностью, в то же время, это создает дополнительные риски при использовании в открытых сетях. Наиболее распространённые симметричные алгоритмы – AES (Advanced Encryption Standard), который является стандартом из-за своей устойчивости к криптоанализу, 3DES (Triple DES). Существует два основных типа такого вида шифрования: блочные и потоковые шифры. Упоминаемый выше AES является блочным шифром. Это означает, что он работает с блоками данных, и это обеспечивает более высокую криптографическую стойкость. В асимметричном шифровании используется два различных ключа: один из них – открытый, им информация шифруется, другой – закрытый, который используется для расшифрования сообщения. Российским аналогом является алгоритм Кузнечик (ГОСТ Р 34.12-2015), который применяется в национальных стандартах шифрования и обеспечивает высокий уровень защиты данных в финансовых учреждениях и государственных системах [16].

Криптографические методы применяются и в банковской сфере. Например, при совершении онлайн-платежей с использованием платежной система МИР, данные передаются через защищённые каналы с использованием протоколов TLS, которые позволяют обеспечить надежную и эффективную защиту информации. Решение процедур аутентификации и авторизации осуществляется на основе использования токенов доступа в целях управления сессиями и обеспечения безопасного доступа к ресурсам. Токены позволяют проверять подлинность пользователей без необходимости повторной авторизации при каждом запросе. Токены доступа делятся на несколько типов, наиболее распространённые из них – OAuth-токены и JWT (JSON Web Tokens). OAuth-токены используются для делегированной авторизации, при которой одно приложение может получать ограниченный доступ к ресурсам пользователя, находящимся на сервере другого приложения. Данная процедура применяется для интеграции сторонних сервисов, когда они могут выполнять операции от имени пользователя, но без доступа к его логину и паролю. Данная технология начинается с аутентификации пользователя на сервере авторизации, после чего выдается токен доступа, который клиент использует для взаимодействия с API. Российским аналогом в финансовой сфере является ГОСТ OAuth 2.0, который разрабатывается в рамках отечественных стандартов безопасности для защиты персональных данных при авторизации пользователей. JWT (JSON Web Tokens) – это компактные токены, в которых полезная нагрузка (payload) кодируется в формате JSON. Каждый такой токен содержит информацию о пользователе, его правах доступа, а также времени действия. Подпись токена выполняется с использованием как асимметричных, так и симметричных ключей, что позволяет убедиться в его подлинности и целостности.

Управление сессиями с использованием токенов доступа включает несколько ключевых аспектов. Во-первых, необходимо контролировать время жизни токенов. Если не ограничивать срок действия токенов, то существуют огромные риски компрометации. В то же время для выпуска нового токена необходимо повторное подтверждение пользователя, что повышает уровень безопасности. Во-вторых, важным аспектом является безопасное хранение токенов на клиентской стороне, так как злоумышленник не должен иметь возможности добраться до токенов, даже если получил доступ к устройству пользователя. Для этого необходимо использовать безопасные каналы связи (HTTPS, TLS 1.3) для передачи токенов, чтобы исключить возможность их перехвата злоумышленниками. В-третьих, если злоумышленник получил токен, необходимо иметь механизм его немедленного аннулирования. Для этого существуют чёрные списки (blacklists), при каждом запросе сервер проверяет, не входит ли полученный токен в список отозванных. Однако у этого метода есть серьезные недостатки: передача учетных данных в каждом запросе увеличивает риск их компрометации. Поэтому были разработаны более безопасные альтернативы, такие как аутентификация через API-ключи, которые представляют собой уникальные идентификаторы, выдаваемые клиентам для доступа к ресурсам API.

Дополнительную защиту API обеспечивает многофакторная аутентификация (MFA), при которой пользователь должен подтвердить свою личность несколькими способами (например, паролем и одноразовым кодом). Это значительно снижает вероят-

ность несанкционированного доступа, даже если злоумышленник получил учетные данные пользователя. OAuth 2.0 предоставляет возможность делегированной авторизации, разделяя процесс доступа на три компонента: Ресурсный сервер – хранит защищенные данные. Сервер авторизации – выдает токены доступа после успешной аутентификации. Клиент – запрашивает доступ к данным.

API активно используются в автоматизированных банковских системах (АБС) и системах дистанционного банковского обслуживания (ДБО). В АБС обеспечивается управление счетами, кредитами и платежами, а в ДБО пользователи взаимодействуют с банковскими сервисами через интернет и мобильные приложения. Надежность API-контроля в этих системах напрямую влияет на безопасность операций. Технология защиты и безопасности API включает четыре компонента: пользователь, клиент (запрашивает доступ), сервер авторизации (выдаёт токен), ресурсный сервер (предоставляет доступ при наличии токена). Эти элементы создают многослойную систему безопасности, в которой каждая роль строго определена, однако безопасность API зависит не только от их взаимодействия, но и от того, какие используются инструменты.

API Gateway играет важную роль в архитектуре API: он управляет потоком данных, организует маршруты запросов и защищает систему от угроз. Он принимает входящие запросы, проверяет их подлинность, маршрутизирует их к соответствующим ресурсам и возвращает ответы клиентам. В сущности, это интеллектуальный диспетчер, определяющий, куда направить каждый запрос, чтобы система работала эффективно.

Для безопасности API применяются различные инструменты: SAST (статический анализ); DAST (динамический анализ); IAST (интерактивное тестирование); Фаззинг.

По результатам сравнительного анализа можно сделать следующие выводы: SAST лучше всего подходит для ранних этапов разработки, когда важно обнаружить ошибки в коде до его развертывания. Он помогает находить логические уязвимости и проблемы в управлении памятью. DAST необходим для тестирования готовых API, он особенно полезен для анализа конфигурационных ошибок, утечек данных и проблем аутентификации. IAST нужен, когда важно понимать, как API ведёт себя в рабочей среде. Он даёт точную информацию о причинах уязвимостей и позволяет тестировать API во время его работы. Фаззинг применяется для поиска нестандартных уязвимостей, помогая выявлять неожиданные ошибки в обработке входных данных, отказоустойчивости API и механизмов защиты.

Лучший подход – это комбинация всех четырёх методов, например, на этапе разработки используется SAST для выявления ошибок ещё в коде. Перед релизом API проходит DAST, чтобы проверить безопасность в реальной среде. После развертывания применяется IAST, чтобы отслеживать динамическое поведение API и выявлять скрытые уязвимости. Фаззинг используется как дополнительный метод, позволяющий тестировать API на отказоустойчивость и выявление неожиданных уязвимостей, которые не обнаруживаются другими методами. Этот подход позволяет закрыть все возможные векторы атак, минимизировать риски и обеспечить надежную защиту API на всех этапах его жизненного цикла.

Процесс работы инструментов мониторинга API можно разделить на три этапа: *1 этап* – сбор данных. Инструменты анализируют входящий трафик, фиксируют все запросы и сравнивают их с нормальным поведением пользователей. *2 этап* – выявление аномалий. Любые отклонения от стандартных моделей поведения – резкое увеличение числа запросов, аномальные значения параметров, использование устаревших методов API – попадают в категорию подозрительных. *3 этап* – автоматическое реагирование. В зависимости от настроек система может отправлять уведомления администратору, блокировать подозрительный трафик, требовать дополнительной аутентификации или временно ограничивать доступ для конкретного IP-адреса.

Шифрование и механизмы токенизации остаются основой защиты API, но их эффективность зависит не только от используемых алгоритмов, но и от того, насколько грамотно они реализованы. Утечки данных происходят не из-за слабости криптографии, а из-за ошибок в её применении. Неправильное хранение ключей, устаревшие методы шифрования, утечки токенов или их повторное использование – всё это превращает даже самые защищённые API в уязвимые точки атаки.

В целях защиты и безопасности API в России действуют стандарты для финансовых API. Например, Приказ ФСТЭК № 17 определяет требования к защите информации в государственных и корпоративных системах [17], Приказ ФСТЭК № 21 регулирует вопросы безопасности государственных информационных систем, включая требования к API, используемым в электронном документообороте [18]. В финансовом секторе также применяются требования ФСБ РФ, в частности Приказ № 378, который касается использования средств криптографической защиты информации (СКЗИ) при передаче данных через API [19]. ГОСТ Р 57580.1-2017 обязывает компании в банковской сфере проводить сертификацию API перед запуском в эксплуатацию, используя сертифицированные средства криптографической защиты информации [20]. Организации должны внедрять системы обнаружения аномалий в API-трафике и анализировать аутентификацию пользователей на предмет аномального поведения.

Заключение и предложения. Формирование инфраструктуры доверия цифрового рубля осуществляется на основе соблюдения комплекса мер по обеспечению ее безопасности, включающей:

1. *Безопасность допуска участников и пользователей к инфраструктуре цифрового рубля:* Взаимодействие клиента с платформой цифрового рубля осуществляется по защищенным каналам через приложение банка, установленное на мобильное устройство пользователя. Доступ пользователя к кошельку, на котором хранятся его цифровые рубли, а также все операции пользователя с цифровым рублем осуществляются с использованием специализированного программного модуля Банка России, интегрированного с мобильными приложениями кредитных организаций. Программный модуль БР разрабатывается Банком России и будет предоставлять API для разработчиков приложений кредитных организаций и использоваться для: обеспечения безопасного взаимодействия пользователя с банком; генерации и хранения криптографического ключа доступа клиента кредитной организации к цифровому кошельку; подписания распоряжений по операциям с цифровыми рублями клиента. Криптографическая защита каналов взаимодействия пользователей с инфраструктурой кредитной организации (шифрование) при использовании мобильного приложения кредитной организации осуществляется с применением СКЗИ, сертифицированных ФСБ России.

2. *Безопасность доступа кредитной организации к платформе цифрового рубля:* при доступе к платформе цифрового рубля осуществляется «строгая» двухсторонняя аутентификация прямых участников с использованием ключей, сертифицированных УЦБР, по защищенным каналам взаимодействия, реализованным с применением сертифицированных ФСБ России СКЗИ.

3. *Безопасность по защите данных на платформе цифрового рубля:* Применение СКЗИ, сертифицированных ФСБ России, для обеспечения целостности и достоверности данных на платформе Банка России при подписании транзакций с цифровым рублем. Создание цифровых рублей исключительно с применением эмиссионного ключа Банка России. Эмиссионный ключ Банка России регистрируется в специально выделенном УЦ Банка России для эмиссии. Применение комплекса технологических мер защиты информации (логический контроль, структурный контроль, контроль дублирования, контроль авторства и так далее). На участках, где невозможно применение сертифицированных СКЗИ, предусмотрено применение специальных технологических мер, обеспечивающих целостность данных для операций с цифровым рублем. Организация контроля целостности «смарт-контрактов» и прав доступа к возможности их запуска.

4. *Безопасность конфиденциальности на платформе цифрового рубля* предусматривает меры по обеспечению безопасности, такие как: об операциях клиентов и защите их персональных данных, а также процедур, предусмотренных законодательством в сфере ПОД/ФТ/ФРОМУ. В этом смысле степень конфиденциальности операций на платформе цифрового рубля будет обеспечена на уровне не ниже, чем при существующем механизме безналичных платежей.

Банком России определён порядок подключения участника платформы к платформе цифрового рубля [21, 22], предусматривая следующую последовательность: процедуру проведения тестовых испытаний взаимодействия; регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платфор-

мы Цифрового рубля; платформа цифрового рубля и правила заполнения полей сертификатов; стандарт платформы цифрового рубля «Требования и рекомендации к пользовательским интерфейсам при совершении операций с цифровым рублем».

Предложения по набору работ, связанных с внедрением инфраструктуры доверия системы цифрового рубля.

Минимальный и оптимальный набор работ:

1. *Удостоверяющие центры (УЦ), средства защиты информации (СЗИ), средства криптографической защиты информации (СКЗИ):*

- проектирование архитектуры решения и разработка проектной и эксплуатационной документации;
- монтаж серверов и автоматизированных рабочих мест (АРМ) обслуживающего персонала, настройка и конфигурация операционной системы (ОС);
- развёртывание и конфигурация Удостоверяющих Центров (включая HSM и сервер точного времени);
- установка и настройка средств защиты информации и средств критической защиты информации на серверах;
- установка и настройка межсетевых экранов, коммутаторов и TLS-шлюзов;
- разработка организационно-распорядительной документации;
- установка решения для автоматизации выпуска сертификатов;
- установка и настройка решения для мониторинга работоспособности Удостоверяющих Центров.

2. *Автоматизация банковской системы (АБС), дистанционное банковское обслуживание (ДБО), Мобильное приложение:*

- развёртывание решения для взаимодействия с платформой цифрового рубля (Контур контроля и контур обработки);
- доработка автоматизированной банковской системы (квитовка платежей (ED101), изменение статуса и баланса цифрового рубля клиента, изменение реквизитов клиента, проверки ПОД / ФТ и проверки АБС, бух. учет по новым счетам 30502-30504;
- API для дистанционного банковского обслуживания физических и юридических лиц;
- доработка дистанционного банковского обслуживания физических и юридических лиц (ПМ БР, экраны для веб-клиента, интеграция с АБС).

3. *Интеграция с единой системой идентификации и аутентификации информационного (ЕСИА) и системы быстрых платежей (СБП):*

- встраивание программного модуля Банка России (ПМБР) в мобильное приложение (при наличии мобильного приложения).

4. *Оценка и аудит:*

- оценка влияния для ПМ БР в мобильное приложение;
- оценка влияния для контура контроля и контура обработки;
- аудит на соответствие ГОСТ Р 57580.1-2017;
- аудит на соответствие для дистанционного банковского обслуживания и программного обеспечения в контуре контроля и контуре обработки;
- оценка влияния для решения автоматизации выпуска сертификатов[1].

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

[1] *График подключения к платформе*: Крупнейшие банки к 1 июля 2025 года должны будут обеспечить своим клиентам возможность проводить операции с цифровыми рублями. Остальным банкам с универсальной лицензией предоставляется больше времени на доработку своих систем – до 1 июля 2026 года, прочим кредитным организациям – до 1 июля 2027 года. Планируется установить сроки обязательного приема оплаты в цифровых рублях для торговых и сервисных предприятий (ТСП). Компании с годовой выручкой более 30 млн рублей должны будут это делать с 1 июля 2025 года, более 20 млн рублей – с 1 июля 2026 года, все другие – с 1 июля 2027 года [https://www.cbr.ru/fintech/dr/].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://blog.eldorado.ru/publications/chto-takoe-tsifrovoy-rubl-prostymi-slovami-komu-i-zachem-on-neobkhodim-36739.
2. https://media.halvacard.ru/financial-literacy/chto-takoe-cifrovoi-rubl-i-dlya-chego-on-nuzhen.
3. *Осипова В.С.* Безопасность цифрового рубля // Экономические науки. – 2024. – № 7 (236).
4. *Саадулаева Т.А., Шляхтина И.А.* Цифровой рубль как механизм обеспечения финансовой безопасности государства // Экономика и бизнес: теория и практика. – 2022. – № 13. – С. 111-116.
5. *Королёв В.И.* Архитектурное построение инфраструктуры открытых ключей интегрированного информационного пространства // Безопасность информационных технологий. – 2015. – Т. 22, № 3.
6. *Мельников Д.А.* Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем: автореф. дисс. … д-ра техн. наук. – М., 2022.
7. *Грачков И.А., Малюк А.А.* Проблемы разработки доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры (организационные и методические аспекты) // Безопасность информационных технологий. – 2019. – Р. 56-63.
8. *Мельников Д.А. и др.* Рекомендации по созданию инфраструктуры доверия системы цифрового рубля // Безопасность информационных технологий. – 2024. – Т. 31, № 3. – С. 43-63.
9. Концепция цифрового рубля. Банк России. – 2021. – С. 9-10. – https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf.
10. *Шашурина Ирина*. – https://in4security.com/news/tpost/jpmmfiab51-chto-nuzhno-znat-o-novih-standartah-bezo?ysclid=m7c1y7gk5404288694.
11. Положение Центрального Банка Российской Федерации от 3 августа 2023 года № 820-П «О платформе цифрового рубля». (В ред. указания ЦБ РФ от 12.07.2024 N 6804-У).
12. Указание ЦБ РФ от 12.07.2024 N 6804-У.
13. Положение Банка России от 7 декабря 2023 г. № 833-п «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля».
14. Положение ПКЗ-2005, утвержденное приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года N 66 Зарегистрирован Минюстом России 3 марта 2005 года, регистрационный N 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года N 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный N 17350); Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 года N 796; Положение Банка России от 7 декабря 2023 г. № 833-п «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля».
15. Регламент аккредитованного Удостоверяющего Центра АО «АЛЬФА-БАНК». Версия 3.0 от 27.04.2021 г. Приложение к Приказу № 519 от 27.04.2021.
16. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12─2015.
17. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК от 11 февраля 2013 г. N 17.
18. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК от 18 февраля 2013 г. N 21.
19. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности. Приказ ФСБ России от 10 июля 2014 г. N 378.
20. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер". Утверждён Приказом Росстандарта от 08.08.2017 N 822-ст.
21. Концепция цифрового рубля. Банк России. 2021.
22. Стандарт платформы цифрового рубля «Порядок подключения участника платформы к платформе цифрового рубля» Версия 1.3.

REFERENCES

1. Available at: https://blog.eldorado.ru/publications/chto-takoe-tsifrovoy-rubl-prostymi-slovami-komu-i-zachem-on-neobkhodim-36739.
2. Available at: https://media.halvacard.ru/financial-literacy/chto-takoe-cifrovoi-rubl-i-dlya-chego-on-nuzhen.

3. *Osipova V.S.* Bezopasnost' tsifrovogo rublya [Security of the digital ruble], *Ekonomicheskie nauki* [Economic sciences], 2024, No. 7 (236).
4. *Saadulaeva T.A., Shlyakhtina I.A.* Tsifrovoy rubl' kak mekhanizm obespecheniya finansovoy bezopasnosti gosudarstva [Digital ruble as a mechanism for ensuring the financial security of the state], *Ekonomika i biznes: teoriya i praktika* [Economy and business: theory and practice], 2022, No. 13, pp. 111-116.
5. *Korolev V.I.* Arkhitekturnoe postroenie infrastruktury otkrytykh klyuchey integrirovannogo informatsionnogo prostranstva [Architectural construction of the public key infrastructure of the integrated information space], *Bezopasnost' informatsionnykh tekhnologiy* [Security of Information], 2015, Vol. 22, No. 3.
6. *Mel'nikov D.A.* Metody i sredstva postroeniya sistemy upravleniya kriptograficheskoy zashchitoy na osnove infrastruktury otkrytykh klyuchey dlya shirokomasshtabnykh informatsionno-telekommunikatsionnykh sistem: avtoref. diss. … d-ra tekhn. nauk [Methods and means of constructing a cryptographic protection management system based on the public key infrastructure for large-scale information and telecommunication systems: abstract of dr. of eng. sc. diss.]. Moscow, 2022.
7. *Grachkov I.A., Malyuk A.A.* Problemy razrabotki doverennogo programmnogo obespecheniya, primenyaemogo na ob"ektakh kriticheskoy informatsionnoy infrastruktury (organizatsionnye i metodicheskie aspekty) [Problems of developing trusted software used at critical information infrastructure facilities (organizational and methodological aspects)], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2019, pp. 56-63.
8. *Mel'nikov D.A. i dr.* Rekomendatsii po sozdaniyu infrastruktury doveriya sistemy tsifrovogo rublya [Recommendations for creating a trust infrastructure for the digital ruble system], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2024, Vol. 31, No. 3, pp. 43-63.
9. Kontseptsiya tsifrovogo rublya. Bank Rossii [The concept of the digital ruble. Bank of Russia], 2021, pp. 9-10. Available at: https://cbr.ru/Content/Document/File/120075/concept_08042021.pdf.
10. *Shashurina Irina.* Available at: https://in4security.com/news/tpost/jpmmfiab51-chto-nuzhno-znat-o-novih-standartah-bezo?ysclid=m7c1y7gk5404288694.
11. Polozhenie TSentral'nogo Banka Rossiyskoy Federatsii ot 3 avgusta 2023 goda № 820-P «O platforme tsifrovogo rublya» [Regulation of the Central Bank of the Russian Federation dated August 3, 2023 No. 820-P "On the Digital Ruble Platform"]. (As amended by Bank of Russia Instruction dated July 12, 2024 No. 6804-U).
12. Ukazanie TsB RF ot 12.07.2024 N 6804-U [Instruction of the Central Bank of the Russian Federation dated July 12, 2024 No. 6804-U].
13. Polozhenie Banka Rossii ot 7 dekabrya 2023 g. № 833-p «O trebovaniyakh k obespecheniyu zashchity informatsii dlya uchastnikov platformy tsifrovogo rublya» [Regulation of the Bank of Russia dated December 7, 2023 No. 833-p "On the Requirements for Ensuring Information Security for Participants of the Digital Ruble Platform"].
14. Polozhenie PKZ-2005, utverzhdennoe prikazom Federal'noy sluzhby bezopasnosti Rossiyskoy Federatsii ot 9 fevralya 2005 goda N 66 Zaregistrirovan Minyustom Rossii 3 marta 2005 goda, registratsionnyy N 6382, s izmeneniyami, vnesennymi prikazom FSB Rossii ot 12 aprelya 2010 goda N 173 (zaregistrirovan Minyustom Rossii 25 maya 2010 goda, registratsionnyy N 17350); Prikaz Federal'noy sluzhby bezopasnosti Rossiyskoy Federatsii ot 27 dekabrya 2011 goda N 796; Polozhenie Banka Rossii ot 7 dekabrya 2023 g. № 833-p «O trebovaniyakh k obespecheniyu zashchity informatsii dlya uchastnikov platformy tsifrovogo rublya» [Regulation PKZ-2005, approved by the order of the Federal Security Service of the Russian Federation dated February 9, 2005 N 66 Registered by the Ministry of Justice of Russia on March 3, 2005, registration N 6382, with amendments introduced by the order of the FSB of Russia dated April 12, 2010 N 173 (registered by the Ministry of Justice of Russia on May 25, 2010, registration N 17350); Order of the Federal Security Service of the Russian Federation dated December 27, 2011 N 796; Regulation of the Bank of Russia dated December 7, 2023 N 833-p "On the requirements for ensuring the protection of information for participants in the digital ruble platform"].
15. Reglament akkreditovannogo Udostoveryayushchego TSentra AO «AL'FA-BANK». Versiya 3.0 ot 27.04.2021 g. Prilozhenie k Prikazu № 519 ot 27.04.2021 [Regulations of the accredited Certification Authority of ALFA-BANK JSC. Version 3.0 dated 04/27/2021. Appendix to Order No. 519 dated 04/27/2021].
16. Natsional'nyy standart Rossiyskoy Federatsii. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry. GOST R 34.12─2015 [National standard of the Russian Federation. Information technology. Cryptographic protection of information. Block ciphers. GOST R 34.12-2015].

17. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. Prikaz FSTEK ot 11 fevralya 2013 g. N 17 [On approval of requirements for the protection of information that does not constitute a state secret, contained in state information systems. Order of the FSTEC dated February 11, 2013 N 17].
18. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. Prikaz FSTEK ot 18 fevralya 2013 g. N 21 [On approval of the composition and content of organizational and technical measures to ensure the security of personal data when processing them in personal data information systems. Order of the FSTEC of February 18, 2013 N 21].
19. Ob utverzhdenii Sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh s ispol'zovaniem sredstv kriptograficheskoy zashchity informatsii, neobkhodimykh dlya vypolneniya ustanovlennykh Pravitel'stvom Rossiyskoy Federatsii trebovaniy k zashchite personal'nykh dannykh dlya kazhdogo iz urovney zashchishchennosti. Prikaz FSB Rossii ot 10 iyulya 2014 g. N 378 [On approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data when Processing them in Personal Data Information Systems Using Cryptographic Information Protection Means Necessary to Meet the Requirements for the Protection of Personal Data for Each of the Security Levels Established by the Government of the Russian Federation. Order of the FSB of Russia of July 10, 2014 N 378].
20. GOST R 57580.1-2017. Natsional'nyy standart Rossiyskoy Federatsii. Bezopasnost' finansovykh (bankovskikh) operatsiy. Zashchita informatsii finansovykh organizatsiy. Bazovyy sostav organizatsionnykh i tekhnicheskikh mer". Utverzhden Prikazom Rosstandarta ot 08.08.2017 N 822-st. [GOST R 57580.1-2017. National standard of the Russian Federation. Security of financial (banking) transactions. Protection of information of financial organizations. Basic composition of organizational and technical measures". Approved by Order of Rosstandart dated 08.08.2017 N 822-st.].
21. Kontseptsiya tsifrovogo rublya. Bank Rossii. 2021 [Concept of the digital ruble. Bank of Russia. 2021].
22. Standart platformy tsifrovogo rublya «Poryadok podklyucheniya uchastnika platformy k platforme tsifrovogo rublya» Versiya 1.3 [Digital ruble platform standard "Procedure for connecting a platform participant to the digital ruble platform" Version 1.3].

Иванов Анатолий Викторович – Финансовый университет при Правительстве Российской Федерации; e-mail: aivanov@fa.ru; г. Москва, Россия; главный научный сотрудник Института цифровых технологий; д. социол. н.; профессор.

Царегородцев Анатолий Валерьевич – Финансовый университет при Правительстве Российской Федерации; e-mail: anvtsaregorodtsev@fa.ru; г. Москва, Россия; главный научный сотрудник Института цифровых технологий; д.т.н.; профессор.

Валеев Михаил Владимирович – Финансовый университет при Правительстве Российской Федерации; e-mail: waleew.miha@hotmail.com; г. Москва, Россия; младший научный сотрудник Института цифровых технологий.

Ivanov Anatoly Viktorovich – Financial University under the Government of the Russian Federation; e-mail: aivanov@fa.ru; Moscow, Russia; chief researcher at the Institute of Digital Technologies; dr. of social. sc.; professor.

Tsaregorodtsev Anatoly Valerievich – Financial University under the Government of the Russian Federation; e-mail: anvtsaregorodtsev@fa.ru; Moscow, Russia; chief researcher at the Institute of Digital Technologies; dr. of eng. sc.; professor.

Valeev Mikhail Vladimirovich – Financial University under the Government of the Russian Federation; e-mail: waleew.miha@hotmail.com; Moscow, Russia; junior research fellow at the Institute of Digital Technologies.

УДК 004.056 DOI 10.18522/2311-3103-2025-3-246-256

К.В. Якименко, В.В. Золотарев

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В ПРОЦЕССЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: МОДЕЛИРОВАНИЕ НА ОСНОВЕ ГЕТЕРОГЕННЫХ ГРАФОВ И МЕТРИК РИСКА

Данное исследование посвящено критической проблеме обеспечения информационной безопасности (ИБ) организаций в условиях активной цифровой трансформации (ЦТ), которая неизбежно влечет за собой увеличение поверхностей атаки, появление новых уязвимостей и рисков дестабилизации систем защиты. Авторы предлагают процессно-ориентированный подход, основанный на моделировании бизнес-процессов (БП) и ИТ-ландшафта с использованием гетерогенных графов. Данная модель, представляет три ключевых типа сущностей: операции, информационные системы (ИС) *и* данные *как объекты защиты, а также атрибутированные ребра, отражающие каналы передачи и их характеристики защищенности. Такой подход обеспечивает полноценную идентификацию объектов КИИ в соответствии с требованиями ФСТЭК и позволяет анализировать сложные взаимосвязи в переходных состояниях ЦТ. В рамках исследования разработан комплекс ключевых количественных метрик для управления рисками ИБ: 1. Количество Критических Путей (ККП): Отражает изменение поверхности атаки при добавлении/удалении ИС и маршрутов данных. 2. Уровень Центральности Узлов (УЦУ): Определяет наиболее критичные для связности и уязвимые ИС (точки концентрации риска). 3. Индекс Распределённости Данных (ИРД): Характеризует соотношение облачных и локальных узлов хранения/обработки данных и связанные с этим риски контроля и безопасности. 4. Время Восстановления (ВВ): Оценивает устойчивость БП к сбоям и атакам. 5. Уровень Автоматизации Защиты (УАЗ): Показывает долю автоматизированных задач ИБ для оперативного реагирования. На основе модели и метрик предложен динамический алгоритм управления ИБ процесса ЦТ. Алгоритм предусматривает: 1. Построение графовых моделей БП "как есть" и "как должно быть". 2. Непрерывное динамическое обновление модели текущего состояния в ходе ЦТ. 3. Регулярный расчет метрик для оценки рисков в* переходных состояниях. *4. Актуализация перечня рисков и защитных мер на основе анализа метрик. Результаты включают практические рекомендации по: снижению поверхности атаки; приоритезации защиты узлов с высоким уровнем критичности; оптимизации распределения данных с учетом требований безопасности и отказоустойчивости. Предложенный подход обеспечивает прозрачность и управляемость ИБ на всех этапах ЦТ, повышает устойчивость ИТ-ландшафта к угрозам и соответствие требованиям регуляторов.*

Управление информационной безопасностью; процессный подход; алгоритм управления безопасностью; угрозы информационной безопасности; цифровая трансформация.

K.V. Yakimenko, V.V. Zolotarev

INFORMATION SECURITY MANAGEMENT IN THE DIGITAL TRANSFORMATION PROCESS: MODELING BASED ON HETEROGENEOUS GRAPHS AND RISK METRICS

This study is devoted to the critical problem of ensuring information security of organizations in the context of active digital transformation, which inevitably entails an increase in attack surfaces, the emergence of new vulnerabilities and risks of destabilization of security systems. The authors propose a process-oriented approach based on modeling business processes (BP) and the IT landscape using heterogeneous graphs. This model represents three key types of entities: operations, information systems (IS), and data as objects of protection, as well as attributed edges reflecting transmission channels and their security characteristics. This approach ensures the complete identification of CII objects in accordance with the requirements of the FSTEC and allows the analysis of complex relationships in the transitional states of CT. The study developed a set of key quantitative metrics for information security risk management: 1. Number of Critical Paths (CCPs): Reflects the change in the attack surface when adding/removing ICS and data routes. 2. Node Centrality Level (UCU): Defines the most critical for connectivity and vulnerable IP (risk concentration points). 3. Data Distribution Index (DDI): Characterizes the ratio of cloud and local data storage/processing nodes and the associated control and security risks. 4. Recovery Time (BB): Evaluates the stability of the PS to failures and attacks. 5. The level of Automation of Protection (UAZ): Shows the proportion of automated information security tasks for rapid response. Based on the model and metrics, a dynamic algorithm for managing the information security of the CT process is proposed. The

algorithm provides: 1. Construction of graph models of BP "as it is" and "as it should be". 2. Continuous dynamic updating of the current state model during the CT. 3. Regular calculation of metrics for risk assessment in transition states. 4. Updating the list of risks and protective measures based on the analysis of metrics. The results include practical recommendations on: reducing the attack surface; prioritizing node protection with a high level of criticality; optimizing data distribution taking into account security and fault tolerance requirements. The proposed approach ensures transparency and manageability of information security at all stages of the IT process, increases the resilience of the IT landscape to threats and compliance with regulatory requirements.

Information security management; process approach; security management algorithm; information security threats; digital transformation.

Введение. Переход к цифровой экономике невозможен без рассмотрения вопросов создания современной информационной инфраструктуры, что регламентировано рядом нормативно правовых документов и национальных программ таких, как, например, «Цифровая экономика Российской Федерации».

Одна из основных проблем при реализации национальных программ и при обеспечении безопасности критической информационной инфраструктуры (далее – КИИ) к внешним и внутренним угрозам связана с созданием эффективной системы управления информационной безопасностью организаций в процессе цифровой трансформации (далее – ЦТ) [1].

Активный процесс цифровизации ведет к объективному увеличению количества угроз и уязвимостей в информационной инфраструктуре предприятий и государственных учреждений, а подкрепление данной тенденции курсом на импортзамещение, а также неблагоприятной внешней конъюнктурой ведет к дестабилизации систем безопасности и потере управления процессами информационной безопасности.

В предыдущей статье были рассмотрены проблемные вопросы ЦТ на примере рассмотрены угрозы и риски возникающие процессе ЦТ и предложен алгоритм информационной безопасностью процесса ЦТ.

В данной статье предполагается расширить и детализировать предложенный ранее алгоритм с учетом проведённого дополнительного исследования предложить математическую модель алгоритма на основе графа, а также сформулировать метрики которые позволят осуществлять управление информационной безопасностью ЦТ.

Основной аспект на который предполагается обратить внимание заключается в т.н. переходных состояниях.

Предполагается что цифровая трансформация представляет собой цепочку переходные состояния от изначального состояния бизнес процесса до определенного конечного которое заявлено как цель трансформации [2]. Цифровая трансформация требует интеграции технологий в существующий ИТ-ландшафт, что можно представить как цепочку взаимодействий между компонентами системы [3, 4].

При этом зачастую движение от одного состояния в другое может осуществляться не планомерно и упорядоченно, а скачкообразно, рывками. Связано это может быть с разнообразными внешними (рыночными, санкционными и иными), так и с внутренними (недостаток временны или финансовых ресурсов) факторами [5, 6].

Идея работы состоит в том, что предлагаемый алгоритм позволит не только отслеживать изменения в процессе ЦТ но осуществлять их контроль с точки зрения обеспечения информационной безопасности предприятия.

Формирование модели. Очевидным решением для формирования модели управления ИБ процесса ЦТ является использование теории графов

Граф – это математическая структура, которая состоит из множества вершин (узлов) и множества рёбер (линий), соединяющих эти вершины. Бизнес-процесс – это последовательность взаимосвязанных задач или действий, выполняемых для достижения определённой бизнес-цели. Он включает в себя ресурсы, роли и системы, необходимые для выполнения этих задач. Логично, что БП можно рассматривать как граф, для наглядной оценки взаимосвязей между различными этапами и элементами процесса. В академической литературе и практике моделирования бизнес-процессов часто используются графические представления для анализа и оптимизации процессов [7].

Одним из наиболее простых видов графов для моделирования - ориентированный граф. Ориентированные графы могут применяться для моделирования бизнес-процесса, где вершины графа описывают компоненты процесса, а дуги — направление протекания элементарных процессов [8].

Попробуем построить простейший, абстрактный БП в виде орграфа (рис. 1).

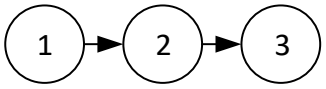


Рис. 1. Схема БП в виде орграфа

Очевидно, что простой ориентированный граф, где узлы представляют только операции, а рёбра – последовательность их выполнения, не соответствует ни задачам исследования и требованиям современных стандартов информационной безопасности по следующим причинам:

1. Отсутствие учета информационных систем (ИС). Требования правил категорирования объектов критической информационной инфраструктуры российской федерации, утвержденных постановлением Правительства Российской Федерации от 08.02.2018 № 127 и приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», требуют однозначной идентификации всех ИС и информационных активов, участвующих в критических процессах, и оценки их защищенности [9,10]. В простом графе операции не привязаны к конкретным ИС, что делает невозможным, например анализ их уязвимостей (устаревшее ПО, отсутствие шифрования в облачном сервисе и т.д.).
2. Отсутствие учета данных как объектов защиты. Согласно нормативно методических документов ФСТЭК для защиты разных видов данных могут использоваться разные ветки НМД [10]. Необходимо учитывать категории данных (персональные данные, коммерческая тайна, информация с ограничительной пометкой ДСП и т.п.). В простом графе данные не выделяются как отдельные сущности, что препятствует оценке рисков утечек или искажений.
3. Неполное отражение взаимосвязей. Требования по защите информацию подразумевают анализ всех каналов передачи данных между ИС. В простом графе рёбра отражают только логическую последовательность операций, но не физические/логические каналы связи (например, API, VPN). В свою очередь требования по защите КИИ прямо указывают на необходимость анализа и защиты от скрытых каналов передачи информации [11].

В качестве решения данной проблемы предлагается использовать гетерогенный граф, включающий узлы трёх типов – операции, ИС, данные, а также рёбра с различными атрибутами.

В первую очередь данных подход позволит обеспечить учёт ИС как узлов-исполнителей. Также каждая операция или набор операций будут связаны с определенной ИС, что позволяет с одной стороны оценивать уязвимости ИС (например, отсутствие обновлений, слабая аутентификация), а также выявлять риски, связанные с интеграцией новых ИС (например, облачных сервисов) на различных этапах и в переходных состояниях ЦТ [12].

Представление данных отдельными узлами, с опциональным указанием атрибутов их конфиденциальности позволяет обеспечить учет как самих данных с точки зрения их категорий конфиденциальности и типов (например, ПДн), а также отслеживать маршруты передачи важных данных через незащищённые каналы.

Рёбра графа, в свою очередь могут включают дополнительные атрибуты, такие как тип канала (API, HTTP, внутренняя сеть передачи данных, беспроводные каналы связи и т.п.) или уровень защищённости (шифрованный туннель, SSL-сертификат, аутентификация), что позволяет выявлять нарушения требований ФСТЭК к защите каналов передачи.

Таким образом, использование гетерогенного графа является методологически обоснованным, соответствует требованиям методических документов ФСТЭК. Данный подход позволит обеспечить идентификацию объектов защиты (ИС, данные, операции), осуществлять проектирование защитных мер на всех этапах ЦТ, а также, что является наиболее важным позволит количественно оценивать риски через метрики и осуществлять управление безопасностью процесса ЦТ в различных переходных состояниях.

Рассмотрим упрощенный бизнес процесс в виде гетерогенного графа (рис. 2). На примере упрощенного гетерогенного графа, включающего в себя ряд наборов данных, ИС и операций над данными в них, мы рассмотрим предлагаемые к использованию метрики, которые помогут осуществлять процесс управления информационной безопасностью процесса ЦТ.

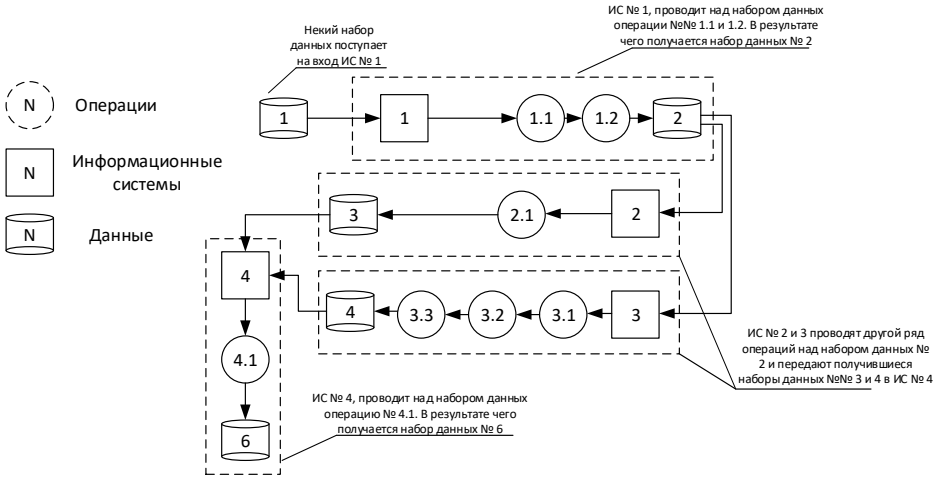


Рис. 2. БП в виде гетерогенного графа

Метрика № 1: Количество критических путей (ККП)

Термин критический путь не является стандартным для теории графов, но имеет свой контекст в теории управления проектами. Критический путь в теории управления проектами и планировании – это самая длинная последовательность задач, определяющая общую продолжительность проекта. Если в проекте есть несколько критических путей, это означает, что проект чувствителен к изменениям и требует особого внимания для своевременного завершения [13]. Количество критических путей (ККП) — это число маршрутов в графе бизнес-процесса, по которым осуществляется переход набора данных от одной ИС к другой [14]. С технической точки зрения изменение количества критических путей будет говорить нам об изменении количества информационных систем, задействованных в обеспечении функционирования БП, что в свою очередь говорит об изменении поверхности атаки доступной для злоумышленников [15].

Более приземленно критический путь можно рассмотреть, как маршрут обхода графа от точки входа (например, API, интерфейс пользователя) и до конечной ИС, обрабатывающий или хранящий выходные данные (например, база данных с ПДн, сервер отчетности). На данном пути могут находиться операции, ИС и каналы передачи данных, каждый из которых может иметь свой набор уязвимых компонентов.

В качестве примера можно рассмотреть БП формирования отчетности из предыдущей статьи. В процессе формирования отчётности критическим путём может быть цепочка состоящая из внешнего запроса → Веб-сервера обрабатывающего запрос → Сервиса агрегации данных → База данных → Генератор отчётов → Сервера публикации данных (рис. 3).

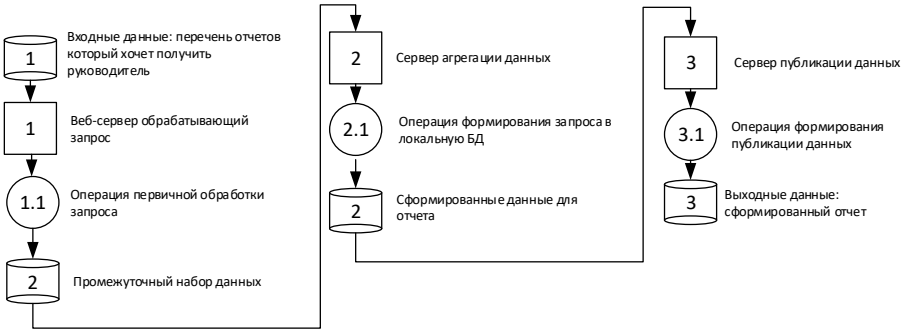


Рис. 3. Пример БП формирования отчетности

В ходе цифровой трансформации данного БП были добавлены новые источники данных предоставляющие их по запросу сервиса агрегации (рис. 4).

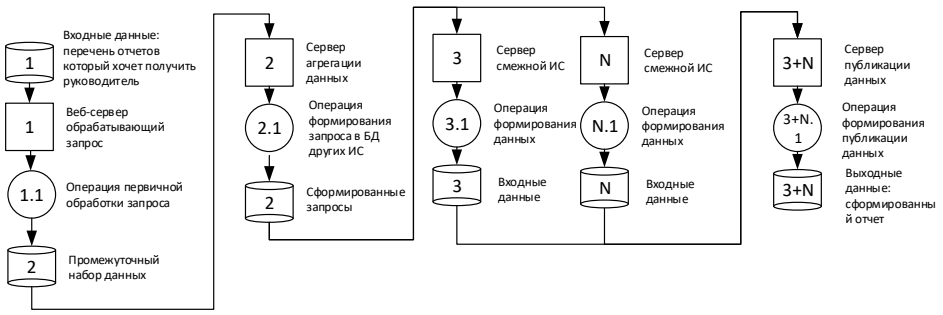


Рис. 4. Пример БП формирования отчетности после цифровой транформации

Увеличение ККП после цифровой трансформации означает, что появились новые маршруты доступа к защищаемым данным (например, интеграция облачного сервиса, добавление доступа через API). Как следствие расширяется поверхность атаки – злоумышленник имеет больше вариантов для вторжения в систему. Увеличение ККП должно быть явным сигналом к необходимости пересмотра перечня защитных мер и существующей матрицы рисков и модели угроз.

Уменьшение ККП в свою очередь будет означать упрощение архитектуры (например, удаление устаревших ИС). Сокращение уязвимых мест для совершения атак. Это хорошо, в тех случаях если не нарушается работоспособность процесса.

Таким образом в процессе управления ИБ ЦТ, мы должны стремиться к минимизации ККП без потери функциональности.

Если ККП = 0 – процесс изолирован, но, скорее всего, нефункционален (например, данные вообще никуда не передаются).

Если ККП = 1 – есть единственный путь обхода, к которому мы применяем защитные меры (например, всё шифруется и аутентифицируется). Это оптимально для высококритичных процессов. Если ККП > 1 – требуется отдельно рассматривать каждый КП и рассматривать ИС на нем, внедрять в них защитные меры.

Пример: предположим в процессе ЦТ ККП вырос с 2 до 4. Это сигнал говорящий о появлении двух маршрутов на которых могут быть новые ИС, к которым должны быть применены защитные меры.

ККП будет выступать параметром, сигнализирующим о появлении новых маршрутов на которых могут быть новые ИС, к которым в свою очередь нужно применить защитные меры. Чем меньше путей к критическим данным – тем лучше. Рост ККП также может быть сигналом к перепроектировать процесс с целью исключения избыточных взаимодействий.

Метрика № 2: Уровень центральности узлов (УЦУ)

Уровень центральности узла показывает, насколько он важен для связности всего бизнес-процесса. Чем больше маршрутов проходит через узел графа, тем выше его центральность. Например, если ИС «Сервер авторизации» участвует в 90% операций (например, проверка доступа, шифрование данных), его центральность будет крайне высокой. Если злоумышленник взломает его, он получит контроль над большей частью процесса [16].

$$\text{Сстепень}=\frac{v}{\text{n}-1},$$

где v – количество ребер, проходящих через узел, n – общее количество узлов графа.

Узел с высокой центральностью будет потенциально критическим ресурсом для атак. Например, ИС, через которую передаются все финансовые транзакции, контроллер домена и т.п., будут представлять особый интерес для злоумышленника. Помимо этого системы с узлами имеющими высокий УЦУ могут быть менее устойчивы – при выходе из строя такого узла под угрозу ставится весь БП.

Узел с низкой центральностью выполняют второстепенную роль. Даже его компрометация не нанесёт серьёзного ущерба.

В качестве примера рассмотрим ИС № 3 на рис. 3 и ИС № 3+N на рис. 4 – серверы публикации данных. До трансформации указанный сервер имел центральность по степени 0.6 (через него проходили два ребра и всего в графе было 3 однотипных узла). Предположим, что после ЦТ и добавлении пяти новых источников данных его центральность выросла и стала составлять 0.75, так как входящие в сервер данные распределены и поступают из различных системам. Это увеличивает нагрузку на указанный сервер.

Для ИБ-специалистов определение данной метрики позволит расставить приоритеты и в первую очередь рассматривать узлы с высоким УЦУ, как потенциально более интересные для злоумышленников.

УЦУ – это «индикатор важности» узла. Снижение центральности ключевых узлов уменьшает риски катастрофических последствий при атаках. Рост центральности будет сигналом к возможно пересмотру архитектуры процесса (например, внедрение распределённых систем). Естественно и то, что нельзя полностью исключить центральные узлы, но можно сделать их защиту приемлемой.

Метрика № 3 Индекс распределённости данных (ИРД)

Индекс распределённости данных (ИРД) показывает отношение количества распределённых (облачных) узлов данных к общему количеству узлов с данными. ИРД показывает насколько данные бизнес-процесса распределены между локальными и облачными системами, серверами или платформами. Чем выше ИРД, тем больше данных хранится или обрабатывается в распределённых средах (например, облаках, географически удалённых серверах), а не в одной централизованной системе.

$$\text{ИРД}=\frac{\text{Количество распределённых узлов данных}}{\text{Общее количество узлов данных}}\times 100\%.$$

Пример: Если 80% данных компании хранятся в трёх разных облачных хранилищах (AWS, Azure, Google Cloud), а 20% – на локальном сервере, ИРД будет высоким.

Высокий ИРД как и низкий имеет свои преимущества и недостатки. Преимущества заключаются в повышенной отказоустойчивости (данные не пропадут при аварии одного узла). В свою очередь увеличивается поверхность атаки (больше точек доступа для злоумышленников) и специалистам ИБ сложнее контролировать соблюдение требований по безопасность. Также могут возникнуть проблемы с согласованностью данных (дублирование, устаревшие версии и т.п.) [17, 18].

Компания хранит данные клиентов в нескольких облачных хранилищах. Это защищает от потери данных, но требует настройки единой политики доступа.

Преимуществом низкого ИРД будет простота управления и защиты поскольку все данные хранятся в одном месте (например в локальном ЦОДе). В свою очередь локальный ЦОД будет являться единой точка отказа: если злоумышленники взломают центральный узел, все данные будут скомпрометированы. Также недостатком низкого ИРД будет слабая масштабируемость – при росте нагрузки система может не справиться.

ИРД – это «индикатор гибкости и уязвимости». При слишком высоком ИРД может снижаться контроль над данными и процессами, при слишком низком снижаться устойчивость системы к атакам. Оптимальное значение зависит от типа данных, бизнес-задач и зрелости системы защиты.

Метрика № 4: Время восстановления (ВВ)

Время восстановления применительно к БП это период времени за который БП возвращаются в рабочее состояние после сбоя, атаки или иного инцидента. Например, после взлома базы данных восстановление может включать устранение уязвимости, восстановление данных из резервной копии, проверку целостности. После отказа сервера – запуск резервного оборудования или переключение на облачный ресурс [19].

Низкое ВВ (часы/минуты) говорит о том, что БП оперативно реагирует на инциденты, есть автоматизированные решения (например, резервные серверы, скрипты восстановления).

Высокое ВВ ведет к долгому простою БП, может привести к финансовым потерям, репутационным рискам, нарушению законодательства и т.п. идеальной ситуацией будет минимизация ВВ для критических систем (платежи, медобслуживание).

Метрика № 5 уровень автоматизации защиты (УАЗ)

Уровень автоматизации защиты (УАЗ) – это показатель, отражающий долю процессов информационной безопасности (ИБ), которые выполняются автоматически, без ручного вмешательства. Чем выше УАЗ, тем больше задач (мониторинг, обнаружение угроз, реагирование) решается с помощью алгоритмов, скриптов и специализированных систем (например, SIEM, SOAR) [20].

Примерами автоматизированных процессов могут быть автоматическое блокирование подозрительных IP-адресов, сканирование уязвимостей, генерация и применение правил межсетевого экрана, отправка оповещений о нарушениях в режиме реального времени.

$$\text{УАЗ}=\frac{\text{Количество автоматизированных задач ИБ}}{\text{Общее количество задач ИБ}}\times 100\%.$$

Высокий УАЗ говорит о возможности оперативного реагирования на угрозы, снижении нагрузки на сотрудников (рутину выполняют системы), минимизации человеческих ошибок (например, пропущенных уязвимостей) [21].

Алгоритм управления информационной безопасностью процесса цифровой трансформации. Исходя из проведённого исследования, сформированной модели и обозначенных проблемных вопросов ЦТ алгоритм действий, применение которого позволит учесть максимально возможное количество аспектов переходных состояний цифровой трансформации, учесть их влияние на защищенность информационных систем и сформулировать при необходимости, дополнительные защитные меры.

Алгоритм выглядит следующим образом:

1. Формирование перечня автоматизируемых бизнес-процессов, их границ и текущих показателей.
2. Определение перечня информационных систем, обрабатывающих информацию, необходимую для функционирования бизнес-процесса на текущем этапе, их взаимосвязи, перечень входных и выходных данных, текущий уровень защищенности и иные показатели информационной системы, отслеживаемые в нормальном режиме её функционирования.

3. Формирование графа бизнес-процессов «как есть» до начала ЦТ с учетом рассмотренных выше требований.
4. Формирование графа бизнес-процессов «как должно быть» после окончания процесса ЦТ, как некого целевого значения к котором мы должны прийти по завершению ЦТ.
5. Динамическое обновление графа БП «как есть» в текущий момент времени.
6. Анализ предложенных метрик.
7. Формирование\актуализация перечня рисков и защитных мер, которые необходимо предпринять в текущем переходном состоянии ЦТ.

Схема алгоритма в нотации EPC представлена на рис. 5.

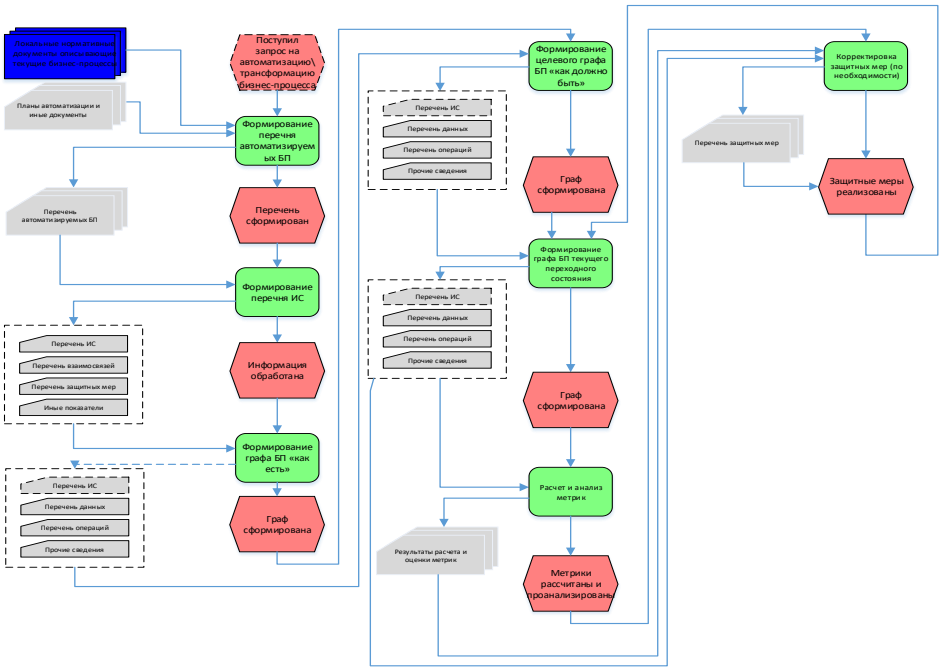


Рис. 5. Алгоритм управления

Описание алгоритма и его графическое представление наглядно демонстрирует, насколько обогащается имеющий набор данных об информационных система, инфраструктурных взаимодействия и потенциальных угрозах информационной безопасности исследуемых систем, а также какие элементы уровня организации процессов могут быть затронуты при внедрении указанного процесса.

Заключение. Исследование сосредоточено на формировании пригодных в практике рекомендаций и алгоритмов управления информационной безопасностью в процессе цифровой трансформации, с точки зрения, как традиционных подходов к управлению рисками и изменениями, так и с точки зрения комплексного подхода, учитывающего взаимосвязи бизнес-процессов и информационных систем, а также влияние изменений на смежные процессы и системы, а также организацию в целом.

Результатом исследования является формирование алгоритма управления информационной безопасностью переходных состояний цифровой трансформации, привязка данного алгоритма к переходным состояниям, измеримым метрикам информационных систем и их параметрам. Подобная привязка позволит учитывать исходное состояние информационной системы до начала процесса цифровой трансформации, а также задавать целевые значения, что в свою очередь позволит сделать процесс цифровой трансформации более прозрачным с точки зрения информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Stefan Rass.* Cyber-Security in Critical Infrastructures. Advanced Sciences and Technologies for Security Applications. – Springer, 2020.
2. *Ana-Marija Stjepić*. Mastering digital transformation through business process management: Investigating alignments, goals, orchestration, and roles. – URL: https://jemi.edu.pl/vol-16-issue-1-2020/mastering-digital-transformation-through-business-process-management-investigating-alignments-goals-orchestration-and-roles.
3. *Баланов А.Н.* Цифровая трансформация бизнеса: учебное пособие для ВУЗов. – СПб.: Лань, 2024.
4. Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16).
5. *Грибанов Ю.И.* Факторы и условия цифровой трансформации социально-экономических систем // Вестник Алтайской академии экономики и права. – 2019. – № 2-2. – С. 253-259. – URL: https://vaael.ru/ru/article/view?id=320 (дата обращения: 24.03.2025).
6. *Ревякин П.И., Зинич А.В., Помогаев В.М.* Цифровая трансформация университетов: угрозы информационной безопасности и направления снижения рисков // Экономическая безопасность. – 2024. – Т. 7, № 11. – С. 2753-2770. – DOI: 10.18334/ecsec.7.11.122061.
7. Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием. – URL: https://digital.gov.ru/uploaded/files/7metodicheskierekomendatsii06092022125913_TZmtVQB.pdf (дата обращения: 21.03.2025).
8. *Дождиков К.В.* Моделирование бизнес-процессов с помощью метаграфов // Проблемы современной экономики (Новосибирск). – 2014. – № 22-2. – URL: https://cyberleninka.ru/article/n/modelirovanie-biznes-protsessov-s-pomoschyu-metagrafov (дата обращения: 23.03.2025).
9. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных постановлением Правительства от 8 февраля 2018 г. № 127.
10. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России от 25 декабря 2017 г. № 239 (в ред. Приказов ФСТЭК России от 9 августа 2018 г. N 138, от 26 марта 2019 г. N 60, от 20 февраля 2020 г. N 35).
11. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ (последняя редакция).
12. Концепция цифровая трансформация 2030. – URL: https://www.rossetivolga.ru/i/files/2019/2/7/kontseptsiya_tsifrovaya_transformatsiya_2030.pdf (дата обращения: 21.03.2025).
13. Метод критического пути в управлении проектами. – URL: https://skillbox.ru/media/management/kak-zavershit-proekt-v-srok-s-pomoshchyu-metoda-kriticheskogo-puti-rasskazyvaem-na-primere/ (дата обращения: 24.03.2025).
14. Подробное руководство по методу критического пути. – URL: https://ru.smartsheet.com/critical-path-method (дата обращения: 24.03.2025).
15. *Пальчевский Е.В.* Прогнозирование угроз в сложных распределенных системах на основе интеллектуального анализа больших данных автоматизированных средств мониторинга // Программные продукты и системы. – 2021. – № 2. – С. 230-236. – URL: https://swsys.ru/index.php?page=article&id=4811&ysclid=m8k65v2fsd994246327.
16. Информационная безопасность и цифровая трансформация. Безопасность функционирования информационных ресурсов. Отчет ПАО «РусГидро». – URL: https://ar2023.rushydro.ru/strategic-review/information-security.html (дата обращения: 24.03.2025).
17. Роль безопасности в цифровой трансформации бизнеса. – URL: https://infars.ru/blog/rol-bezopasnosti-v-tsifrovoy-transformatsii-biznesa/ (дата обращения: 24.03.2025).
18. Технологии информационной безопасности, важные для цифровой трансформации крупного бизнеса. – URL: https://www.nic.ru/help/tehnologii-informacionnoj-bezopasnosti-vazhnye-dlya-cifrovoj-transformacii-krupnogo-biznesa_14011.html.
19. *Лобкова Е.В., Ки-Юан А.А.* Цифровая трансформация систем обеспечения безопасности // Государственное и муниципальное управление. Ученые записки. – 2023. – № 2. – С. 115-127. – URL: https://doi.org/10.22394/2079-1690-2023-1-2-115-127.
20. Цифровая трансформация, стратегия и процессы ИТ. – URL: https://kept.ru/services/tsifrovaya-transformatsiya-strategiya-i-protsessy-it (дата обращения: 24.03.2025).
21. Кибербезопасность и цифровая трансформация: 3 главных тенденции защиты данных. – URL: https://cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (дата обращения: 24.03.2025).

REFERENCES

1. *Stefan Rass.* Cyber-Security in Critical Infrastructures. Advanced Sciences and Technologies for Security Applications. Springer, 2020.
2. *Ana-Marija Stjepić*. Mastering digital transformation through business process management: Investigating alignments, goals, orchestration, and roles. Available at: https://jemi.edu.pl/vol-16-issue-1-2020/mastering-digital-transformation-through-business-process-management-investigating-alignments-goals-orchestration-and-roles.
3. *Balanov A.N.* Tsifrovaya transformatsiya biznesa: uchebnoe posobie dlya VUZov [Digital transformation of business: a textbook for universities]. Sait Petersburg: Lan', 2024.
4. Pasport natsional'noy programmy «Tsifrovaya ekonomika Rossiyskoy Federatsii», utverzhden prezidiumom Soveta pri Prezidente Rossiyskoy Federatsii po strategicheskomu razvitiyu i natsional'nym proektam (protokol ot 24 dekabrya 2018 g. № 16) [Passport of the national program "Digital Economy of the Russian Federation", approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects (minutes of December 24, 2018, No. 16)].
5. *Gribanov Yu.I.* Faktory i usloviya tsifrovoy transformatsii sotsial'no-ekonomicheskikh sistem [Factors and conditions of digital transformation of socio-economic systems], *Vestnik Altayskoy akademii ekonomiki i prava* [Bulletin of the Altai Academy of Economics and Law], 2019, No. 2-2, pp. 253-259. Available at: https://vaael.ru/ru/article/view?id=320 (accessed 24 March 2025).
6. *Revyakin P.I., Zinich A.V., Pomogaev V.M.* Tsifrovaya transformatsiya universitetov: ugrozy informatsionnoy bezopasnosti i napravleniya snizheniya riskov [Digital transformation of universities: threats to information security and directions for risk reduction], *Ekonomicheskaya bezopasnost'* [Economic Security], 2024, Vol. 7, No. 11, pp. 2753-2770. DOI: 10.18334/ecsec.7.11.122061.
7. Metodicheskie rekomendatsii po tsifrovoy transformatsii gosudarstvennykh korporatsiy i kompaniy s gosudarstvennym uchastiem [Methodological recommendations for the digital transformation of state corporations and companies with state participation]. Available at: https://digital.gov.ru/uploaded/files/7metodicheskierekomendatsii06092022125913_TZmtVQB.pdf (accessed 21 March 2025).
8. *Dozhdikov K.V.* Modelirovanie biznes-protsessov s pomoshch'yu metagrafov [Modeling business processes using metagraphs], *Problemy sovremennoy ekonomiki (Novosibirsk)* [Problems of Modern Economy (Novosibirsk)], 2014, No. 22-2. Available at: https://cyberleninka.ru/article/n/modelirovanie-biznes-protsessov-s-pomoschyu-metagrafov (accessed 23 March 2025).
9. Pravila kategorirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii, a takzhe perechnya pokazateley kriteriev znachimosti ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i ikh znacheniy, utverzhdennykh postanovleniem Pravitel'stva ot 8 fevralya 2018 g. № 127 [Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values, approved by Government Resolution No. 127 of February 8, 2018].
10. Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Prikaz FSTEK Rossii ot 25 dekabrya 2017 g. № 239 (v red. Prikazov FSTEK Rossii ot 9 avgusta 2018 g. N 138, ot 26 marta 2019 g. N 60, ot 20 fevralya 2020 g. N 35) [On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation: Order of the FSTEC of Russia dated December 25, 2017 No. 239 (as amended by Orders of the FSTEC of Russia dated August 9, 2018 No. 138, dated March 26, 2019 No. 60, dated February 20, 2020 No. 35)].
11. Federal'nyy zakon «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» ot 26 iyulya 2017 g. № 187-FZ (poslednyaya redaktsiya) [Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 No. 187-FZ (latest revision)].
12. Kontseptsiya tsifrovaya transformatsiya 2030 [Concept of Digital Transformation 2030]. Available at: https://www.rossetivolga.ru/i/files/2019/2/7/kontseptsiya_tsifrovaya_transformatsiya_2030.pdf (accessed 21 March 2025).
13. Metod kriticheskogo puti v upravlenii proektami [The critical path method in project managemen]. Available at:https://skillbox.ru/media/management/kak-zavershit-proekt-v-srok-s-pomoshchyu-metoda-kriticheskogo-puti-rasskazyvaem-na-primere/ (accessed 24 March 2025).
14. Podrobnoe rukovodstvo po metodu kriticheskogo puti [A detailed guide to the critical path method]. Available at:https://ru.smartsheet.com/critical-path-method (accessed 24 March 2025).

15. *Pal'chevskiy E.V.* Prognozirovanie ugroz v slozhnykh raspredelennykh sistemakh na osnove intellektual'nogo analiza bol'shikh dannykh avtomatizirovannykh sredstv monitoringa [Forecasting threats in complex distributed systems based on intelligent analysis of big data of automated monitoring tools], *Programmnye produkty i sistemy* [Software Products and Systems], 2021, No. 2, pp. 230-236. Available at: https://swsys.ru/index.php?page=article&id=4811&ysclid=m8k65v2fsd994246327.
16. Informatsionnaya bezopasnost' i tsifrovaya transformatsiya. Bezopasnost' funktsionirovaniya informatsionnykh resursov. Otchet PAO «RusGidro» [Information security and digital transformation. Security of functioning of information resources. Report of PJSC RusHydro]. Available at:https://ar2023.rushydro.ru/strategic-review/information-security.html (accessed 24 March 2025).
17. Rol' bezopasnosti v tsifrovoy transformatsii biznesa [The role of security in digital business transformation]. Available at: https://infars.ru/blog/rol-bezopasnosti-v-tsifrovoy-transformatsii-biznesa/ (accessed 24 March 2025).
18. Tekhnologii informatsionnoy bezopasnosti, vazhnye dlya tsifrovoy transformatsii krupnogo biznesa [Information security technologies important for the digital transformation of large businesses]. Available at: https://www.nic.ru/help/tehnologii-informacionnoj-bezopasnosti-vazhnye-dlya-cifrovoj-transformacii-krupnogo-biznesa_14011.html.
19. *Lobkova E.V., Ki-Yuan A.A.* Tsifrovaya transformatsiya sistem obespecheniya bezopasnosti [Digital transformation of security systems], *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski* [State and Municipal Administration. Scientific Notes], 2023, No. 2, pp. 115-127. Available at: https://doi.org/10.22394/2079-1690-2023-1-2-115-127.
20. Tsifrovaya transformatsiya, strategiya i protsessy IT [.Available at: https://kept.ru/services/tsifrovaya-transformatsiya-strategiya-i-protsessy-it [Digital transformation, strategy and IT processes] (accessed 24 March 2025).
21. Kiberbezopasnost' i tsifrovaya transformatsiya: 3 glavnykh tendentsii zashchity dannykh [Cybersecurity and digital transformation: 3 main trends in data protection]. Available at: https://cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (accessed 24 March 2025).

Якименко Кирилл Викторович – Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева; e-mail: Yakimenko.KV@yandex.ru; г. Красноярск, Россия; аспирант; ORCID: 0009-0003-3374-1569.

Золотарев Вячеслав Владимирович – Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева; e-mail: zolotorev@mail.sibsau.ru; г. Красноярск, Россия; к.т.н.; зав. кафедрой безопасности информационных технологий; ORCID: 0000-0002-8054-8564.

Yakimenko Kirill Viktorovich – Reshetnev Siberian State University of Science and Technology; e-mail: Yakimenko.KV@yandex.ru; Krasnoyarsk, Russia; graduate student; ORCID: 0009-0003-3374-1569.

Zolotarev Vyacheslav Vladimirovich – Reshetnev Siberian State University of Science and Technology; e-mail: zolotorev@mail.sibsau.ru; Krasnoyarsk, Russia; cand. of eng. sc.; head of Information Technologies Security Department; ORCID: 0000-0002-8054-8564.

УДК 621.396.624 DOI 10.18522/2311-3103-2025-3-256-264

А.П. Плёнкин

ЭНЕРГЕТИЧЕСКАЯ МОДЕЛЬ МАГИСТРАЛЬНОЙ КВАНТОВОЙ СЕТИ

Уже сегодня в России и во всём мире активно разворачиваются и создаются сети квантовых коммуникаций, разрабатываются стандарты в области квантовых технологий. В рамках дорожной карты по развитию квантовых коммуникаций в России реализуется протяженность квантовых сетей более 7 тыс. км, а к 2030 году планируется более 15 тыс. км. Квантовые коммуникации сегодня – это, по сути, технология квантового распределения ключей, которая находятся на стадии интенсивного научного исследования и развития. Применительно к магистральным квантовым сетям технология распределения секретных ключей нуждается в новых подходах реализации, так как использование аппаратуры различных вендоров и протяженность волоконно-оптических линий связи накладывают преодолимые ограничения на топологии магистральных сетей. Немаловажным аспектом при проектировании квантовых сетей является расчет потерь в

оптических каналах связи. Затухания, вносимые различными пассивными и активными элементами, как правило, рассчитываются индивидуально для каждого участка сети и в итоге формируют комплексную энергетическую модель. В статье рассматривается несколько топологий магистральных квантовых сетей и приводится расчет оптических потерь для волоконно-оптического канала связи. В общем виде описан способ обнаружения оптического сигнала в сетях квантовых коммуникаций. Целью статьи является сравнительный анализ энергетических моделей топологий магистральных квантовых сетей и представление варианта реализации участка городской квантовой сети. В работе описывается применимость системы квантового распределения ключей, как в двухпроходном варианте исполнения, так и в однопроходной конфигурации. Приведены результаты анализа энергетической модели и расчет усредненных потерь в квантовом канале. В заключении мы предлагаем к рассмотрению возможный вариант топологии квантовой сети.

Квантовые коммуникации; квантовый ключ; фотонный импульс; вероятность обнаружения; доверенные узлы.

A.P. Pljonkin

ENERGY MODEL OF THE QUANTUM BACKBONE NETWORK

Already today, quantum communications networks are being actively deployed and created in Russia and around the world, and standards in the field of quantum technologies are being developed. As part of the roadmap for the development of quantum communications in Russia, the length of quantum networks is more than 7 thousand km, and by 2030 it is planned to be more than 15 thousand km. Quantum communications today are, in fact, a technology of quantum key distribution, which is at the stage of intensive scientific research and development. With regard to backbone quantum networks, the technology of secret key distribution requires new approaches to implementation, since the use of equipment from various vendors and the length of fiber-optic communication lines impose surmountable restrictions on the topology of backbone networks. An important aspect in the design of quantum networks is the calculation of losses in optical communication channels. Attenuations introduced by various passive and active elements are usually calculated individually for each section of the network and ultimately form a comprehensive energy model. The article considers several topologies of backbone quantum networks and presents the calculation of optical losses for fiber-optic communication channels of these topologies. In general, a method for detecting an optical signal in quantum communication networks is presented. The purpose of the article is a comparative analysis of energy models of backbone quantum networks and a presentation of a variant of implementing a section of an urban quantum network. The work describes a generalized principle of operation of a quantum key distribution system both in a two-pass version and in a single-pass configuration. The results of the analysis of the energy model and the calculation of average losses in a quantum channel are presented. In conclusion, we propose for consideration a possible variant of the topology of a quantum network.

Quantum communications; quantum key; photon pulse; detection probability; trusted nodes.

Введение. Квантовые коммуникации сегодня технически сводятся к квантовому распределению ключей [1, 2]. В простейшей конфигурации квантовое распределение представляет собой отправителя и получателя, которые обмениваются сигналами по оптическому каналу связи, соединяющему их. Такая простая топология именуется «точка-точка» и на практике является базовой топологией при конфигурации сложных сетей квантовых коммуникаций, включая магистральные сети. Известно, что топология «точка-точка» имеет ряд ограничений на использование в реальных условиях эксплуатации, например, максимальное расстояние передачи оптического сигнала, которое обусловлено особенностями распространения света в волокне и работой квантовых протоколов. Большинство протоколов квантового распределения ключей требуют использования оптических сигналов, ослабленных до уровня одного фотона или слабее – 0,1 фотона. Последнее означает, что в среднем каждый импульс света содержит 0,1 фотона. Это понятие используется в квантовой криптографии и указывает на то, что в среднем только один из десяти импульсов содержит фотон. Остальные девять импульсов не содержат фотонов. Это связано с вероятностной природой квантовой механики: фотоны в импульсе подчиняются статистике Пуассона. В квантовых сетях такие слабые сигналы используются для передачи квантовых состояний между узлами. Однако из-за затухания в оптических во-

локнах сигнал может становиться ещё слабее, что требует использования повторителей или других методов для увеличения дальности передачи. Использование повторителей или квантовой памяти при квантовом распределении ключей на сегодняшний день невозможно. Данные технологии в обозримом будущем не имеют перспектив достаточной степени реализации. Предел допустимого расстояния, на котором могут работать системы квантового распределения ключей в топологиях магистральных сетей требует наличия доверенных промежуточных узлов (ДПУ). Через ДПУ секретные ключи передаются по цепочке к нужным узлам сети [3]. В России также применяется подход с использованием ДПУ при построении квантовых сетей. Технически доверенный узел – это защищённое помещение, оснащённое оборудованием для квантовой криптографии. В последнее десятилетие активно исследуются методы квантового распределения ключей, которые основаны на перепутанных парах фотонов (TF QKD). Такая технология теоретически позволяет использовать конфигурацию сети с недоверенными промежуточными узлами (НПУ). В таких недоверенных узлах допускается, что злоумышленник обладает всей информацией о работе аппаратуры и имеет к ней доступ. Топология сети с НПУ представляет собой конфигурацию «точка-НПУ-точка». Квантовое распределение в такой сети реализуется по протоколу MDI (Measurement Device Independent) [4].

Обзор топологий магистральных квантовых сетей. Рассмотрим несколько примеров реализованных топологий квантовых сетей. В работе [5] продемонстрирована система квантового распределения ключей по оптическому кабелю в городской телекоммуникационной сети методом квантовой коммуникации на боковых частотах. Топология сети – «точка-точка». Длина линии ВОЛС составляла 1 км, собственные потери в ВОЛС – 1,63 дБ, марка волокна – SMF-28e. Оптическая синхронизация осуществлялась по отдельному волокну в том же кабеле. Для обмена данными по открытому каналу между станциями было установлено соединение по локальной сети. Ориентировочные суммарные потери с учетом вносимых элементами станций системы КРК затуханий составили ~ 50 дБ. В статье [6] предложена схема синхронизации квантовых часов для нескольких пользователей, которая реализована на основе источника запутанных фотонов. Сервер распределяет запутанные фотоны среди нескольких пользователей с помощью мультиплексирования. Разделение происходит по длине волны. Длина ВОЛС в эксперименте составила 75 км с собственными потерями 15 дБ. В работе не описывается энергетическая модель системы, но по составу элементов можно предположить, что суммарные потери составляют порядка 75 дБ. Статья [7] описывает систему квантового распределения ключей на основе квантовой запутанности. Источник запутанности расположен на расстоянии 32,6 км от одной станции и на расстоянии 15,2 км от другой. Результаты экспериментальных исследований показывают работу системы при потерях в 32 дБ и теоретические расчеты работы СКРК при потерях 48дБ. Исследование в [8] показывает работу системы КРК на базе протокола BB84 с предельными потерями 71,2 дБ. Отметим, что более детальная энергетическая модель или значения вносимых потерь отдельными элементами квантовой сети в статьях [7, 8] также не представлены.

Рассматривая магистральные квантовые сети с точки зрения оптических потерь, можно составить обобщенную энергетическую модель сети, основанную на сегментировании отдельных участков. В работах [9, 10] описаны основные топологии магистральных квантовых сетей и предложены способы распределения ключей, а в исследовании [11] рассматривается нестандартная топология сети и рассчитана ее энергетическая модель. На рис. 1 приведена модель магистральной квантовой сети, которая сочетает в себе несколько различных топологий. Особенностью такой структуры является возможность использования оборудования различных вендоров.

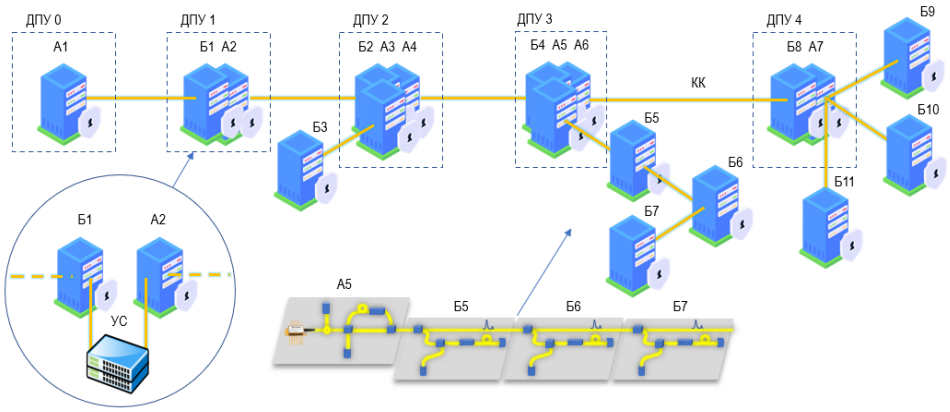


Рис. 1. Схема магистральной квантовой сети смешанной топологии

Предположим, что общая магистральная протяженность сети от ДПУ0 до ДПУ4 (рис. 1) составляет 200 км. Для удобства сеть разбита на равные по длине квантового канала сегменты (ДПУ0 – ДПУ1, ДПУ1 – ДПУ2, ДПУ2 – ДПУ3, ДПУ3 – ДПУ4), каждый из которых имеет конфигурацию «точка-точка». А – станция «Алиса», Б – станция «Боб». В каждом из доверенных промежуточных узлов станции КРК соединены физически с управляющим сервером (УС). *Напомним, что задача систем КРК заключается в выработке случайной последовательности, которую далее можно преобразовать в секретный ключ (с набором атрибутов)*. Обработкой последовательностей, формированием ключей и их использованием занимается управляющий сервер. Способы передачи секретного ключа от сегмента к сегменту описаны в [10–12]. Отметим, что подобная конфигурация сети позволяет использовать оборудование квантовой криптографии разных производителей. При рассмотрении сегмента сети с ДПУ2 видно, что узел содержит три станции СКРК, две из которых (Б2, А4) отвечают за взаимодействие с предшествующим и последующим сегментами магистральной сети. Предположим, что участок А3 – Б3 представляет собой «вертикальное» подключение к магистральной сети с длиной ВОЛС 30 км. На этом участке применяются системы КРК с односторонним квантовым протоколом [13]. Последнее означает, что Б3 содержит в своем составе лавинные фотодетекторы (ОЛФД) и при расчете потерь актуально учитывать распространение оптического сигнала только в одном направлении (от А3 к Б3). Для ДПУ2 также необходим УС, который будет взаимодействовать с тремя СКРК. В качестве УС может быть комплекс устройств, включающий, например, сервер взаимодействия с системой КРК, шифратор, коммутатор и т.д. Конфигурация участка с ДПУ3 показывает нестандартную топологию сети, в которой предполагается использование одной станции Алиса (А5) и нескольких станций Боб (Б5 – Б7). Особенностью схемы является то, что станции Боб соединены последовательно через волоконно-оптические ответвители [11]. На участке А5 – Б5 – Б6 – Б7 используется двухпроходная схема распространения оптического излучения. Это связано с тем, что станции Б5 – Б7 не содержат дорогостоящих ОЛФД, а удаленность станций позволяет использовать схему с автоматической компенсацией поляризационных (фазовых) искажений.

Рассмотрим более детально участок сети с ДПУ4 (рис. 2).

На данном сегменте предполагается использование нестандартной топологии, при которой конечными пользователями являются, как и в случае [11], устройства без ОЛФД. Отличительная особенность конфигурации заключается в наличии одной станции Алиса (А7) и нескольких систем КРК Боб (Б9 – Б11), соединенных параллельно друг другу через оптический разветвитель. Так как источник излучения и ОЛФД расположены в одной станции (А7), то возможно использование автокомпенсационного принципа с распространением оптического сигнала по одному волокну в двух направлениях. Расстояние от А7 до каждой станции Б примем равным 30 км.

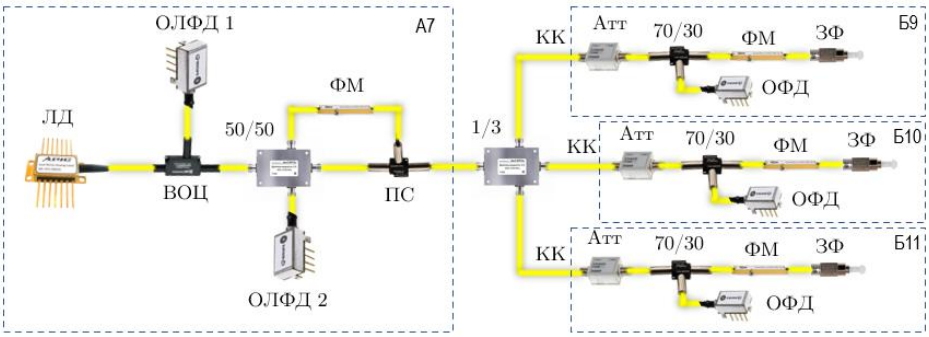


Рис. 2. Топология квантовой сети с разветвителем 1/3. ЛД – лазерный диод; ОЛФД – лавинный фотодиод; ПС – поляризационный сплиттер; КК – квантовый канал; Атт – аттенюатор управляемый

Анализ прохождения сигнала. Работа квантового протокола представляет собой одну из завершающих стадий в функционировании систем КРК, которые не могут работать без предварительных процедур настройки и синхронизации. Канал синхронизации (или калибровки) в некоторых случаях является отдельным волоконно-оптическим каналом, предназначенным для согласования и периодической настройки компонентов системы КРК. Квантовый канал и канал синхронизации могут быть объединены, то есть физически реализованы в одном оптическом волокне. В последнем случае все влияющие на оптическое волокно факторы будут одинаково отражаться как на работе квантового протокола, так и на процессе синхронизации. Общедоступный канал – это сеть передачи данных, используемая для процессов аутентификации, шифрования и дешифрования. Подавляющее большинство исследований сосредоточено на обеспечении защищенности квантовых протоколов, и лишь малая часть работ описывает процессы тактовой синхронизации. В исследовании [14] показано, что незащищенность синхронизации может быть потенциальным каналом несанкционированного доступа к системе КРК и злоумышленник, имея информацию о процессе синхронизации, может навредить работе системы. Обратимся к рис. 2. Оптический сигнал с длиной волны 1550 нм от источника излучения (ЛД) поступает на циркулятор (ВОЦ), где полностью перенаправляется против часовой стрелки на светоделитель (50/50). Далее равными долями сигнал распределяется в плечи интерферометра Маха-Цендера. В процессе синхронизации часть элементов схемы КРК не функционируют и не влияют на процесс, поэтому мы не будем акцентировать на них внимание. После интерферометра сигнал в одном волокне поступает на светоделитель 1/3. Конструктивно удобнее интегрировать светоделитель в станцию А7 или сразу после нее (в пределах ДПУ). Далее сигнал распространяется по параллельным квантовым каналам (КК) на станции Б. В каждой станции на светоделителе (70/30) сигнал поступает на фотодетектор (ОФД) и распространяется к зеркалу Фарадея (ЗФ) через фазовый модулятор (ФМ). Классический фотодетектор выполняет функцию регистрации момента поступления импульсов и фиксирует точные временные отрезки времени. Эта информация в последствии используется, например, для прикладывания напряжения к фазовому модулятору в определенный момент времени. Отраженный от ЗФ сигнал следует в обратном направлении по тому же оптическому пути к станции А7, где регистрируется ОЛФД. Мы не фокусируем внимание на способе кодирования, так как для синхронизации это не имеет значения. Отметим, что в подобных двухпроходных схемах можно использовать как поляризационное, так и фазовое кодирование состояний фотонов. Технически обнаружение синхросигнала выполняется путем последовательного анализа временных интервалов, которые измеряются в наносекундах и пикосекундах [15, 16]. Отправляя сигналы синхронизации с частотой, например, 800 Гц, и фиксируя отраженные сигналы, станция Алиса будет знать, в какой момент времени необходимо активировать ОЛФД для каждой станции Б. Исследуемая топология предполагает наличие трех параллельно со-

единенных станций Б. Последнее может вызывать следующие вопросы при физической реализации: *какова вероятность события, когда отраженные от станций Б импульсы поступят на ОЛФД А7 в один момент времени?* Предположим, что расстояние от ЛД до ЗФ у двух станций одинаковое с точностью (во временном выражении) до 1 нс. Тогда на разветвителе 1/3 при обратном распространении произойдет интерференция излучения и электроника А7 не сможет различить принадлежность сигнала к определенной станции. На практике вероятность такого события стремится к нулю, так как длительность оптического импульса в процессе калибровки составляет 1 нс, что соответствует в выражении расстояния 20 сантиметрам оптического волокна (с учетом коэффициента преломления). Кроме того, ситуацию с абсолютно равной длиной КК можно исключить путем измерения длины ВОЛС при помощи, например, оптического рефлектометра.

Нужно ли станции А7 идентифицировать станции Б, т.е. в процессе синхронизации станция А7 должна знать, какой отраженный импульс следует от какой станции Б? С одной стороны, эта задача решается классическими способами, применяемыми в топологии «точка-точка». Но рассмотрим иную сторону вопроса. При работе квантового протокола, несомненно, станции должны быть идентифицированы и аутентификация должна осуществляться до квантового распределения. Задачей синхронизации является обнаружение точных моментов регистрации импульсов в станциях А7, Б9 – Б11. Для А7 – это момент подачи напряжения на ОЛФД для активации однофотонного режима, а для станций Б – это тактовый счетчик импульсов и момент подачи напряжения, например, на фазовый модулятор. *Последнее позволяет выдвинуть гипотезу о том, что процесс синхронизации в схеме с несколькими параллельными станциями Б не нуждается в предварительной идентификации станций.* Еще один инженерный вопрос, который может возникнуть при реализации схемы: *какова вероятность того, что отраженный импульс встретится с вновь испускаемым импульсом?* Вероятность этого события исключается достаточно тривиальным способом: в реализованных системах КРК интервал между тактовыми импульсами составляет более 1 мс, что вдвое превышает предельно допустимое рабочее расстояние, даже с учетом обратного пути следования.

Отметим, что мы описываем задачу обнаружения оптического сигнала в конфигурации, когда отраженный сигнал с вероятностью 100% поступит на фотодетектор. Смешанная топология магистральной квантовой сети может содержать оборудование КРК, которое функционирует по односторонней схеме. В таком случае задача синхронизации сохраняется и, более того, алгоритм обнаружения оптического сигнала практически не изменяется. В схеме, когда квантовое распределение функционирует по одностороннему протоколу, ОЛФД расположены в удаленной станции. Обнаружение оптического синхросигнала в двухпроходной и односторонней схемах осуществляется последовательным анализом временных интервалов. В открытых источниках встречается несколько вариантов реализации пошагового поиска сигнала [15–21].

Энергетическая модель сети. Проведем усредненный анализ потерь оптического сигнала для непрерывной магистральной сети (рис. 1). Принимаем потери на сварных соединениях *(lw) = 0.03 дБ,* собственные потери в КК для одномодового волокна *(lk)* и потери на разъемных соединениях *(lf)* принимаем равными *0.2 дБ/км.* При физической реализации квантового канала схема соединения оборудования для сегментов будет выглядеть следующим образом: оптическая розетка станции соединена патч-кордом с оптическим кроссом; кросс соединен с переходной муфтой сварным соединением; далее, с учетом строительной длины кабеля, расположены проходные муфты; вводная муфта соединена с оптическим кроссом, который патч-кордом связан с розеткой станции. Отметим, что данная конфигурация является обобщенной, но в тоже время она применима к большинству топологий оптических сетей.

Суммарные потери в сегментах рассчитаем по формулам:

$$L_{\text{а1б1}} = 0.2\ (lf) * 4 + 0.03(lw) * 14 + 0.2(lk) * 50 = 11.22 \text{ дБ}.$$

$$L_{\text{а3б3}} = 0.2(lf) * 4 + 0.03(lw) * 10 + 0.2(lk) * 30 = 7.1 \text{ дБ}.$$

$$L_{\text{а5б7}} = 0.2(lf) * 8 + 0.03(lw) * 61 + 0.2(lk) * 45 = 12.43 \text{ дБ}.$$

Строительную длину кабеля ВОЛС принимаем равной 1 км. Расстояние в сегменте ДПУ3 на участках А5 – Б5, Б5 – Б6, Б6 – Б7 составляет по 15 км. Так как длина КК между сегментами ДПУ0 – ДПУ1, ДПУ1 – ДПУ2, ДПУ2 – ДПУ3, ДПУ3 – ДПУ4 одинаковая, то расчет потерь $L_{\text{а1б1}}$ справедлив и для остальных сегментов, а $L_{\text{а3б3}} = L_{\text{а7б9}} = L_{\text{а7б10}} = L_{\text{а7б11}}$ (за исключением делителя оптической мощности 1/3, вносимые затухания которого в данном случае можно отнести к погрешности). Отметим, что для всех сегментов сети, кроме А3 – Б3 необходимо учитывать обратное распространение сигнала, следовательно, потери будут вдвое больше.

Выводы и дискуссия. В исследовании рассмотрена магистральная квантовая сеть, состоящая из нескольких нестандартных топологий. Проведен расчет потерь для оптической части непрерывной квантовой сети. В общем виде описан способ обнаружения оптического сигнала в сетях квантовых коммуникаций и принцип функционирования системы квантового распределения ключей, как в двухпроходном варианте исполнения, так и в однопроходной конфигурации. Предложена модель нестандартной топологии абонентской квантовой сети, в которой одна станция Алиса взаимодействует с тремя параллельно соединенными станциями Боб. Для описанной топологии предлагается двухпроходная схема работы, когда источник излучения и ОЛФД расположены в станции Алиса.

Переходя к дискуссии, можно акцентировать внимание на нескольких актуальных проблемах по мнению автора при технической реализации квантовых сетей смешанной топологии: *защищенность каналов аутентификации* (как обеспечить безусловную защищенность процесса предварительной аутентификации удаленных станций и возможно ли это осуществить без использования классической криптографии? *Возможна ли физическая реализация предложенных в статье топологий и будет ли это эффективным решением для частных случаев?* (как в этом случае можно реализовать распределение квантовых ключей на различных принципах и протоколах – перепутанных парах фотонов, боковых частотах?). *Если злоумышленник имеет доступ к процессу тактовой синхронизации и аутентификации, то как это отражается на комплексной защищенности сети?*

Автор статьи благодарен читателю и приглашает дать обратную связь по приведенным вопросам.

Исследование выполнено за счет гранта Российского научного фонда № 25-29-00007, https://rscf.ru/project/25-29-00007/.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
2. *Bennett C.H., Brassard G., & Ekert A.K.* Quantum Cryptography // Scientific American. – 1992. – 267 (4). – P. 50-57. – http://www.jstor.org/stable/24939253.
3. *Chen Y. . et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. – 2021. – Vol. 589, No. 7841. – P. 214-219.
4. *Кулик С.П., Молотков С.Н.* MDI–Measurement Device Independent квантового распределения ключей // Письма в Журнал экспериментальной и теоретической физики. – 2023. – Т. 118, № 1. – С. 62-70.
5. *Gleĭm A.V., Chistyakov V.V., Bannik O.I. [et al.].* Sideband quantum communication at 1 Mbit/s on a metropolitan area network // Journal of Optical Technology. – 2017. – Vol. 84, No. 6. – P. 362-367.
6. *Tang B.Y. et al.* Demonstration of 75 km-fiber quantum clock synchronization in quantum entanglement distribution network // EPJ Quantum Technology. – 2023. – Vol. 10, No. 1. – P. 1-10.
7. *Pelet Y. et al.* Entanglement-based clock syntonization for quantum key distribution networks. Demonstration over a 50 km-long link // arXiv preprint arXiv:2501.16796. – 2025.
8. *Krause J. et al.* Clock offset recovery with sublinear complexity enables synchronization on low-level hardware for quantum key distribution // arXiv preprint arXiv:2404.04081. – 2024.
9. *Пленкин А.П.* Обзор топологий сетей квантовых коммуникаций // Инженерный вестник Дона. – 2024. – № 9 (117). – С. 87-97.
10. *Сабанов А.Г., Шелупанов А.А.* Идентификация и аутентификация в цифровом мире. – М.: Горячая Линия–Телеком, 2022.

11. *Пленкин А.П.* Способ обнаружения оптического сигнала в квантовых сетях // Известия ЮФУ. Технические науки. – 2024. – № 5 (241). – С. 254-260.
12. *Поздняков А.М.* Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей. – 2019.
13. *Кравцов К.С. и др.* Система релятивистской квантовой криптографии. – 2018.
14. *Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K.* Nonclassical attack on a quantum keydistribution system // Entropy. – 2021. – Vol. 23, No. 5.
15. *Pljonkin A., Rumyantsev K., Kumar Singh P.* Synchronization in quantum key distribution systems // Cryptography. – 2017. – Vol. 1, No. 3. – P. 18.
16. *Гальярди Р.М., Карп Ш.* Оптическая связь: пер. с англ. / под ред. А.Г. Шереметьева. – М.: Связь, 1978. – 424 с.
17. *Румянцев К.Е., Рудинский Е.А.* Двухэтапный временной алгоритм синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Известия ЮФУ. Технические науки. – 2017. – № 5 (190). – С. 75-89.
18. *Прудников В., Плёнкин А., Юшицына В.* Квантово-криптографические сети. – Litres, 2024.
19. *Румянцев К.Е., Миронов Я.К., Миронова П.Д.* Сравнительный анализ временных характеристик алгоритмов обнаружения синхроимпульса в системе квантового распределения ключа // IV Всероссийская научно-практическая конференция "Digital Era", Грозный, 01 марта 2024 года. – Грозный: Чеченский государственный университет имени Ахмата Абдулхамидовича Кадырова, 2024. – С. 139-141.
20. *Миллер А.В.* Синхронизация времени в спутниковом квантовом распределении ключей // Проблемы передачи информации. – 2023. – Т. 59, №. 4. – С. 13-27.
21. *Андреев С.А., Свистунова А.И.* Системы синхронизации для квантового канала связи в открытом пространстве // Наука, техника, педагогика в высшей школе: Матер. Всероссийской научно-практической конференции, Москва, 20–27 февраля 2023 года. – М.: Московский Политех, 2023. – С. 398-404.

REFERENCES

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics,* 2002, Vol. 74, No. 1, pp. 145-195.
2. *Bennett C.H., Brassard G., & Ekert A.K*. Quantum Cryptography, *Scientific American,* 1992, 267 (4), pp. 50-57. Available at: http://www.jstor.org/stable/24939253.
3. *Chen Y.A. et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature,* 2021, Vol. 589, No. 7841, pp. 214-219.
4. *Kulik S.P., Molotkov S.N.* MDI–Measurement Device Independent kvantovogo raspredeleniya klyuchey [MDI–Measurement Device Independent of Quantum Key Distribution], *Pis'ma v Zhurnal eksperimental'noy i teoreticheskoy fiziki* [Letters to the Journal of Experimental and Theoretical Physics], 2023, Vol. 118, No. 1, pp. 62-70.
5. *Gleĭm A.V., Chistyakov V.V., Bannik O.I. [et al.].* Sideband quantum communication at 1 Mbit/s on a metropolitan area network, *Journal of Optical Technology,* 2017, Vol. 84, No. 6, pp. 362-367.
6. *Tang B.Y. et al.* Demonstration of 75 km-fiber quantum clock synchronization in quantum entanglement distribution network, *EPJ Quantum Technology,* 2023, Vol. 10, No. 1, pp. 1-10.
7. *Pelet Y. et al.* Entanglement-based clock syntonization for quantum key distribution networks. Demonstration over a 50 km-long link, *arXiv preprint arXiv:2501.16796,* 2025.
8. *Krause J. et al.* Clock offset recovery with sublinear complexity enables synchronization on low-level hardware for quantum key distribution, *arXiv preprint arXiv:2404.04081,* 2024.
9. *Plenkin A.P.* Obzor topologiy setey kvantovykh kommunikatsiy [Review of quantum communications network topologies], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2024, No. 9 (117), pp. 87-97.
10. *Sabanov A.G., SHelupanov A.A.* Identifikatsiya i autentifikatsiya v tsifrovom mire [Identification and authentication in the digital world]. Moscow: Gorya-chaya Liniya–Telekom, 2022.
11. *Plenkin A.P.* Sposob obnaruzheniya opticheskogo signala v kvantovykh setyakh [Method for detecting an optical signal in quantum networks], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 5 (241), pp. 254-260.
12. *Pozdnyakov A.M.* Sposob peredachi soobshcheniya cherez vychislitel'nuyu set' s primeneniem apparatury kvantovogo raspredeleniya klyuchey [Method for transmitting a message through a computer network using quantum key distribution equipment], 2019.
13. *Kravtsov K.S. i dr.* Sistema relyativistskoy kvantovoy kriptografii [Relativistic quantum cryptography system], 2018.

14. *Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K.* Nonclassical attack on a quantum keydistribution system, *Entropy,* 2021, Vol. 23, No. 5.
15. *Pljonkin A., Rumyantsev K., Kumar Singh P.* Synchronization in quantum key distribution systems, *Cryptography,* 2017, Vol. 1, No. 3, pp. 18.
16. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz' [Optical communications]: trans. from engl, ed. by A.G. Sheremet'eva. Moscow: Svyaz', 1978, 424 p.
17. *Rumyantsev K.E., Rudinskiy E.A.* Dvukhetapnyy vremennoy algoritm sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Two-stage time synchronization algorithm in a quantum key distribution system with automatic compensation of polarization distortions], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 5 (190), pp. 75-89.
18. *Prudnikov V., Plenkin A., Yushitsyna V.* Kvantovo-kriptograficheskie seti [Quantum cryptographic networks], Litres, 2024.
19. *Rumyantsev K.E., Mironov Ya.K., Mironova P.D.* Sravnitel'nyy analiz vremennykh kharakteristik algoritmov obnaruzheniya sinkhroimpul'sa v sisteme kvantovogo raspredeleniya klyucha [Comparative analysis of temporal characteristics of sync pulse detection algorithms in a quantum key distribution system], *IV Vserossiyskaya nauchno-prakticheskaya konferentsiya "Digital Era", Groznyy, 01 marta 2024 goda* [IV All-Russian scientific and practical conference "Digital Era", Grozny, March 01, 2024]. Groznyy: Chechenskiy gosudarstvennyy universitet imeni Akhmata Abdulkhamidovicha Kadyrova, 2024, pp. 139-141.
20. *Miller A.V.* Sinkhronizatsiya vremeni v sputnikovom kvantovom raspredelenii klyuchey [Time synchronization in satellite quantum key distribution], *Problemy peredachi informatsii* [Problems of Information Transmission], 2023, Vol. 59, No. 4, pp. 13-27.
21. *Andreev S.A., Svistunova A.I.* Sistemy sinkhronizatsii dlya kvantovogo kanala svyazi v otkrytom prostranstve [Synchronization systems for a quantum communication channel in open space], *Nauka, tekhnika, pedagogika v vysshey shkole: Materialy Vserossiyskoy nauchno-prakticheskoy konferentsii, Moskva, 20–27 fevralya 2023 goda* [Science, technology, pedagogy in higher education: Proceedings of the All-Russian scientific and practical conference, Moscow, February 20-27, 2023]. Moscow: Moskovskiy Politekh, 2023, pp. 398-404.

Плёнкин Антон Павлович – Южный федеральный университет; e-mail: pljonkin@sfedu.ru; г. Таганрог, Россия; тел.: 89054592158; кафедра ИБТКС; к.т.н.; доцент.

Pljonkin Anton Pavlovich – Southern Federal University; e-mail: pljonkin@sfedu.ru; Taganrog, Russia; phone: +79054592158; the Department of Information Security of Telecommunication Systems; cand. of eng. sc.; associate professor.

УДК 004.089 DOI 10.18522/2311-3103-2025-3-264-273

П.Д. Борисов, Ю.В. Косолапов

О ФУНКЦИИ ПОХОЖЕСТИ ГРАФИЧЕСКИХ ПРЕДСТАВЛЕНИЙ ИСПОЛНЯЕМЫХ ФАЙЛОВ В МОДЕЛИ ОЦЕНКИ ОБФУСЦИРУЮЩИХ ПРЕОБРАЗОВАНИЙ

Обфускация программного кода используется с целью затруднения его анализа в модели, когда аналитик имеет полный доступ к программе. Обычно обфускация делится на криптографически стойкую и эвристически стойкую. В первом случае сложность анализа сопоставима с трудностью решения некоторой известной математической задачи. Во втором случае стойкость обосновывается, как правило, отсутствием известных на момент создания метода обфускации эффективных техник ее анализа. Криптографически стойкая обфускация пока не нашла применения на практике, в то время как эвристически стойкая широко применяется. Ранее авторами была предложена модель оценки эффективности и стойкости эвристических обфусцирующих преобразований, в основе которой лежит применение функции похожести. В настоящей работе с помощью методов машинного обучения строится такая функция похожести на основе сравнения графического представления исполняемых файлов программ. В частности, сравнение выполняется с помощью сверточной сети с четырьмя сверточными слоями, оптимизатором RMSprop, функцией потерь NLLLoss и двумя выходами полносвязного слоя. Предложенная функция применяется в

рамках реализации модели оценки эффективности и стойкости обфусцирующих преобразований. Кроме функции похожести, реализация модели также включает: базовый набор обфусцирующих преобразований, предоставляемых обфускатором Hikari; набор последовательностей обфусцирующих преобразований на основе базового набора; тестовое множество программ для обучения моделей, построенное на основе наборов CoreUtils, PolyBench и HashCat; аппроксимацию самой "понятной" версии программы с помощью наименьшей по размеру версии программы (ищется среди версий, полученных с помощью различных опций оптимизации компиляторов GCC, Clang и AOCC); схему деобфускации программ на основе оптимизирующего компилятора из состава LLVM. Результаты экспериментального исследования с реализованной моделью показали, что построенную функцию похожести применять в рамках модели оценки нецелесообразно из-за ее невысокой точности, но возможно ее применение при построении более сложных функций.

Оценка эффективности и стойкости обфусцирующих преобразований; графическое представление исполняемых файлов; функция похожести.

P.D. Borisov, Yu.V. Kosolapov

ON THE SIMILARITY FUNCTION OF GRAPHIC REPRESENTATIONS OF EXECUTIVE FILES IN THE OBFUSCING TRANSFORMATION EVALUATION MODEL

Obfuscation of program code is used to complicate its analysis in a model when the analyst has full access to the program. Obfuscation is usually divided into cryptographically secure and heuristically resistant. In the first case, the complexity of the analysis is comparable to the difficulty of solving some known mathematical problem. In the second case, the resistance is usually justified by the lack of effective techniques for analyzing the obfuscation method known at the time of its creation. Cryptographically secure obfuscation has not yet found practical application, while heuristically resistant is widely used. Previously, the authors proposed a model for assessing the efficiency and resistance of heuristic obfuscating transformations based on the use of a similarity function. In this paper, such a similarity function is constructed using machine learning methods based on a comparison of the graphical representation of program executable files. In particular, the comparison is performed using a convolutional network with four convolutional layers, an RMSprop optimizer, an NLLLoss loss function, and two outputs of a fully connected layer. The proposed function is used in the implementation of a model for evaluating the efficiency and resistance of obfuscating transformations. In addition to the similarity function, the implementation of the model also includes: a basic set of obfuscating transformations provided by the Hikari obfuscator; a set of obfuscating transformation sequences based on the basic set; a test set of programs for training models based on the CoreUtils, PolyBench and HashCat program sets; approximation of the most "understandable" version of the program using the smallest version of the program (searched among the versions obtained using various optimization options of the GCC, Clang and AOCC compilers); a program deobfuscation scheme based on the optimizing compiler from LLVM. The results of an experimental study with the implemented model showed that it is impractical to use the constructed similarity function in the framework of the evaluation model due to its low accuracy, but it is possible to use it when constructing more complex functions.

Evaluation of the effectiveness and resilience of obfuscating transformations; graphical representation of executable files; similarity function.

Введение. Защита программного обеспечения (далее – ПО) от исследования, изменения данных и алгоритмов была и остается актуальной задачей. Целью такой защиты может быть сокрытие хранимых в ПО криптографических ключей, препятствие поиску и эксплуатации уязвимостей ПО, защита от нелегитимного использования лицензированного ПО (включая модификацию кода и компонентов), защита от мошенничества в компьютерных играх и т.п. Предполагается, что аналитик, исследующий программу, не ограничен по времени, в выборе средств и способов исследования, более того, аналитик может приобрести полную лицензированную версию ПО, обладающую всеми интересующими его данными и алгоритмами (модель угроз MATE, сокр. от англ. Man At The End). В такой модели одним из средств защиты является обфускация – изменение исходного кода или исполняемого образа программы, сохраняющее ее исходную функциональность, но затрудняющее ее анализ, понимание реализованных в ней алгоритмов, а также их модификацию.

С позиции надежности методы обфускации можно разделить на доказуемо надежные и эвристически надежные [1]. Первые гарантируют надежность запутывания ряда программ (отдельных классов программ [2–4]) по отношению к любому полиномиально ограниченному аналитику, а вторые нацелены на затруднение анализа существующими на текущий момент времени средствами. Пока на практике чаще применяются эвристические методы обфускации из-за их универсальности (применимости к любым алгоритмам). Кроме того, применение доказуемо надежных методов обфускации приводит в ряде случаев к сильному разрастанию даже небольших программ и росту времени выполнения обфусцированного кода [5]. С другой стороны, разработано большое количество методов обфускации (например, [6–8]), но эффективность таких методов часто или не оценивается, или не учитывает всех аспектов обратного проектирования программы аналитиком [9].

Поэтому важной и актуальной остается проблема автоматизированной (без привлечения аналитиков) количественной оценки эффективности и стойкости методов обфускации. Обфускация для компилируемых программ может применяться на разных уровнях (на уровне исходного кода, уровне промежуточного представления, уровне бинарного кода). Соответственно, в рамках модели MATE, когда аналитику доступны только исполняемые файлы программы, оценку эффективности и стойкости эвристических методов обфускации представляется уместным выполнять именно для исполняемого файла обфусцированной программы. Отметим, что попытки выполнить оценку на уровне бинарного кода уже предпринимались: для обфусцирующих преобразований, применяемых на уровне исходного кода – в работе [10], а для преобразований на уровне бинарного кода – в работе [11].

Известен ряд практических способов и метрик для оценки эффективности эвристических обфусцирующих преобразований, а также их стойкости к анализу и пониманию программ. Относительно недавно вышел обзор, в котором была рассмотрена 571 работа, посвященная защите ПО с помощью обфускации программного кода [9]. В обзоре отмечается, что в большинстве работ посвященных обфускации в первую очередь оценивается влияние на быстродействие программы (стоимость). Оценка эффективности обфускации производится значительно реже, при этом используются наборы тестовых программ, которые или не доступны публично, или не обладают достаточным разнообразием. Такие вопросы как "На сколько можно доверять обфускации?" и "Как строить стойкие методы обфускации?" остаются без ответа [3]. В частности, авторы [3], отметили, что данные вопросы не решены для компилируемых программ. К нерешенным также можно отнести вопрос "На сколько можно доверять средствам обфускации, реализующим существующие техники запутывания кода?".

В работе [12] отмечено, что ответы на поставленные вопросы также зависят от цели аналитика и имеющихся у него средств анализа. Таким образом задача разработки и/или совершенствования способов количественной оценки эффективности и стойкости обфусцирующих преобразований, учитывающих статические и динамические характеристики программ, при наличии подходящих средств анализа у противника была и является актуальной. Способы оценки обфусцирующих преобразований должны учитывать широкое разнообразие техник, применяемых аналитиками при исследовании программ (например, дизассемблирование, отладку, анализ в виртуальной среде, символьное исполнение).

В настоящей работе используется предложенная ранее в [13] модель количественной оценки эффективности и стойкости обфусцирующих преобразований, для которой в рамках настоящей работы предложена новая функция похожести. В разделе 0 кратко приводится модель количественной оценки. В разделе 0 описывается новая функция похожести, а в разделе 0 представлены результаты экспериментальных исследований с новой функцией похожести.

Модель количественной оценки эффективности и стойкости обфусцирующих преобразований. Рассмотрим множество $\mathcal{P}_{\mathcal{P}}$ программ, полученных из программы P с помощью преобразований, сохраняющих семантику. Пусть $P_0 \in \mathcal{P}_{\mathcal{P}}$ – самая "понимаемая" версия программы P. В качестве P_0, например, можно рассматривать программу наименьшего размера, так как считается, что чем меньше размер программы, тем она

"читабельнее" [14]. С другой стороны, выбор P_0 может быть основан на сложности символьной интерпретации машинного кода [15, 16], когда в качестве P_0 может рассматриваться версия программы с наименьшим временем символьного исполнения. В [17] такой подход обоснован тем, что символьное исполнение можно рассматривать как модель динамического исследования программы аналитиком-человеком.

Понятность программы P будем рассматривать, как величину похожести программы P на P_0. Для этого рассмотрим функцию похожести

$$\delta: \mathcal{P} \times \mathcal{P} \to [0,1](\subseteq \mathrm{R}),$$

где *0* соответствует наименьшей степени похожести, а *1* – наибольшей. Также будем полагать, что $\delta(\mathrm{P}_1, \mathrm{P}_2) = \delta(\mathrm{P}_2, \mathrm{P}_1)$ для всех $(\mathrm{P}_1, \mathrm{P}_2) \in \mathcal{P} \times \mathcal{P}$ и $\delta(\mathrm{P}, \mathrm{P}) = 0$ для всех P из $\mathcal{P}$. В этом случае для фиксированных $\mathrm{P}_0 \in \mathcal{P}_{\mathcal{P}}$ и δ под *понятностью* программы $\mathrm{P} \in \mathcal{P}_{\mathcal{P}}$ можно подразумевать величину $\delta(\mathrm{P}, \mathrm{P}_0)$, как степень похожести на самую "понимаемую" версию программы.

Заметим, что поиск самой короткой программы или поиск программы с наименьшим временем символьного исполнения, являются вычислительно сложными задачами. Поэтому вместо P_0 предлагается использовать ее *аппроксимацию* $\mathrm{A}(P_0)$, найденную по P. Аналогичный подход применяется в [18], где при количественной оценке эффективности обфусцирующих преобразований вместо невычислимой Колмогоровской сложности программы применяется ее аппроксимация результатом сжатия программы. В качестве аппроксимации $\mathrm{A}(P_0)$ может быть выбрана, например, наименьшая по размеру версия программы P, полученная с помощью доступного набора оптимизирующих преобразований компиляторов. Представляется, что аппроксимацию также возможно построить на основе характеристик символьной интерпретации: например, в качестве $A(P_0)$ может быть выбрана версия программы (например, среди версий, полученных с помощью разных компиляторов и разных опций компиляции) с наименьшим временем символьной интерпретации.

Таким образом *понятностью* программы $\mathrm{P} \in \mathcal{P}_{\mathcal{P}}$ при фиксированных δ и $\mathrm{A}(\mathrm{P}_0) \in \mathcal{P}_{\mathcal{P}}$ назовем величину

$$\mathcal{C}(\mathrm{P}) = \delta\big(\mathrm{P}, \mathrm{A}(\mathrm{P}_0)\big) \in [0,1]. \quad (1)$$

Пусть $\mathcal{Q}$ – исследуемое множество последовательностей обфусцирующих преобразований, построенное на основе базового набора преобразований $\mathcal{O}$. С помощью характеристики (1) определим эффективность e обфусцирующего преобразования $O^t \in \mathcal{Q}$, примененного к программе P, а также стойкость r этого преобразования по отношению к деобфускатору D следующим образом:

$$\mathrm{e}(\mathrm{O}^{\mathrm{t}}, \mathrm{P}) = 1 - \mathcal{C}\big(\mathrm{O}^{\mathrm{t}}(\mathrm{P})\big) = 1 - \delta\big(\mathrm{O}^{\mathrm{t}}(\mathrm{P}), \mathrm{A}(\mathrm{P}_0)\big), \quad (2)$$

$$\mathrm{r}(\mathsf{D}, \mathrm{O}^{\mathrm{t}}, \mathrm{P}) = 1 - \mathcal{C}\left(\mathsf{D}\big(\mathrm{O}^{\mathrm{t}}(\mathrm{P})\big)\right) = 1 - \delta\left(\mathsf{D}\big(\mathrm{O}^{\mathrm{t}}(\mathrm{P})\big), \mathrm{A}(\mathrm{P}_0)\right). \quad (3)$$

В рамках определений (2) и (3), задача выбора наиболее эффективного обфусцирующего преобразования для P решается так: $\mathrm{O}_1^{\mathrm{t}}$ эффективнее $\mathrm{O}_2^{\mathrm{t}}$, если

$$\mathrm{e}(\mathrm{O}_1^{\mathrm{t}}, \mathrm{P}) > \max\{1 - \mathcal{C}(\mathrm{P}), \mathrm{e}(\mathrm{O}_2^{\mathrm{t}}, \mathrm{P})\}.$$

Задача выбора среди этих же преобразований наиболее стойкого по отношению к деобфускатору D решается так: $\mathrm{O}_1^{\mathrm{t}}$ является D-устойчивее $\mathrm{O}_2^{\mathrm{t}}$, если

$$\mathrm{r}(\mathsf{D}, \mathrm{O}_1^{\mathrm{t}}, \mathrm{P}) > r(\mathsf{D}, \mathrm{O}_2^{\mathrm{t}}, \mathrm{P}).$$

Набор $\mathcal{M} = (\mathcal{O}, \mathcal{Q}, \delta, \mathsf{D}, \mathsf{A})$ с определенными в соответствии с (2) и (3) функциями e и r называется *моделью оценки эффективности и стойкости обфусцирующих преобразований*. Для реализации этой модели необходимо зафиксировать набор $\mathcal{O}$, множество $\mathcal{Q}$, выбрать функцию похожести δ исполняемых файлов программ, деобфускатор D и способ аппроксимирования A самой понятной программы $\mathrm{P}_0 \in \mathcal{P}_{\mathcal{P}}$ для каждого P.

Для зафиксированного алгоритма A понятность программы P зависит от выбора функции похожести δ, определенной на парах программ. По этой причине поиск *подходящих* и *эффективно вычислимых* функций похожести, а также установление корреляции

между различными функциями являются актуальными задачами. Далее предлагается функция похожести, построенная на основе сравнения графических представлений исполняемых файлов программ.

Функция похожести графических представлений файлов. В настоящем разделе строится функция похожести δ_{im} исполняемых файлов на основе их представления в виде изображений. Именно, при таком подходе исполняемый файл программы P представляется в виде двумерного изображения $Im(P)$ в оттенках серого цвета, в котором яркость серого пикселя определяется значением соответствующего байта в исполняемом коде: минимальное значение 0 соответствует черному цвету пикселя, а максимальное значение 255 – белому. Отметим, что графическое представление исполняемых файлов не является новым подходом в области информационной безопасности и часто используется при классификации вредоносного программного обеспечения (например, в [19–21] и [22]).

Опишем предлагаемый в настоящей работе способ построения функции похожести δ_{im} для исполняемых файлов. Сначала уточним способ представления файлов в графическом виде, используемый в работе. Исполняемый файл программы P размера b байтов преобразуется в квадратное изображение $Im(P)$ размера $b_i \times b_i$, где b_i – наибольшее целое число, для которого $b_i^2 \leq b$, после чего изображение приводится к размеру 512×512 (растягивается или сжимается). Последнее преобразование выполняется с целью обеспечения возможности сравнения исполняемых файлов разного размера. Таким образом, все исполняемые файлы преобразуются в изображения размера 512×512 в оттенках серого.

Способ сравнения исполняемых файлов с графическим представлением основан на применении сверточной сети, которая обучается на множестве пар сравниваемых программ, а результатом ее работы являются два числа от 0 до 1, в сумме дающие единицу. Из этих двух чисел первое характеризует уверенность сети в том, что пара программ функционально идентична, а второе характеризует уверенность сети в том, что сравниваемые программы функционально разные. Одной паре сравниваемых программ (P_1, P_2) из множества пар соответствует изображение $Im(P_1, P_2) = Im(P_1) - Im(P_2)$ размера 512×512, где побайтовое вычитание выполняется по модулю 256 (в кольце Z_{256}). Множество пар состоит из двух подмножеств: множества пар функционально одинаковых программ и множества пар функционального разных программ. Пары из первого множества имеют метку 0, а пары из второго – метку 1. Целью обучения сети является выделение (визуальных) признаков, позволяющих судить о функциональной идентичности двух сравниваемых программ. Таким образом, значением функции $\delta_{im}(P_1, P_2)$ для пары программы (P_1, P_2) является первое значение из двух, возвращаемых обученной сетью, то есть значением является число от 0 до 1 – степень уверенности сети в том, что сравниваемые программы функционально идентичны. Далее вместо $\delta_{im}(P_1, P_2)$ будет использоваться запись $\delta_{im}\big(Im(P_1, P_2)\big)$, подчеркивающая, что при вычислении похожести программ P_1 и P_2 используется разность их графических представлений.

Для реализации предложенного способа за основу сети взята структура сверточной сети из [20] с четырьмя сверточными слоями (модель 2 в статье [20]), оптимизатором RMSprop, функцией потерь NLLLoss и двумя выходами полносвязного слоя. Формирование множества пар функционально одинаковых и разных программ реализовано на основе построенного в [13] множества исполняемых файлов. Именно, множество пар формируется на основе наборов программ CoreUtils[1], PolyBench[2] и HashCat[3] (всего 164 программы), собранных девятью компиляторами – GCC (версий 7.5.0, 8.4.0, 9.4.0, 10.3.0), Clang (версий 7.0.1, 8.0.1, 9.0.1, 10.0.0) и AOCC[4] (версии 3.0.0) – с пятью опциями оптимизации O0, O1, O2, O3 и Os. Таким образом, множество исполняемых файлов, постро-

[1] https://github.com/coreutils/coreutils (дата обращения: 13.04.2025).
[2] https://github.com/MatthiasJReisinger/PolyBenchC-4.2.1 (дата обращения: 13.04.2025).
[3] https://github.com/hashcat/hashcat-utils (дата обращения: 13.04.2025).
[4] https://www.amd.com/en/developer/aocc.html (дата обращения: 13.04.2025).

енное в [13], состоит из $164 \cdot 9 \cdot 5 = 7380$ файлов. Подмножество пар функционально одинаковых программ строилось по следующей схеме: 1) случайно выбиралась одна из 164-х программ, 2) для выбранной программы строились две случайные конфигурации (*компилятор*, *опция оптимизации*); шаги 1) и 2) повторялись для построения 10 тысяч уникальных пар. Подмножество пар функционально разных программ строилось путем построения 10 тысяч пар уникальных случайных конфигураций (*компилятор*, *опция оптимизации*, *программа*) с условием, чтобы в конфигурациях каждой пары не было одинаковых программ. Обучающая выборка содержала 50% пар из каждого подмножества, а контрольная и тестовая выборки – по 25% пар. Результаты обучения сети в течение 100 эпох показали точность (accuracy) 0.713. Попытки увеличить точность модификацией оптимизатора, функции потерь или увеличением числа эпох к положительному результату не привели.

Оценка обфусцирующих преобразований. В настоящей работе оценка обфусцирующих преобразований выполняется в соответствии с моделью, описанной в разделе 0, когда $\delta = \delta_{im}$, а остальные параметры модели выбраны такими же, как и в [13]. Именно, базовым набором обфусцирующих преобразований $\mathcal{O}$ здесь является набор из 7 преобразований, предоставляемых обфускатором Hikari[5].

В табл. 1 перечислены обозначения (столбец o) и описание этих преобразований, а также указан соответствующий тип $\theta(o)$ преобразований на основе определений, введенных для обфускатора Tigress в [15]. Набор Q представляет собой набор из 63-х последовательностей O^t, состоящих из одного, двух и трех разных преобразований, входящих в базовый набор (полный перечень обфусцирующих последовательностей можно найти в [13], табл. 6). В качестве деобфускатора используется предложенная в [16] и реализованная в [13] модель, основанная на оптимизирующем компиляторе, а в качестве аппроксимации A наиболее понятной версии P_0 программы P используется версия, полученная с помощью компилятора AOCC с опцией оптимизации Os (см. [13], раздел 6). Версию программы P, полученную с помощью компилятора AOCC с опцией оптимизации Os, будем обозначать $AOCC_{Os}(P_0)$. Таким образом, эффективность e и стойкость r обфусцирующей последовательности преобразований $O^t \in Q$ для программы P в рамках модели $\mathcal{M}$ вычисляется по формулам:

$$\mathrm{r}(O^t, P) = 1 - \delta_{im}\left(Im\left(\mathrm{D}\left(O^t(P)\right), AOCC_{Os}(P_0)\right)\right),$$

$$\mathrm{r}(O^t, P) = 1 - \delta_{im}\left(Im\left(\mathrm{D}\left(O^t(P)\right), AOCC_{Os}(P_0)\right)\right).$$

Таблица 1

Базовый набор обфусцирующих преобразований (столбец o($\in \mathcal{O}$) в таблице) обфускатора Hikari для программ на языке C

o($\in \mathcal{O}$)	**Описание**	$\theta(o)$
bcf	Встраивание непрозрачных предикатов	C
cff	Сглаживания графа потока управления	C
enc	Кодирование статических строк	D
fcw	Создание фиктивных функций-прокси	A
ind	Замена инструкций ветвления косвенными переходами	C
sbb	Разбиение базовых блоков	A
sub	Замена инструкций эквивалентными	D

[5] https://github.com/HikariObfuscator/Hikari (дата обращения: 13.04.2025).

Для оценки эффективности и стойкости обфусцирующих преобразований выбраны два набора программ: набор из 164 программ, использовавшихся при построении функции δ_{im} (CoreUtils, PolyBench, HashCat), и набор Small-Programs[6] из 20 программ, которые не использовались при построении этой функции. Для каждого из наборов была вычислена средняя эффективность $\mathrm{e}(O^t,\cdot)$ и средняя стойкость $\mathrm{r}(O^t,\cdot)$преобразования $O^t \in Q$ (усреднение выполнялось по всем программам соответствующего набора). Также для каждого из наборов вычислена средняя эффективность $\mathrm{e}(\theta(O^t),\cdot)$ типа преобразования $\theta(O^t)$ и средняя стойкость $\mathrm{r}(\theta(O^t),\cdot)$ этого типа. Интуитивно ожидается, что преобразование, включающее все обфусцирующие преобразования (которая далее называется all), должно быть как наиболее эффективным, так и наиболее стойким. Поэтому в работе в качестве референсных значений вычисляются описанным выше способом эффективность и стойкость последовательности all.

В табл. 2 указаны последовательности, которые для обоих наборов программ попали в группу из $N(\in \{8,16,32\})$ лучших (худших) последовательностей, имеющих наибольшее (соответственно наименьшее) значение эффективности, стойкости или и того и другого одновременно.

В табл. 3 указаны типы последовательностей (полученные на основании табл. 1), которые для обоих наборов программ попали в группу из $N(\in \{3,7,15\})$ лучших (худших) типов последовательностей, имеющих наибольшее (соответственно наименьшее) значение эффективности, стойкости или и того и другого одновременно.

Таблица 2

Обфусцирующие последовательности, входящие в N лучших (T<N>) и худших (B<N>) последовательностей, как для первого, так и для второго набора программ ($N(\in \{8,16,32\})$)

	Относительно $\mathrm{e}(O^t,\cdot)$	**Относительно** $\mathrm{r}(O^t,\cdot)$	**Относительно** $\mathrm{e}(O^t,\cdot)$ **и** $\mathrm{r}(O^t,\cdot)$
T32	all, bcf-fcw, bcf-fcw-cff, bcf-ind, bcf-ind-fcw, bcf-ind-sbb, bcf-ind-sub, bcf-sbb, bcf-sub-sbb, cff-sub-sbb, fcw-cff-sbb,fcw-sbb, ind-cff-sub, ind-sub-sbb, sbb	all, bcf-cff-sub, bcf-ind, bcf-ind-fcw, bcf-ind-sbb, bcf-ind-sub, cff, enc-bcf-fcw, enc-bcf-ind, enc-fcw-cff, enc-ind-sub, fcw-sub-sbb, ind, ind-cff-sbb, ind-fcw-sbb, sbb, sub	all, bcf-ind, bcf-ind-fcw, bcf-ind-sbb, bcf-ind-sub, sbb
B32	bcf, bcf-cff, bcf-sub, enc, enc-cff, enc-fcw-cff, enc-ind, enc-ind-cff, enc-ind-fcw, enc-ind-sbb, enc-ind-sub, fcw-cff, fcw-sub, ind-fcw, ind-fcw-cff	bcf, bcf-cff, bcf-cff-sbb, bcf-fcw-sub, bcf-sbb, bcf-sub, cff-sbb, enc, enc-bcf, enc-bcf-cff, enc-bcf-sub, enc-cff, enc-cff-sbb, enc-fcw-sub, enc-ind-sbb, enc-sbb, enc-sub-sbb	bcf, bcf-cff, bcf-sub, enc, enc-cff, enc-ind-sbb
T16	all, bcf-ind-sbb, cff-ind-sub	all, bcf-ind-fcw, bcf-ind-sbb, bcf-ind-sub, enc-bcf-fcw, enc-fcw-cff, enc-ind-sub	all, bcf-ind-sbb, bcf-ind-sub
B16	enc, enc-cff, enc-ind, enc-ind-cff	bcf-cff-sbb, enc-bcf-cff, enc-cff-sbb	—
T8	all, bcf-ind-sbb	all, bcf-ind-sbb, enc-fcw-cff	all, bcf-ind-sbb
B8	—	bcf-cff-sbb	—

[6] https://github.com/Boriskin61/small-programs (дата обращения: 13.04.2025).

Таблица 3

Типы обфусцирующих последовательностей, входящие в N лучших (T<N>) и худших (B<N>) типов последовательностей, как для первого, так и для второго набора программ (N$(\in \{3, 7, 15\})$)

	Относительно $e(\theta(O^t),\cdot)$	**Относительно** $r(\theta(O^t),\cdot)$	**Относительно** $e(\theta(O^t),\cdot)$ **и** $r(\theta(O^t),\cdot)$
T15	all, C-D-A, C-C-A, C-C-D, A, A-C-A, A-A	all, C-C-A, C-C-D, A-C-D, A-C-A, A-D-A, C-A-A, D-A-C	all, C-C-A, C-C-D, A-C-A
B15	A-C, D-A-C, D-C, A-D, D	D-A, D-D-A, C-A, D-C, D-A-D, C-D	D-C
T7	all, C-D-A, C-C-A	all, C-C-D, D-A-C	all
B7	D-C	D-C, D-A-D	D-C
T3	all, C-C-A	all, D-A-C	all
B3	—	—	—

Из табл. 2 и 3 видно, что последовательность all всегда относится к наиболее эффективным и стойким последовательностям, что соответствует интуитивным ожиданиям. Последовательность bcf-ind-sbb, вошедшая в топ-8 (T8) наиболее стойких и эффективных обфусцирующих последовательностей для обоих наборов программ (согласно табл. 2), входит также в топ-32 (T32) по эффективности и топ-8 (T8) по стойкости для обоих наборов, согласно результатам работы [13] (см. табл. 6 и 14), полученным с помощью других функций похожести. Тип C-C-A, согласно табл. 3, входит в топ-15 (T15) наиболее эффективных и стойких типов, что коррелирует с результатами работы [13], где этот тип по эффективности и стойкости входит в число лучших (см. таблицы 12 и 20 в [13]). Меньше корреляция с результатами из работы [13] проявляется в части выделения наименее эффективных и стойких преобразований. Из таблицы 3 видно только, что почти все наиболее слабые типы последовательностей в своем составе содержат преобразование типа D. В [13] преобразование такого типа также обладает наименьшей эффективностью и стойкостью.

Заключение. Наблюдения, отмеченные в предыдущем разделе, а также невысокая точность построенной функции δ_{im} (0.713) позволяют использовать ее только в качестве вспомогательной при построении более сложных функций похожести, учитывающих и другие способы представления исполняемых файлов. Например, эта функция может быть применена для пополнения арсенала показателей похожести, на основе которых строятся функции похожести в [13]. Отметим, что вместо побайтовой разности $Im(P_1) - Im(P_2)$ может использоваться другое представление пары изображений, например, побитовое исключающее “или” изображений $Im(P_1) \oplus Im(P_2)$ или их горизонтальная склейка $Im(P_1) \parallel Im(P_2)$. Это может являться одним из направлений исследования возможности совершенствования функции похожести, в основе которой лежит сравнение графических представлений исполняемых файлов. Другим направлением исследования является применение известных сверточных нейронных сетей VGG16, InceptionV3, Efficientnetv2b0, Vision Transformers, которые показали высокую точность при классификации вредоносного программного обеспечения на основе графического представления исполняемых файлов [22].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Varnovsky N. et al.* The current state of art in program obfuscations: definitions of obfuscation security // Proceedings of the Institute for system programming of the RAS. – 2014. – Vol. 26, No. 3.
2. *Garg S. et al.* Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits // 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. – 2013.
3. *Xu H. et al.* Layered obfuscation: a taxonomy of software obfuscation techniques for layered security. – 2020. – Vol. 3.

4. *BinShamlan M. H. B.M.A..Z.A.A.* The impact of control flow obfuscation technique on software protection against human attacks // First International Conference of Intelligent Computing and Engineering (ICOICE). – 2019.
5. *Halevi S. et al.* Implementing BP-obfuscation using graph-induced encoding // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. – 2017.
6. *Collberg C. T.C..L.D.* A taxonomy of obfuscating transformations. – 1997.
7. *Nagra J. C.C.* Surreptitious software: obfuscation, watermarking, and tamperproofing for software protection. – Pearson Education, 2009.
8. *Banescu S. P.A.* A tutorial on software obfuscation. – 2018. – Vol. 108.
9. *De Sutter B. et al.* Evaluation methodologies in software protection research. – 2024. – Vol. 57, No. 4.
10. *.Madou M. et al.* On the effectiveness of source code transformations for binary obfuscation // Proceedings of the International Conference on Software Engineering Research and Practice (SERP06). – 2006.
11. *Manikyam R. et al.* Comparing the effectiveness of commercial obfuscators against MATE attacks // Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering. – 2016.
12. *Schrittwieser S., Katzenbeisser S., Kinder J., Merzdovnik G., Weippl E*. Protecting software through obfuscation: Can it keep pace with progress in code analysis? // ACM Computing Surveys (CSUR). – 2016. – Vol. 49. – P. 1-37.
13. *Борисов П.Д., Косолапов Ю.В.* Способ количественного сравнения обфусцирующих преобразований // Информатика и автоматизация. – 2024. – Т. 23. – С. 684-726.
14. *Gulwani S., Polozov O., Singh R., others.* Program synthesis // Foundations and Trends® in Programming Languages. – 2017. – Vol. 4. – P. 1-119.
15. *Holder W., McDonald J.T., Andel T.R.* Evaluating optimal phase ordering in obfuscation executives // Proceedings of the 7th Software Security, Protection, and Reverse Engineering/Software Security and Protection Workshop. – 2017. – P. 1-12.
16. *Borisov P.D., Kosolapov Y.V.* On the Automatic Analysis of the Practical Resistance of Obfuscating Transformations // Automatic Control and Computer Sciences. – 2020. – Vol. 54. – P. 619-629.
17. *Borisov P.D., Kosolapov Y.V.* On the Characteristics of Symbolic Execution in the Problem of Assessing the Quality of Obfuscating Transformations // Automatic Control and Computer Sciences. – 2022. – Vol. 56. – P. 595-605.
18. *Mohsen R., Pinto A.* Evaluating Obfuscation Security: A Quantitative Approach October 2015.
19. *Lekssays A., Falah B., Abufardeh S.* A Novel Approach for Android Malware Detection and Classification using Convolutional Neural Networks // ICSOFT. – 2020. – P. 606-614.
20. *Kiger J., Ho S.S., Heydari V.* Malware binary image classification using convolutional neural networks // International Conference on Cyber Warfare and Security. – 2022. – Vol. 17. – P. 469-478.
21. *Jiang H., Polsani H., Liu Y.* DeepGray: Malware Classification Using Grayscale Images with Deep Learning // The International FLAIRS Conference Proceedings. – 2024. – Vol. 37.
22. *Ben Abdel Ouahab I., Bouhorma M., Boudhir A.A., El Aachak L.* Classification of grayscale malware images using the K-nearest neighbor algorithm // Innovations in Smart Cities Applications Edition 3: The Proceedings of the 4th International Conference on Smart City Applications 4. – 2020. – P. 1038-1050.

REFERENCES

1. *Varnovsky N. et al.* The current state of art in program obfuscations: definitions of obfuscation security, *Proceedings of the Institute for system programming of the RAS,* 2014, Vol. 26, No. 3.
2. *Garg S. et al.* Candidate Indistinguishability Obfuscation and Functional Encryption for all Circuits, *2013 IEEE 54th Annual Symposium on Foundations of Computer Science,* 2013.
3. *Xu H. et al.* Layered obfuscation: a taxonomy of software obfuscation techniques for layered security, Vol. 3, 2020.
4. *BinShamlan M. H. B.M.A..Z.A.A.* The impact of control flow obfuscation technique on software protection against human attacks, *First International Conference of Intelligent Computing and Engineering (ICOICE),* 2019.
5. *Halevi S. et al.* Implementing BP-obfuscation using graph-induced encoding, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security,* 2017.
6. *Collberg C. T.C..L.D.* A taxonomy of obfuscating transformations, 1997.
7. *Nagra J. C.C.* Surreptitious software: obfuscation, watermarking, and tamperproofing for software protection. Pearson Education, 2009.
8. *Banescu S. P.A.* A tutorial on software obfuscation, 2018, Vol. 108.
9. *De Sutter B. et al.* Evaluation methodologies in software protection research, 2024, Vol. 57, No. 4.
10. *.Madou M. et al.* On the effectiveness of source code transformations for binary obfuscation, *Proceedings of the International Conference on Software Engineering Research and Practice (SERP06),* 2006.

11. *Manikyam R. et al.* Comparing the effectiveness of commercial obfuscators against MATE attacks, *Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering,* 2016.
12. *Schrittwieser S., Katzenbeisser S., Kinder J., Merzdovnik G., Weippl E*. Protecting software through obfuscation: Can it keep pace with progress in code analysis?, *ACM Computing Surveys (CSUR),* 2016, Vol. 49, pp. 1-37.
13. *Borisov P.D., Kosolapov Yu.V.* Sposob kolichestvennogo sravneniya obfustsiruyushchikh preobrazovaniy [Method for quantitative comparison of obfuscating transformations], *Informatika i avtomatizatsiya* [Computer Science and Automation], 2024, Vol. 23, pp. 684-726.
14. *Gulwani S., Polozov O., Singh R., others.* Program synthesis, *Foundations and Trends® in Programming Languages,* 2017, Vol. 4, pp. 1-119.
15. *Holder W., McDonald J.T., Andel T.R.* Evaluating optimal phase ordering in obfuscation executives, *Proceedings of the 7th Software Security, Protection, and Reverse Engineering/Software Security and Protection Workshop,* 2017, pp. 1-12.
16. *Borisov P.D., Kosolapov Y.V.* On the Automatic Analysis of the Practical Resistance of Obfuscating Transformations, *Automatic Control and Computer Sciences,* 2020, Vol. 54, pp. 619-629.
17. *Borisov P.D., Kosolapov Y.V.* On the Characteristics of Symbolic Execution in the Problem of Assessing the Quality of Obfuscating Transformations, *Automatic Control and Computer Sciences,* 2022, Vol. 56, pp. 595-605.
18. *Mohsen R., Pinto A.* Evaluating Obfuscation Security: A Quantitative Approach October 2015.
19. *Lekssays A., Falah B., Abufardeh S.* A Novel Approach for Android Malware Detection and Classification using Convolutional Neural Networks, *ICSOFT,* 2020, pp. 606-614.
20. *Kiger J., Ho S.S., Heydari V.* Malware binary image classification using convolutional neural networks, *International Conference on Cyber Warfare and Security,* 2022, Vol. 17, pp. 469-478.
21. *Jiang H., Polsani H., Liu Y.* DeepGray: Malware Classification Using Grayscale Images with Deep Learning, *The International FLAIRS Conference Proceedings,* 2024, Vol. 37.
22. *Ben Abdel Ouahab I., Bouhorma M., Boudhir A.A., El Aachak L.* Classification of grayscale malware images using the K-nearest neighbor algorithm, *Innovations in Smart Cities Applications Edition 3: The Proceedings of the 4th International Conference on Smart City Applications 4,* 2020, pp. 1038-1050.

Борисов Петр Дмитриевич – ФГАНУ НИИ "Спецвузавтоматика"; e-mail: borisovpetr@mail.ru; г. Ростов-на-Дону, Россия; тел.: +7863201-2817; зав. лабораторией.

Косолапов Юрий Владимирович – Южный федеральный университет; e-mail: yvkosolapov@sfedu.ru; г. Ростов-на-Дону, Россия; тел.: +7863297-5111; кафедра алгебры и дискретной математики; к.т.н.; доцент.

Borisov Petr Dmitrievich – FSASE SRI "Specvuzavtomatika"; e-mail: borisovpetr@mail.ru; Rostov-on-Don, Russia; phone: +78632012817; head of the laboratory.

Kosolapov Yury Vladimirovich – Southern Federal University; e-mail: yvkosolapov@sfedu.ru; Rostov-on-Don, Russia; phone: +78632975111; the Department of Algebra and Discrete Mathematics; cand. of eng. sc.; associate professor

УДК 629.735.015 DOI 10.18522/2311-3103-2025-3-273-284

И.В. Борисов, А.С. Кузьменко, В.Е. Курьян, М.В. Курьян, Е.М. Левченко

ОПРЕДЕЛЕНИЕ ПОГРЕШНОСТЕЙ КООРДИНАТ ЦЕЛИ ПРИ МНОГОПОЗИЦИОННОЙ РАДИОЛОКАЦИИ С ИСПОЛЬЗОВАНИЕМ ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Предлагается и развивается алгебраический метод для определения координат целей и их погрешностей в составе группы беспилотных летательных аппаратов. Обоснованы основные допущения разрабатываемой модели функционирования группы беспилотных летательных аппаратов: скорости летательных аппаратов не превышают скорости звука в воздухе, а скорости целей, – не превосходят первую космическую. Представлены качественные оценки времени приёма радиолокационного сигнала для заданной пространственной погрешности координат цели, оценены требования к кварцевому генератору с целью обеспечения стабильности частоты. Сформулированы условия по количеству летательных аппаратов в группе, повышающих точность опреде-

ления местоположения цели в пространстве. Проанализированы различные виды погрешностей, возникающих при организации поиска целей скоординированной группой летательных аппаратов. Исследованы вопросы зависимости результирующей погрешности вычисления координат цели поиска от погрешности измерения расстояния между летательными аппаратами в группе и самой целью в зависимости от их взаимной пространственной ориентацией. Разработан алгоритм, проведены расчёты и анализ результатов для этой постановки задачи. Выполнено моделирование на основе предложенного алгоритма с учётом случайных координат цели в фиксированном секторе и с учётом случайных погрешностей в измеренном расстоянии между группой летательных аппаратов и объектом поиска. Представлены результаты моделирования влияния конфигурации группы беспилотных летательных аппаратов и расположения цели на погрешность определения её координат. Проведена оценка для определения координат целей и оценка погрешности развиваемого алгебраического подхода. Определены, в связи с этим, пути дальнейших исследований. Рассмотрены вопросы оценки объёма вычисления при большом числе целей. Определена область использования и эффективность предлагаемого алгоритма и метода решения задачи в целом.

Алгебраический метод; алгебраические уравнения; координаты цели; погрешности координат; погрешности радиосигнала; летательные аппараты; беспилотный летательный аппарат; группа беспилотных летательных аппаратов; математическое моделирование; сектор поиска.

I.V. Borisov, A.S. Kuzmenko, V.E. Kuryan, M.V. Kuryan, E.M. Levchenko

DETERMINATION OF TARGET COORDINATE ERRORS IN MULTI-POSITION RADAR USING GROUPS OF UNMANNED AIRCRAFT

The article proposes and develops an algebraic method for determining the coordinates of targets and their errors as part of a group of unmanned aerial vehicles. The main assumptions of the developed model of the functioning of a group of unmanned aerial vehicles: The speeds of aircraft do not exceed the speed of sound in the air, and the speeds of targets do not exceed the first space were justified. The main assumptions of the model of operation of a group of unmanned aerial vehicles: the UAV speeds do not exceed the speed of sound in the air, and the target speeds do not exceed the first space one, are justified in the article. Qualitative estimates of the radar signal reception time for a given spatial error of the target coordinates were presented. The conditions for the number of aircraft in the group are formulated, which increase the accuracy of determining the location of the target in space. The various types of errors that arise when organizing the search for targets by a group of aircraft are analyzed. The issues of dependence of the resulting error in calculating the coordinates of the search target on the error in measuring the distance between the aircraft in the group and the target itself, depending on their mutual spatial orientation, are investigated. An algorithm has been developed, calculations and analysis of the results for this task have been carried out. The simulation is based on the proposed algorithm, taking into account random coordinates of the target in a fixed sector and taking into account random errors in the measured distance between a group of aircraft and the search object. The results of modeling the influence of the configuration of a group of unmanned aerial vehicles and the location of the target on the error in determining its coordinates are presented. An assessment was carried out to determine the coordinates of the goals and an error estimate of the proposed algebraic approach. The ways of further research are determined. The issues of estimating the amount of calculation for a large number of goals are considered. The scope and effectiveness of the proposed algorithm and method for solving the problem as a whole are determined.

Algebraic method; algebraic equations; target coordinates; coordinate errors; radio signal errors; aircraft; unmanned aircraft; group of unmanned aircraft; mathematical simulation; search sector.

Введение. Задачи обороны объектов от воздушно-космического нападения и угроз со стороны моря требуют организованного применения разнородных сил и средств. В этой связи возникает актуальная задача исследования путей оптимизации боевых действий. Не повторяя анализа, выводов и постановку задач в сфере разработок по беспилотным летательным аппаратам (БПЛА), отмеченных в работе [1], заметим следующее. Необходим поиск научно обоснованных путей обеспечения заданного уровня эффективности, при минимуме стоимости выполнения поставленной задачи [2]. К отмеченным задачам тесно примыкают задачи поиска объектов и подвижных средств террористов, а также поиск терпящих бедствие во всех средах [3].

Кроме того, актуальность предлагаемых мероприятий связана, прежде всего, с необходимостью контроля больших удалённых территорий, например, арктических с помощью летательных аппаратов (ЛА) [4]. Погрешность определения направления на цель в радиолокации определяется шириной диаграммы направленности антенны [5].

Современное состояние техники радионавигации и радиолокации, контроля космического пространства, а также радиоуправления привело к созданию многопозиционных радиотехнических комплексов.

Главным образом эти комплексы стационарного, наземного базирования: стационарные РЛС типа «Cobra Dane», «Pave Paws», «Дарьял», «Даугува», «Дон –2Н». Кроме того, созданы и эксплуатируются высокопотенциальные радиолокационные станции, базирующиеся и на плавучих платформах(«Cobra Dudy») [6].

Все названные РЛС способны контролировать пространство до нескольких тысяч километров. Но всем им присущ главный недостаток – низкая живучесть и высокая стоимость [6].

Известные грунтовые, транспортируемые РЛС, например, «GBR-T», «Ground Master 403» имеют незначительную дальность обнаружения, – до 1000 км и 470 км соответственно. Их мобильность, а значит, и живучесть так же под вопросом, – они размещены на большом количестве, технически связанных, транспортных средств [6, 7].

В современных условиях развития высокоточного оружия и средств воздушно-космического нападения требуется высокая мобильность всей системы для обеспечения живучести.

В этой связи возникает задача создания многопозиционной радиолокационной системы, размещённой на БПЛА или группе БПЛА (ГБПЛА).

В интересах радиолокации в многопозиционных радиолокационных комплексах при контроле воздушно-космического пространства возможно применение как пассивных пеленгаторов в плоскости ГБПЛА, так и активных РЛС.

Однако, при пассивной локации с пространственно-разнесённой системой РЛС и с ростом скорости пеленгуемых целей, образуется только небольшая область пространства, где возможно пересечение диаграмм направленностей.

Несколько лучше обстоят дела в системе разнесённых активных РЛС на ГБПЛА. Но и здесь, с ростом скорости цели, существует аналогичная проблема. Высокоскоростная цель может и не попасть в область пересечения, например, трёх лучей диаграмм направленностей РЛС ГБПЛА, так как цель, переместившись на некоторое расстояние, может оказаться вне области пересечения. А повышение энергетического потенциала РЛС БПЛА вступает в противоречие с авиационным весом – увеличение массы и габаритов.

Поэтому существует граничное значение энергетического потенциала РЛС, при котором рассматриваемая мобильность и живучесть невозможна. Поэтому возможны следующие направления решения проблемы.

Первое, – исследования в направлении организации синхронного обзора воздушного пространства всеми РЛС группы и реализация при этом адаптивных процедур обнаружения целей в конечной области пространства.

Второе, – решение задачи подбора оптимальной конфигурации группировки ЛА (БПЛА) в зависимости от требуемой конечной погрешности, погрешности измерения прихода отраженного от цели радиолокационного импульса.

Второе направление связано с формированием боевого порядка группы.

Целью статьи является построение и анализ модели определения погрешностей координат цели при многопозиционной радиолокации с использованием группы беспилотных летательных аппаратов.

В работе ставиться задача нахождения координат цели по измерению с четырёх БПЛА.

Основная часть. Для получения зависимости погрешности определения координат цели, от конфигурации группировки БПЛА и погрешности измерения времени, необходим алгоритм, расчеты по которому привели бы к минимальной погрешности определения координат цели с учётом конфигурации ГБПЛА [8, 9].

Для определения координат целей будем рассматривать систему, состоящую из: группировки беспилотных летательных аппаратов; наземных пунктов обслуживания беспилотных летательных аппаратов (БПЛА); наземной приемо-передающей аппаратуры. Часть аппаратуры может быть установлена, например, на кораблях, что существенно повысить качество и дальность сопровождения БПЛА [5]. Скорости летательных аппаратов не превосходят скорость звука в воздухе, а скорости целей, – не превосходят первую космическую скорость [4].

Перемещением цели и группы беспилотных летательных аппаратов (ГБПЛА) за время прохождения радиолокационного импульса можно пренебречь. Для определения местоположения цели с погрешностью, не превосходящей δr необходимо измерять время приема радиолокационного импульса с погрешностью не больше δt= δr/c. Так при погрешности δr~3м, погрешность измерения времени приема импульса не должна превышать 10^{-8} с.

При дальности прямой видимости L_0 ~400 км, имеем $\Delta t=2\cdot10^{-3}$с. Для обеспечения погрешности измерения времени не больше δt в течение промежутка времени Δt, требуется иметь генератор со стабильностью частоты не хуже $\Delta\acute{\omega}/\acute{\omega}=5\cdot10^{-6}$ на интервале времени порядка нескольких миллисекунд, что легко достижимо использованием простого кварцевого генератора.

Для однозначного определения координат цели достаточно использовать один излучатель и 4 приемника радиолокационных сигналов. Приемники не должны лежать в одной плоскости [10]. Если приемников больше, чем 4, то точность определения местоположения цели возрастает [11].

Будем предполагать, что у нас имеется n приемников, например, по количеству БПЛА в группе [12]. Пусть в момент времени t координаты цели x_c,y_c,z_c, координаты i-го (i пробегает значения 1,2,3,4...n) БПЛА x_i,y_i, z_i. Обозначим L_{cl} – расстояние между целью и i -ым БПЛА, а l_{ij} – расстояние между i-ым и j-ым БПЛА.

Для обнаружения цели j-ый БПЛА излучает локационный радиосигнал в момент времени t. На i-ом БПЛА он принимается в момент времени t_{0ji}. Отраженный от цели локационный сигнал принимается на i-ом БПЛА в момент времени t_{ci}. Тогда для расстояний и времен имеем следующее соотношение [4]:

$$L_{cj}+L_{ci}-L_{ij}=c\left(t_{ci}-t_{oji}\right). \quad (1)$$

Здесь индекс i пробегает значения 1,2,3,4...n, c – скорость света. Эти общие уравнения не зависят от выбора системы координат, и справедливы в любой координатной системе, хотя явный вид уравнений зависит от выбора системы координат. Для определения трех значений координат цели x_c,y_c,z_c, у нас есть как минимум четыре алгебраических уравнения.

Эта система уравнений имеет единственное решение. Следует отметить, что трех уравнения для однозначного определения местоположения цели недостаточно.

Если мы имеем три БПЛА, то соответствующая система из трех уравнений (1), с i=1,2,3, имеет два решения симметричных относительно плоскости, проходящих через три БПЛА. Для исключения этой неоднозначности требуется четвертый БПЛА и, соответственно, четвертое уравнение. Систему уравнений для определения координат цели можно записать и в инвариантной форме.

Предположим, что первый ЛА излучает и принимает отраженный от цели сигнал. В этом случае i=j=1, $l_{ij}=0$, $L_{ci}=L_{cj}=2r_1$, где r_1 расстояние между целью и первым ЛА. Зная расстояние между целью и всеми ЛА, мы легко находим из системы (1) расстояния между вторым, третьим и четвертым ЛА. Таким образом, задача решения системы (1) сводится к определению положения цели по известным расстояниям до каждого из n ЛА координаты которых известны.

Систему уравнений (1) при известных расстояниях между ЛА и целью можно записать в декартовых координатах следующим образом:

$$(x-x_1)^2+(y-y_1)^2+(z-z_1)^2={r_1}^2. \quad (2)$$

$$(x-x_2)^2+(y-y_2)^2+(z-z_2)^2={r_2}^2. \quad (3)$$

$$(x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2 = {r_3}^2. \quad (4)$$

$$(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2 = {r_4}^2. \quad (5)$$

Для определения координат цели введём декартову систему координат следующим образом. Начало системы координат находится в точке нахождения опорного летательного аппарата 1. Ось X проходит от БПЛА 1 к БПЛА 2, ось Y перпендикулярно оси X так, что БПЛА 3 лежит в плоскости XY. Ось Z ортогональна осям X и Y и составляет с ними правую тройку координатных осей. При таком выборе системы координат имеем координаты БПЛА 1 (0,0,0), координаты БПЛА 2 (l_{12},0,0), координаты БПЛА 3 (x_3, y_3, 0), координаты БПЛА 4 (x_4, y_4, z_4).

А значит, системы координат, уравнения (2-4), будут иметь вид:

$$x^2 + y^2 + z^2 = r_1^2. \quad (6)$$

$$(x - x_2)^2 + y^2 + z^2 = r_2^2. \quad (7)$$

$$(x - x_3)^2 + (y - y_3)^2 + z^2 = r_3^2. \quad (8)$$

Вычитая из уравнения (6) уравнение (7) получаем

$$2x_2 \cdot x - x_2^2 = r_1^2 - r_2^2 \quad (9)$$

Вычитая из уравнения (6) уравнение (8) получаем

$$2x_3 \cdot x - x_3^2 + 2y_3 \cdot y - y_3^2 = r_1^2 - r_3^2 \quad (10)$$

Из (8)-(9) получаем возможные координаты цели (x_0, y_0, z_0) и $(x_0, y_0, -z_0)$

$$x_0 = \frac{x_2^2 + r_1^2 - r_2^2}{2x_2}. \quad (11)$$

$$y_0 = \frac{x_3^2 + y_3^2 + r_1^2 - r_3^2 - 2x_3^2}{2x_2}. \quad (12)$$

$$z_0 = \pm\sqrt{r_1^2 - x_0^2 + y_0^2}. \quad (13)$$

Заметим, что нахождение координат цели по измерению с трех БПЛА дают два возможных варианта симметричных относительно плоскости проходящей через эти три аппарата. Для устранения этой неоднозначности подставим значения, полученные из (11)-(13), в (5) и выберем из них те значения, при котором соотношение (5) является тождеством. Результаты моделирования представлены на рис. 1.

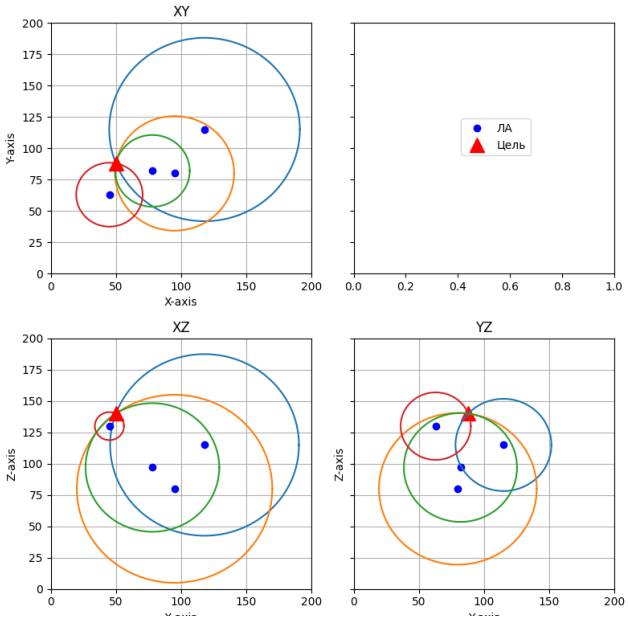


Рис. 1. Результаты моделирования взаимного положения цели и ГБПЛА

На данном рисунке изображены: цель (синяя точка), четыре БПЛА (красные точки), проекции на плоскость сферы радиусов $r_1 - r_4$ в километрах, с центрами в месте расположения БПЛА. Цель находится на пересечении всех четырех сфер.

Поскольку при всех измерениях возникают погрешности, то времена прихода сигналов на БПЛА фиксируются также с погрешностью, что эквивалентно погрешности измерения величин $r_1 - r_4$. Этот неоспоримый факт приводит к тому, что координаты цели рассчитываются с определенной погрешностью.

Погрешность определения координат цели зависит как от погрешности измерения времени прихода сигнала, так и от погрешности измерения собственных координат БПЛА, от пространственного положения боевого порядка группировки БПЛА, и от координат цели соответственно.

Далее, исследуем, как зависит результирующая погрешность вычисления координат цели от погрешности измерения расстояния между БПЛА и целью в зависимости от конфигурации ГБПЛА. Используя эти результаты, можно определить оптимальную конфигурацию группировки, её боевой порядок, при заданных погрешностях измерений и ограничении на высоты и удаление БПЛА между собой для обеспечения минимальной погрешности определения координат цели.

Для получения зависимости погрешности определения координат цели, от конфигурации группировки БПЛА и погрешности измерения времени, проводились расчеты по следующему алгоритму.

Задавались координаты БПЛА, на различных удалениях друг от друга, случайным образом задавались координаты цели в фиксированном секторе поиска, в результат измерения расстояний между БПЛА и целью вносилась случайная погрешность, после этого вычислялись координаты цели и сравнивались с истинными значениями. Результат моделирования приведен на рис. 2.

По горизонтальной оси отложена погрешность измерения времени прихода сигнала, умноженная на скорость света, по вертикальной оси отложена погрешность определения координат цели (все моделируемые параметры представлены в метрах). Расстояние между БПЛА в горизонтальной плоскости 100 км, в вертикальной плоскости один из них находился на высоте на 5 км выше остальных, максимальное расстояние от цели до ближайшего БПЛА 100 км.

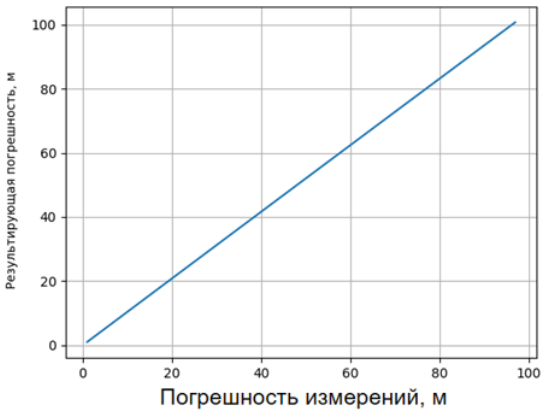


Рис. 2. Зависимость погрешности определения координат цели от погрешности измерения времени прихода сигнала

Влияние конфигурации ГБПЛА и расположения цели на погрешность определения координат с учетом задания фиксированной погрешности прихода импульса для различных расположений цели показывает зависимость на рис. 3.

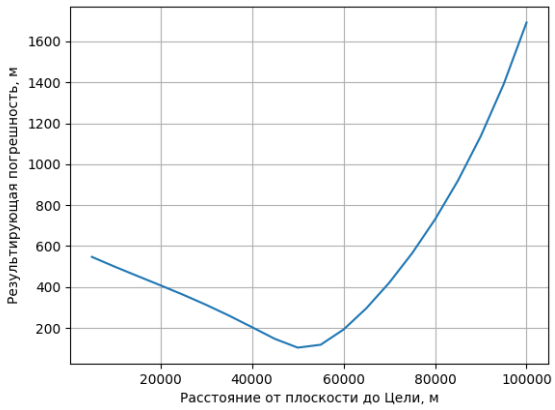


Рис. 3. Зависимость погрешности определения координат цели от расстояния между целью и плоскостью, в которой расположены три БПЛА

Из рисунка видно, что зависимость погрешности определения координат цели не монотонна. Расстояние между первым и каждым из других БПЛА 100 км. Погрешность определения времени импульсов, умноженная на скорость света составляет 100 м. Моделирование зависимости погрешности определения координат цели от ее расположения представлены на рис. 4.

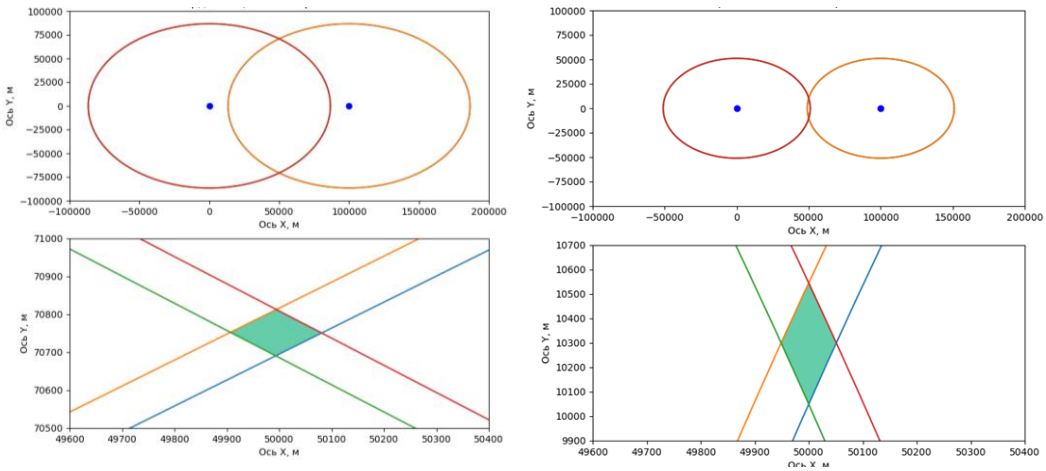


Рис. 4. Зависимости погрешности определения координат цели от ее расположения

Как видно из рис. 4, при различных удалениях цели от плоскости БПЛА угол пересечения окружностей, центры которых находятся в точках расположения ГБПЛА, а радиусы равны расстоянию между БПЛА и целью различны. Минимальная погрешность получается, как следует из анализа графиков, изображённых на рис. 4 и 5, когда угол пересечения окружностей близок к 90 градусам, а при малом угле погрешность будет заметно больше.

График зависимости погрешности определения координат цели от расстояния между ГБПЛА и погрешности измерения времени прихода импульса от цели показан на рис. 6.

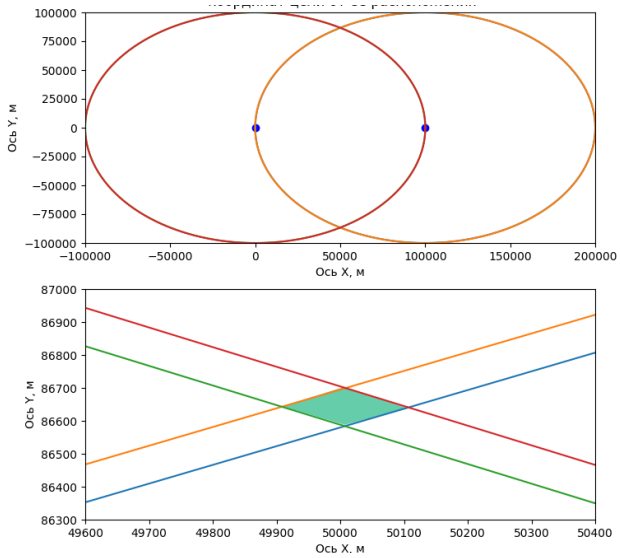


Рис. 5. Зависимости погрешности определения координат цели от ее расположения при углах пересечения окружностей близких к 90 градусам

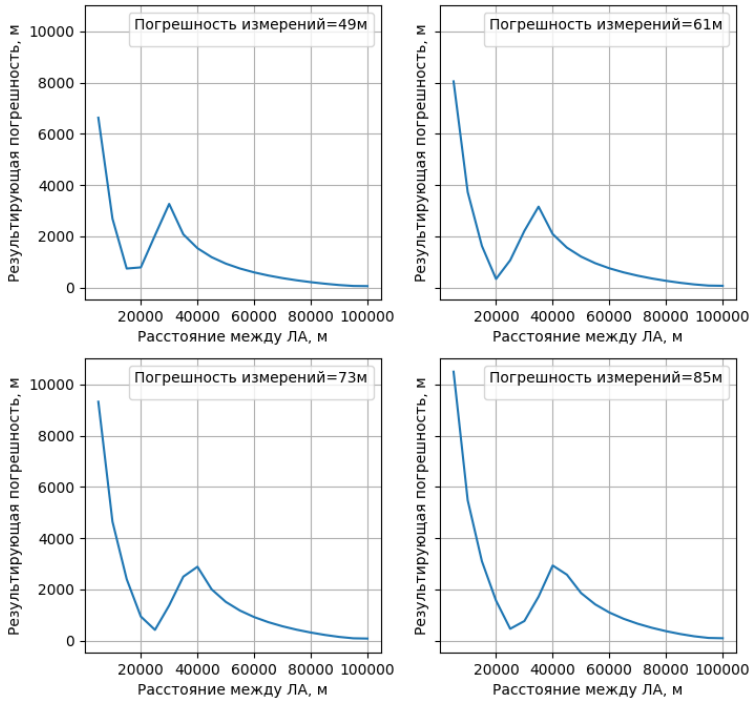


Рис. 6. График зависимости погрешности определения координат цели, в зависимости от погрешности измерений времени прихода импульсов и расстояниями между ЛА (БПЛА)

Из рис. 6 видно, что для уменьшения погрешности определения координат цели желательно иметь большее число БПЛА, находящихся в различных положениях. При этом использование данных с большего числа БПЛА позволит уменьшить погрешность определения координат цели.

Полученные результаты, по порядку величины, совпадают с оценками ошибками измерения, в 50-60 метров, приведёнными в работе. При этом, заметим, что в указанной работе оценка проведена без учёта эффекта Доплера, который вызовет несколько большую ошибку и сравняется с нашим результатом. Для уменьшения влияния эффекта Доплера на ошибку измерения на практике прибегают к увеличению девиации частоты при одновременном увеличении полосы пропускания фильтров. В этом случае соответствующая максимальная оценка сократится, по порядку величины, до полученных нами результатов [25].

Задаче подбора оптимальной конфигурации группировки ЛА (БПЛА) в зависимости от требуемой конечной погрешности, погрешности измерения прихода отраженного от цели радиолокационного импульса будут посвящены последующие работы.

Заключение. Подходы, применяемые для малоразмерных БПЛА [13] не могут быть автоматически перенесены на полноразмерные ЛА, применяемые в составе группы [14]. Применение искусственного интеллекта [15] не решает всех проблем поиска, автономного полета, и навигации даже при низкой цене за полёт [16]. Потребуется ещё достаточно много времени и средств для изучения способов дистанционного и автономного управления БПЛА, хотя уже сейчас и сделаны прорывные шаги в области искусственного интеллекта по этим направлениям [17]. Поэтому ещё достаточно предстоит приложить усилий для создания роботизированных комплексов, способных в автономном полёте собирать информацию из окружающей среды и проводить обучение бортового искусственного интеллекта [18]. Для организации группового полёта и поиска, в этой связи, важны задачи, обозначенные в [19], а также способы решения больших задач, представленные в [20], и даже начальные, дилетантские, задачи [21], не говоря уже о применении искусственного интеллекта [22].

В этой связи, заметим, что актуальны принципы формирования модели оптимизации системы роботизированных авиационных средств [23], на ряду с вопросами обеспечения безопасности каналов управления и обмены информацией в ГБПЛА [24].

Но какие бы задачи организации полёта БПЛА не решались, всегда нужно иметь ввиду, что динамика полёта имеет существенно стохастический характер. Поэтому, следует отметить, что из-за наличия погрешностей в определении времен прихода радиолокационного импульса на БПЛА система уравнений (2)-(5), вообще говоря, несовместна. Поэтому вместо решения алгебраической задачи решения системы алгебраических уравнений необходимо решать задачу поиска экстремума функции суммы разности квадратов левых и правых частей соотношений (2)-(5), что потребует итерационных процедур и методов [4]. Эти вопросы также, как и вероятностный подход [3] будут исследованы в последующих работах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Евтодьева М.Г., Целищкий С.В.* Беспилотные летательные аппараты военного назначения: тенденции в сфере разработок и производства // Пути к миру и безопасности. – 2019. – № 2 (57). – С. 104-111.
2. *Абросимов В.К.* Групповое движение интеллектуальных летательных аппаратов в антагонистических средах. – М.: Наука, 2013. – 168 с.
3. *Антюхов И.Н., Левченко Е.М.* Вероятностная модель обнаружения объектов, перемещаемых с нарушением таможенного законодательства // Академический вестник Ростовского филиала Российской таможенной академии. – 2024. – № 4 (57). – С. 19-22.
4. *Зайцев А.А., Курьян В.Е., Левченко Е.М., Родионов В.А.* Научно-методические аспекты группового управления беспилотными летательными аппаратами // «Фундаментальная наука – Военно-Морскому Флоту». Т. 3: Матер. круглого стола в рамках VIII Международного военно-морского салона (МВМС-2017). 27 июня 2017 г. – Тверь: НИИ «Центрпрограммсистем», 2018. – С. 180-187.
5. *Зайцев А.А., Курьян В.Е., Левченко Е.М., Соколов С.В.* Применение нейронных сетей в задачах исследования волновых явлений морской поверхности // Методологические основы создания и применения технологий и систем для военно-морской деятельности. Фундаментальная наука – Военно-Морскому Флоту: монография в двух томах. Т. 2. – СПб.: Изд-во СПбГЭУ, 2021. – 123 с.

6. *Леонов С.А.* Радиолокационные средства противовоздушной обороны. – М.: Военное издательство, 1988. – С. 122-133.
7. *Боев С.Ф.* Глаза и интеллект РКО. Высокопотенциальные радиолокационные станции: прошлое, настоящее и будущее // Военный парад. – 2001. – № 5 (47). – С. 58.
8. *Литвинов В.В.* Системы ракетно-космической обороны – гарант безопасности страны // Военный парад. – 2001. – № 4 (46). – С. 88-89.
9. *Алешин Б.С., Суханов В.Л., Шибаев В.М., Шнырёв А.Г.* Состояние дел и перспективы развития комплексов с беспилотными летательными аппаратами в России // Деловая слава России. – 2014. – № 3 (46). – С. 32-37.
10. *Бабушкин И.Н., Котков А.С., Растимешин Г.Д.* Интеллект группы БПЛА: анализ последних достижений и текущее развитие // Вестник новой ЭРЫ: Сб. статей. – 2024. – С. 285-299.
11. *Гончаренко В.И., Лебедев Г.Н., Кананадзе С.С. [и др.].* Задача целераспределения движущихся объектов при их наблюдении группой беспилотных летательных аппаратов // Нейрокомпьютеры и их применение: Сб. тезисов XXI Всероссийской научной конференции (Москва, 28 марта 2023 г.). – 2023. – С. 55-57.
12. *Воронов Е., Репкин А., Кусля А., Сычёв С*. Комплексный алгоритм обнаружения, идентификации и целераспределения для группы управляемых объектов // Norwegian Journal of Development of the International Science. – 2024. – № 126. – С. 41-50.
13. *Ступницкий М.М., Мырова Л.О., Королев П.С.* Рой БПЛА – новая парадигма применения малоразмерных БПЛА // Электросвязь. – 2023. – № 4. – С. 2-10.
14. *Беляев П.Ю., Зикратов И.А., Зикратова Т.В., Неверов Е.А.* Использование пчелиного алгоритма для управления роями БПЛА при мониторинге местности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сб. научных статей. XII Международная научно-техническая и научно-методическая конференция (Санкт-Петербург, 28 февраля – 01 марта 2023 г.). – 2023. – Т. 1. – С. 153-158.
15. *Li C.* Artificial Intelligence Technology in UAV Equipment // 2021 IEEE/ACIS 20th International Fall Conference on Computer and Information Science (ICIS Fall). – Xi'an, China, 2021. – P. 299-302. – DOI: 10.1109/ICISFall51598.2021.9627359.
16. *Varatharasan V., Rao A.S.S., Toutounji, E., et al.* Target Detection, Tracking and Avoidance System for Low-cost UAVs using AI-Based Approaches // 2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS). – Cranfield, UK, 2019. – P. 142-147. – DOI: 10.1109/REDUAS47371.2019.8999683.
17. *Zheng L., Ai P., and Wu Y.* Building Recognition of UAV Remote Sensing Images by Deep Learning // IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium. – Waikoloa, HI, USA, 2020. – P. 1185-1188. – DOI: 10.1109/IGARSS39084.2020.9323322.
18. *Zhang Y., McCalmon J., Peake A., et al.* A Symbolic-AI Approach for UAV Exploration Tasks // 2021 7th International Conference on Automation, Robotics and Applications (ICARA). – Prague, Czech Republic, 2021. – P. 101-105. – DOI: 10.1109/ICARA51699.2021.9376403.
19. *Wang Y., Su Z., Zhang N., and Benslimane A.* Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing // in IEEE Transactions on Network Science and Engineering. – April-June 2021. – Vol. 8, No. 2. – P. 1055-1069. – DOI: 10.1109/TNSE.2020.3014385.
20. *Kusyk J., Uyar M.U., Ma K., et al.* AI and Game Theory based Autonomous UAV Swarm for Cybersecurity // 2019 IEEE Military Communications Conference (MILCOM). – Norfolk, VA, USA, 2019. – P. 1-6. – DOI: 10.1109/MILCOM47813.2019.9020811.
21. *Molina-Padrón N., Cabrera-Almeida F., Araña V., et al.* Monitoring in Near-Real Time for Amateur UAVs Using the AIS // IEEE Access. – 2020. – Vol. 8. – P. 33380-33390. – DOI: 10.1109/ACCESS.2020.2973503.
22. *Zhang S., Wu X., Zhang G., et al.* Analysis of intelligent inspection program for UAV grid based on AI // 2020 IEEE International Conference on High Voltage Engineering and Application (ICHVE). – Xi'an, China, 2020. – P. 1-4. – DOI: 10.1109/ICHVE49031.2020.9279634.
23. *Кутахов В.П., Мещеряков Р.В.* Принципы формирования модели оптимизации системы роботизированных авиационных средств // Сб. трудов XIII Всероссийского совещания по проблемам управления ВСПУ-2019. – М.: Институт проблем управления им. В.А. Трапезникова РАН, 2019. – С. 1211-1214.
24. *Жарко Е.Ф., Промыслов В.Г., Исхакова А.Ю. и др.* Кибербезопасность беспилотных транспортных средств. Архитектура. Методы проектирования. – М.: Радиотехника, 2021. – 160 с.
25. Радилокационные устройства / под ред. В.В. Григорина-Рябова. – М.: Советское радио, 1970. – 231 с.

REFERENCES

1. *Evtod'eva M.G., Tselitskiy S.V.* Bespilotnye letatel'nye apparaty voennogo naznacheniya: tendentsii v sfere razrabotok i proizvodstva [Unmanned aerial vehicles for military purposes: trends in the field of development and production], *Puti k miru i bezopasnosti* [Paths to Peace and Security], 2019, No. 2 (57), pp. 104-111.
2. *Abrosimov V.K.* Gruppovoe dvizhenie intellektual'nykh letatel'nykh apparatov v antagonisticheskikh sredakh [Group movement of intelligent aircraft in antagonistic environments]. M.: Nauka, 2013, 168 p.
3. *Antyukhov I.N., Levchenko E.M.* Veroyatnostnaya model' obnaruzheniya ob"ektov, peremeshchaemykh s narusheniem tamozhennogo zakonodatel'stva [Probabilistic model for detecting objects moved in violation of customs legislation], *Akademicheskiy vestnik Rostovskogo filiala Rossiyskoy tamozhennoy akademii* [Academic Bulletin of the Rostov branch of the Russian Customs Academy], 2024, No. 4 (57), pp. 19-22.
4. *Zaytsev A.A., Kur'yan V.E., Levchenko E.M., Rodionov V.A.* Nauchno-metodicheskie aspekty gruppovogo upravleniya bespilotnymi letatel'nymi apparatami [Scientific and methodological aspects of group control of unmanned aerial vehicles], «Fundamental'naya nauka – Voenno-Morskomu Flotu». T. 3: Mater. kruglogo stola v ramkakh VIII Mezhdunarodnogo voenno-morskogo salona (MVMS-2017). 27 iyunya 2017 g. ["Fundamental science - Naval 3. Materials of the round table within the framework of the VIII International Naval Salon (MVMS-2017). June 27, 2017]. Tver': NII «Tsentrprogrammsistem», 2018, pp. 180-187.
5. *Zaytsev A.A., Kur'yan V.E., Levchenko E.M., Sokolov S.V.* Primenenie neyronnykh setey v zadachakh issledovaniya volnovykh yavleniy morskoy poverkhnosti [Application of neural networks in the tasks of studying wave phenomena of the sea surface], *Metodologicheskie osnovy sozdaniya i primeneniya tekhnologiy i sistem dlya voenno-morskoy deyatel'nosti. Fundamental'naya nauka – Voenno-Morskomu Flotu: monografiya v dvukh tomakh* [Methodological foundations of the creation and application of technologies and systems for naval activities. Fundamental Science to the Navy: A monograph in two volumes]. Vol. 2. Saint Petersburg: Izd-vo SPbGEU, 2021, 123 p.
6. *Leonov S.A.* Radiolokatsionnye sredstva protivovozdushnoy oborony [Radar anti-aircraft defense systems]. Moscow: Voennoe izdatel'stvo, 1988, pp. 122-133.
7. *Boev S.F.* Glaza i intellekt RKO. Vysokopotentsial'nye radiolokatsionnye stantsii: proshloe, nastoyashchee i budushchee [Eyes and intelligence of the Red Army. High-potential radar stations: past, present and future], *Voennyy parad* [Military Parade], 2001, No. 5 (47), pp. 58.
8. *Litvinov V.V.* Sistemy raketno-kosmicheskoy oborony – garant bezopasnosti strany [Rocket and space defense systems are the guarantor of the country's security], *Voennyy parad* [Military Parade], 2001, No. 4 (46), pp. 88-89.
9. *Aleshin B.S., Sukhanov V.L., Shibaev V.M., Shnyrev A.G.* Sostoyanie del i perspektivy razvitiya kompleksov s bespilotnymi letatel'nymi apparatami v Rossii [The state of affairs and prospects for the development of complexes with unmanned aerial vehicles in Russia], *Delovaya slava Rossii* [Business glory of Russia], 2014, No. 3 (46), pp. 32-37.
10. *Babushkin I.N., Kotkov A.S., Rastimeshin G.D.* Intellekt gruppy BPLA: analiz poslednikh dostizheniy i tekushchee razvitie [Intelligence of the UAV group: analysis of recent achievements and current development], *Vestnik novoy ERY: Sb. statey* [Bulletin of the new ERA: Collection of articles], 2024, pp. 285-299.
11. *Goncharenko V.I., Lebedev G.N., Kananadze S.S. [i dr.].* Zadacha tseleraspredeleniya dvizhushchikhsya ob"ektov pri ikh nablyudenii gruppoy bespilotnykh letatel'nykh apparatov [The task of target distribution of moving objects during their observation by a group of unmanned aerial vehicles], *Neyrokomp'yutery i ikh primenenie: Sb. tezisov XXI Vserossiyskoy nauchnoy konferentsii (Moskva, 28 marta 2023 g.)* [Neurocomputers and their application. Collection of abstracts of the XXI All–Russian Scientific Conference (Moscow, March 28, 2023)], 2023, pp. 55-57.
12. *Voronov E., Repkin A., Kuslya A., Sychev S.* Kompleksnyy algoritm obnaruzheniya, identifikatsii i tseleraspredeleniya dlya gruppy upravlyaemykh ob"ektov [Complex algorithm of detection, identification and target allocation for a group of controlled objects], *Norwegian Journal of Development of the International Science,* 2024, No. 126, pp. 41-50.
13. *Stupnitskiy M.M., Myrova L.O., Korolev P.S.* Roy BPLA – novaya paradigma primeneniya malorazmernykh BPLA [Swarm of UAVs – a new paradigm for the use of small-sized UAVs], *Elektrosvyaz'* [Telecommunications], 2023, No. 4, pp. 2-10.
14. *Belyaev P.Yu., Zikratov I.A., Zikratova T.V., Neverov E.A.* Ispol'zovanie pchelinogo algoritma dlya upravleniya royami BPLA pri monitoringe mestnosti [The use of a bee algorithm for controlling swarms of UAVs when monitoring terrain], *Aktual'nye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2023): Sb. nauchnykh statey. XII Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya (Sankt-Peterburg, 28 fevralya – 01 marta 2023 g.)* [Actual problems of infotelecommunications in science and education (APINO 2023). Collection of scientific articles. XII International Scientific, Technical and Scientific-methodological Conference (St. Petersburg, February 28 – March 01, 2023), 2023, Vol. 1, pp. 153-158.

15. *Li C.* Artificial Intelligence Technology in UAV Equipment, *2021 IEEE/ACIS 20th International Fall Conference on Computer and Information Science (ICIS Fall)*. Xi'an, China, 2021, P. 299-302. DOI: 10.1109/ICISFall51598.2021.9627359.
16. *Varatharasan V., Rao A.S.S., Toutounji, E., et al.* Target Detection, Tracking and Avoidance System for Low-cost UAVs using AI-Based Approaches, *2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS)*. Cranfield, UK, 2019, pp. 142-147. DOI: 10.1109/REDUAS47371.2019.8999683.
17. *Zheng L., Ai P., and Wu Y.* Building Recognition of UAV Remote Sensing Images by Deep Learning, *IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium*. Waikoloa, HI, USA, 2020, pp. 1185-1188. DOI: 10.1109/IGARSS39084.2020.9323322.
18. *Zhang Y., McCalmon J., Peake A., et al.* A Symbolic-AI Approach for UAV Exploration Tasks, *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*. Prague, Czech Republic, 2021, pp. 101-105. DOI: 10.1109/ICARA51699.2021.9376403.
19. *Wang Y., Su Z., Zhang N., and Benslimane A.* Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing, *in IEEE Transactions on Network Science and Engineering*. April-June 2021, Vol. 8, No. 2, pp. 1055-1069. DOI: 10.1109/TNSE.2020.3014385.
20. *Kusyk J., Uyar M.U., Ma K., et al.* AI and Game Theory based Autonomous UAV Swarm for Cybersecurity, *2019 IEEE Military Communications Conference (MILCOM)*. Norfolk, VA, USA, 2019, pp. 1-6. DOI: 10.1109/MILCOM47813.2019.9020811.
21. *Molina-Padrón N., Cabrera-Almeida F., Araña V., et al.* Monitoring in Near-Real Time for Amateur UAVs Using the AIS, *IEEE Access,* 2020, Vol. 8, pp. 33380-33390. DOI: 10.1109/ACCESS.2020.2973503.
22. *Zhang S., Wu X., Zhang G., et al.* Analysis of intelligent inspection program for UAV grid based on AI, *2020 IEEE International Conference on High Voltage Engineering and Application (ICHVE)*. Xi'an, China, 2020, pp. 1-4. DOI: 10.1109/ICHVE49031.2020.9279634.
23. *Kutakhov V.P., Meshcheryakov R.V.* Printsipy formirovaniya modeli optimizatsii sistemy robotizirovannykh aviatsionnykh sredstv [Principles of forming a model for optimizing a system of robotic aviation facilities], *Sb. trudov XIII Vserossiyskogo soveshchaniya po problemam upravleniya VSPU-2019* [Proceedings of the XIII All-Russian Meeting on management problems of VSPU–2019]. Moscow: Institut problem upravleniya im. V.A. Trapeznikova RAN, 2019, pp. 1211-1214.
24. *Zharko E.F., Promyslov V.G., Iskhakova A.Yu. i dr.* Kiberbezopasnost' bespilotnykh transportnykh sredstv. Arkhitektura. Metody proektirovaniya [Cybersecurity of unmanned vehicles. Architecture. Design methods]. Moscow: Radiotekhnika, 2021, 160 p.
25. Radilokatsionnye ustroystva [Radar devices], ed. by V.V. Grigorina-Ryabova. Moscow: Sovetskoe radio, 1970, 231 p.

Борисов Игорь Викторович – Южный федеральный университет; e-mail: ivborisov@sfedu.ru; г. Таганрог, Россия; кафедра летательных аппаратов; к.т.н.; доцент.

Кузьменко Алла Сергеевна – Южный федеральный университет; e-mail: akuzm@sfedu.ru; г. Таганрог, Россия; тел.: +79043437260; кафедра летательных аппаратов; к.т.н.; доцент.

Курьян Виктор Евгеньевич – Государственный научно-исследовательский институт авиационных систем; e-mail: kuryan@phystech.edu; г. Москва, Россия; к.ф.м.н.; ведущий инженер.

Курьян Михаил Викторович – Национальный исследовательский университет «Московский институт электронной техники»; e-mail: mishavbsefg@icloud.com; г. Москва, Россия; студент.

Левченко Евгений Михайлович – Южный федеральный университет; e-mail: elevche@sfedu.ru; г. Ростов-на-Дону, Россия; к.т.н.; зав. кафедрой летательных аппаратов.

Borisov Igor Viktorovich – Southern Federal University; e-mail: ivborisov@sfedu.ru; Taganrog, Russia; the Department of Aircraft; cand. of eng. sc.; associate professor.

Kuzmenko Alla Sergeevna – Southern Federal University; e-mail: akuzm@sfedu.ru; Taganrog, Russia; phone: +79043437260; the Department of Aircraft; cand. of eng. sc.; associate professor.

Kuryan Viktor Evgenievich – State Scientific Research Institute of Aviation Systems; e-mail: kuryan@phystech.edu; Moscow, Russia; cand. of phys. and math. sc; senior engineer.

Kuryan Mikhail Viktorovich – National Research University "Moscow Institute of Electronic Technology"; e-mail: mishavbsefg@icloud.com; Moscow, Russia; student.

Levchenko Evgeny Mikhailovich – Southern Federal University; e-mail: elevche@sfedu.ru; Rostov-on-Don, Russia; cand. of eng. sc.; head of the Department of Flight Devices.

УДК 623.624 DOI 10.18522/2311-3103-2025-3-285-294

Д.И. Коньков, А.А. Шмидт, Д.Н. Поляков, В.Р. Бикбулатов

ТЕОРЕТИЧЕСКОЕ ИССЛЕДОВАНИЕ ОЦЕНКИ ВЕРОЯТНОСТИ СВЯЗИ В СИСТЕМАХ С ШИРОКОПОЛОСНЫМИ СИГНАЛАМИ И ППРЧ

Статья посвящена теоретическому исследованию вероятностных характеристик систем связи с широкополосными сигналами и псевдослучайной перестройкой рабочей частоты (ППРЧ) в условиях сложной электромагнитной обстановки. Представлен аналитический аппарат для расчета вероятности связи с учетом комплексного влияния многолучевого распространения, частотно-селективных замираний и преднамеренных помех. Исследована зависимость вероятности связи от отношения сигнал/шум с применением интегральных выражений, учитывающих нормальное распределение мощностей на входе приемного устройства. Проведен математический анализ передаточной функции канала связи как комплексной характеристики, описывающей амплитудно-частотные и фазовые искажения при распространении сигнала. Разработаны теоретические модели процессов синхронизации, включающие этапы поиска сигнала, захвата и слежения, с применением функции Маркума для описания вероятности обнаружения сигнала на фоне гауссовского шума. Предложены способы оптимизации ключевых параметров системы ППРЧ, таких как период перестройки частоты, общее количество частотных каналов и ширина защитного частотного интервала. Описаны теоретические основы адаптивного управления, опирающиеся на метод максимального правдоподобия и рекурсивную фильтрацию для оценки параметров канала. Исследована энергетическая эффективность систем с ППРЧ с учетом потерь на перестройку частоты и необходимой корректировки отношения сигнал/шум. Предложен комплексный показатель качества системы связи, объединяющий вероятностные, энергетические и временные характеристики. Разработаны аналитические выражения для оценки интенсивности срыва синхронизации на основе статистического анализа экспериментальных данных и вычисления ковариационной матрицы шума измерений. Обоснована целесообразность применения эталонных сигналов для повышения достоверности измерений параметров канала связи при адаптивном управлении. Выведены соотношения для определения длительности окна синхронизации с учетом максимально допустимого времени вхождения в синхронизм и коэффициента запаса, учитывающего возможные нестабильности частоты опорных генераторов. Проанализировано влияние защитного частотного интервала на предотвращение межканальных помех и обеспечение электромагнитной совместимости соседних каналов. Представленные теоретические результаты создают научную основу для проектирования радиосистем повышенной помехозащищенности и могут быть использованы при разработке адаптивных алгоритмов управления системами ППРЧ в условиях динамически изменяющейся электромагнитной обстановки, обеспечивая баланс между надежностью передачи информации и эффективностью использования частотно-временных ресурсов системы связи.

Широкополосные сигналы; псевдослучайная перестройка рабочей частоты; ППРЧ; вероятность связи; помехозащищенность; сложная электромагнитная обстановка; многолучевое распространение; частотно-селективные замирания; синхронизация; функция Маркума; отношение сигнал/шум; передаточная функция канала; адаптивное управление; энергетическая эффективность; оптимизация параметров; межканальные помехи; электромагнитная совместимость; рекурсивная фильтрация; метод максимального правдоподобия.

D.I. Konkov, A.A. Shmidt, D.N. Polyakov, V.R. Bikbulatov

THEORETICAL STUDY OF ESTIMATING THE PROBABILITY OF A CONNECTION IN SYSTEMS WITH BROADBAND SIGNALS AND FHSS

The article is devoted to a theoretical study of the probabilistic characteristics of communication systems with broadband signals and pseudorandom tuning of the operating frequency in a complex electromagnetic environment. An analytical tool for calculating the communication probability is presented, taking into account the complex effects of multipath propagation, frequency-selective fading, and intentional interference. The dependence of the communication probability on the signal-to-noise ratio is investigated using integral expressions that take into account the normal power distribution at the input of the receiving device. A mathematical analysis of the transmission function of the communication channel as a complex characteristic describing the amplitude-frequency and phase distortions during signal propaga-

tion is performed. Theoretical models of synchronization processes are developed, including the stages of signal search, capture, and tracking, using the Markum function to describe the probability of signal detection against the background of Gaussian noise. Methods for optimizing the key parameters of the RFP system, such as the frequency tuning period, the total number of frequency channels, and the width of the protective frequency interval, are proposed. The theoretical foundations of adaptive control based on the maximum likelihood method and recursive filtering for estimating the parameters of the channel\are described. The energy efficiency of systems with RFP is studied, taking into account the frequency tuning losses and the necessary adjustment of the signal-to-noise ratio. A comprehensive indicator of the quality of a communication system combining probabilistic, energy, and time characteristics of the system is proposed. Analytical expressions are developed for estimating the intensity of synchronization failure based on statistical analysis of experimental data and calculation of the covariance matrix of measurement noise. The expediency of using reference signals to increase the reliability of measurements of communication channel parameters in adaptive control of the system is justified. Relations are derived for determining the duration of the synchronization window, taking into account the maximum allowable time of entering synchronism and the margin factor, which takes into account possible frequency instabilities of the reference generators. The influence of the protective frequency interval on preventing inter-channel interference and ensuring electromagnetic compatibility of neighboring channels is analyzed. The presented theoretical results provide a scientific basis for the design of radio systems with increased noise immunity and can be used in the development of adaptive algorithms for controlling RF control systems in a dynamically changing electromagnetic environment, ensuring a balance between the reliability of information transmission and the efficiency of using frequency-time resources of the communication system.

Broadband signals; frequency hopping spread spectrum; FHSS; communication probability; interference immunity; complex electromagnetic environment; multipath propagation; frequency-selective fading; synchronization; Marcum function; signal-to-noise ratio; channel transfer function; adaptive control; energy efficiency; parameter optimization; inter-channel interference; electromagnetic compatibility; recursive filtering; maximum likelihood method.

Введение. В современных системах радиосвязи особую актуальность приобретает задача обеспечения надежной связи в условиях сложной электромагнитной обстановки. Наличие естественных и преднамеренных помех, многолучевое распространение сигналов, а также требования по электромагнитной совместимости создают существенные трудности при организации радиосвязи [1]. В данном контексте значительный интерес представляет теоретический анализ вероятности связи для систем, использующих широкополосные сигналы и сигналы с псевдослучайной перестройкой рабочей частоты.

Современные исследования в области радиосвязи показывают [2–5], что применение широкополосных сигналов и систем с ППРЧ позволяет существенно повысить помехозащищенность каналов связи. При этом особый интерес представляет случай, когда распределение мощностей полезного сигнала и помех на входе приемного устройства подчиняется нормальному закону распределения, что часто встречается на практике.

Теоретические основы анализа широкополосных сигналов. Фундаментальным параметром систем широкополосной связи является ширина полосы частот ΔF [6], представляющая собой разность между верхней и нижней границами рабочего диапазона частот. В условиях нормального распределения мощностей сигнала и помех вероятность связи для широкополосного сигнала может быть представлена в виде интегрального выражения:

$$P_{\text{св}} = \frac{1}{\Delta F}\int_{f_{\min}}^{f_{\max}} \Phi\left(\frac{\bar{z}(f)-z_{\text{тр}}}{z}\right) H(f)df, \quad (1)$$

В данном выражении функция Ф(x) представляет собой интеграл вероятности, а $\bar{z}(f)$ характеризует отношение медианных значений мощности сигнала к мощности помехи на входе приемного устройства. Параметр $z_{\text{тр}}$ определяет требуемое превышение сигнала над помехой, необходимое для обеспечения заданного качества связи. Среднеквадратическое отклонение $_z$ отражает степень флуктуаций отношения сигнал/помеха в канале связи.

Передаточная функция канала $H(f)$ представляет собой комплексную характеристику, учитывающую амплитудно-частотные и фазо-частотные искажения сигнала при его распространении:

$$H(f) = A(f)e^{j\ (f)}, \tag{2}$$

где $A(f)$ характеризует амплитудно-частотную характеристику канала, а (f) отражает фазовые искажения, вносимые каналом связи.

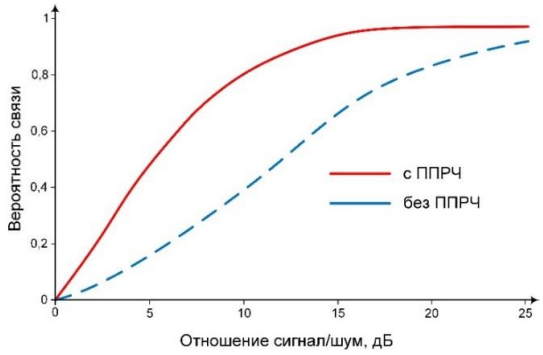


Рис. 1. График зависимости вероятности связи от отношения сигнал/шум

На рис. 1 представлены экспериментальные характеристики помехоустойчивости системы связи с ППРЧ и без нее. Как видно из графика, применение ППРЧ позволяет существенно снизить вероятность ошибки при одинаковом отношении сигнал/шум.

Особенности систем с псевдослучайной перестройкой рабочей частоты. Системы с псевдослучайной перестройкой рабочей частоты представляют собой сложные радиотехнические комплексы, характеризующиеся специфическими вероятностными характеристиками [7]. В основе их функционирования лежит принцип быстрого изменения несущей частоты передаваемого сигнала по псевдослучайному закону, что обеспечивает высокую помехозащищенность канала связи.

Математическое описание таких систем требует учета множества параметров, ключевым из которых является общее количество частотных каналов M, определяемое отношением всей выделенной полосы частот к ширине одного частотного канала:

$$M = \frac{\Delta F}{\Delta f_k}. \tag{3}$$

Обобщенная структурная схема системы ППРЧ представлена на рис. 2, где отражены основные функциональные блоки передающей части и их взаимосвязи.

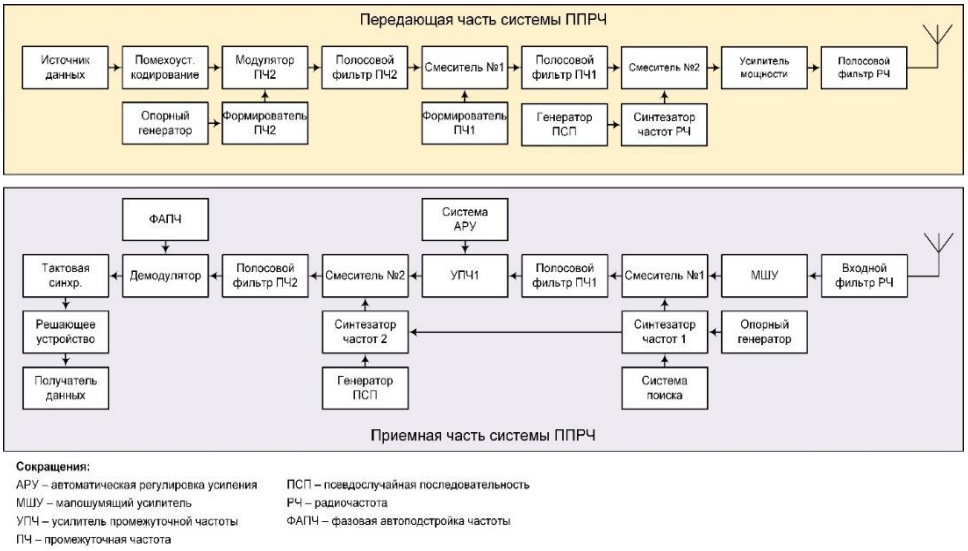


Рис. 2. Обобщенная структурная схема системы ППРЧ

При этом ширина частотного канала Δf_k представляет собой сумму ширины спектра информационного сигнала B и защитного частотного интервала $\Delta f_{зи}$:

$$\Delta f_k = B + \Delta f_{зи}. \quad (4)$$

Защитный частотный интервал необходим для предотвращения межканальных помех и обеспечения электромагнитной совместимости соседних каналов [8]. Его величина выбирается исходя из спектральных характеристик передатчика и требований к избирательности приемного устройства.

Теоретические аспекты синхронизации в системах ППРЧ. Одним из ключевых факторов, определяющих эффективность систем с ППРЧ, является качество синхронизации приемной и передающей сторон. Вероятность успешной синхронизации может быть описана следующим математическим выражением [9]:

$$P_{\text{синхр}} = (1 - P_{\text{ош}})^L \cdot \frac{T_{\text{ос}}}{T_{\text{пч}}}. \quad (5)$$

Данное выражение учитывает вероятность ошибки на бит в синхропоследовательности $P_{\text{ош}}$, которая зависит от отношения сигнал/шум в канале связи и выбранного метода модуляции. Длина синхропоследовательности L выбирается как компромисс между надежностью синхронизации и временными затратами на её установление [10, 11]. Отношение длительности окна синхронизации $T_{\text{ос}}$ к периоду перестройки частоты $T_{\text{пч}}$ характеризует временную эффективность процесса синхронизации.

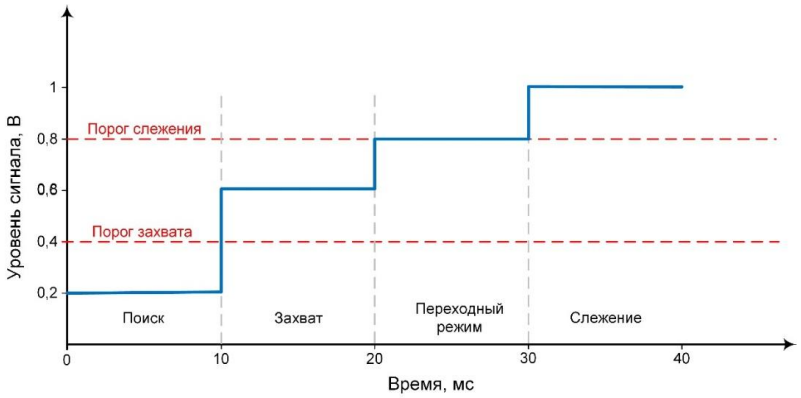


Рис. 3. Временная диаграмма процесса синхронизации

На рис. 3 представлена временная диаграмма процесса синхронизации системы ППРЧ, отражающая три основных этапа установления и поддержания синхронизации. На интервале времени (t_1–t_2) осуществляется поиск сигнала, длительность которого определяется выражением:

$$\text{T}_{\text{поиск}} = M \cdot T_x \cdot P_{\text{ош}}, \quad (6)$$

где M – число частотных каналов; T_x – длительность шага поиска; $P_{\text{ош}}$ – вероятность ошибки обнаружения сигнала. Вероятность ошибки обнаружения сигнала определяется через отношение сигнал/шум на входе приемного устройства и порог обнаружения с использованием функции Маркума:

$$P_{\text{ош}} = Q\left(\sqrt{2\ ^2},\ \sqrt{2}\right), \quad (7)$$

где $Q(a,b)$ – функция Маркума; h^2 – отношение сигнал/шум по мощности; – пороговый уровень обнаружения. Функция Маркума представляет собой обобщение функции вероятности для комплексной огибающей сигнала и определяется интегральным выражением:

$$Q(a,b) = \int_b x \exp\left(-\frac{x^2 + a^2}{2}\right) I_0(ax)dx, \quad (8)$$

где $I_0(x)$ – модифицированная функция Бесселя первого рода нулевого порядка. Использование функции Маркума обусловлено тем, что при обнаружении сигнала на фоне гауссовского шума огибающая сигнала на выходе оптимального приемника имеет распределение Райса.

В интервале (t_2–t_3) происходит захват синхронизации, время которого зависит от длины синхропоследовательности L и периода перестройки частоты $T_{\text{пч}}$:

$$T_{\text{захв}} = L \cdot T_{\text{пч}}. \quad (9)$$

На заключительном этапе (t_3–t_4) система переходит в режим слежения, минимальная длительность которого определяется выражением:

$$T_{\text{слеж}} \geq T_{\text{пч}} \cdot (1 + k_{\text{зап}}), \quad (10)$$

где $K_{\text{зап}}$ – коэффициент запаса, обеспечивающий устойчивость синхронизации в условиях помех.

Как видно из временной диаграммы, наиболее длительным является этап поиска сигнала, что обусловлено необходимостью просмотра всей полосы частот системы. Этап захвата характеризуется снижением уровня сигнала рассогласования по мере установления синхронизации. В режиме слежения наблюдаются минимальные флуктуации сигнала рассогласования, определяемые точностью работы системы фазовой автоподстройки частоты.

Комплексная оценка вероятности связи в системах ППРЧ. При анализе систем с ППРЧ итоговая вероятность связи [12, 13] представляет собой произведение трех вероятностных характеристик:

$$P_{\text{св.ППРЧ}} = P_{\text{св}} \cdot P_{\text{синхр}} \cdot \frac{1}{M}. \quad (11)$$

В данном выражении множитель $1/M$ отражает вероятность правильного выбора частотного канала в конкретный момент времени при условии равновероятного использования всех доступных каналов системы связи.

Теоретические основы оптимизации параметров системы ППРЧ. В процессе проектирования систем с псевдослучайной перестройкой рабочей частоты существенное значение приобретает задача оптимизации параметров системы. Фундаментальным параметром, требующим особого внимания, является период перестройки частоты $T_{\text{пч}}$. Его выбор представляет собой сложную оптимизационную задачу, учитывающую противоречивые требования к системе связи [12].

Оптимальное значение периода перестройки может быть определено из условия максимизации вероятности связи:

$$\frac{\partial P_{\text{св.ППРЧ}}}{\partial T_{\text{пч}}} = 0. \quad (12)$$

При этом необходимо учитывать, что вероятность синхронизации с учетом возможного срыва описывается более сложным выражением:

$$P_{\text{синхр}} = (1 - P_{\text{ош}})^L \cdot \frac{T_{\text{ос}}}{T_{\text{пч}}} \cdot e^{-\lambda T_{\text{пч}}}, \quad (13)$$

где представляет собой параметр, характеризующий интенсивность срыва синхронизации в системе связи.

Интенсивность срыва синхронизации определяется путем статистического анализа экспериментальных данных в реальных условиях функционирования системы связи. При использовании метода максимального правдоподобия оценка интенсивности срыва может быть найдена как:

$$= \frac{1}{N} \sum_{i=1}^{N} \frac{1}{\Delta t_i}, \quad (14)$$

где Δt_i – интервалы времени между последовательными срывами синхронизации; N – общее число зарегистрированных срывов. Достоверность оценки характеризуется дисперсией:

$$^2 = \frac{1}{N(N-1)} \sum_{i=1}^{N} \left(\frac{1}{\Delta t_i} - \quad \right)^2. \tag{15}$$

Исследование влияния характеристик канала связи. Передаточная функция канала в реальных условиях формируется под влиянием множества [13] факторов и может быть представлена как произведение частных передаточных функций:

$$H(f) = H_{\text{мн}}(f) \cdot H_{\text{зам}}(f) \cdot H_{\text{доп}}(f). \tag{16}$$

Данное выражение учитывает влияние многолучевого распространения $H_{\text{мн}}(f)$, замираний сигнала $H_{\text{зам}}(f)$ и дополнительных искажений $H_{\text{доп}}(f)$, вносимых аппаратурой связи.

Составные элементы передаточной функции канала определяются следующим образом. Функция многолучевого распространения может быть представлена в виде:

$$H_{\text{мн}}(f) = \sum_{i=1}^{L} \; _i \, e^{-j2\pi f \tau_i}. \tag{17}$$

где $_i$ и τ_i – амплитуды и задержки отдельных лучей; L – общее число учитываемых лучей.

Функция замираний при рэлеевской модели описывается выражением:

$$H_{\text{зам}}(f) = \sqrt{\frac{2}{^2}} \exp\left(-\frac{|H(f)|^2}{2\sigma^2} \right), \tag{18}$$

где ^{2} – дисперсия замираний.

Особую значимость для систем с ППРЧ приобретает анализ вероятности связи в канале с частотно-селективными замираниями:

$$P_{\text{св}} = \frac{1}{\Delta F} \int_{f\min}^{f\max} \Phi\left(\frac{\bar{z}(f) - z_{\text{тр}}}{z} \right) \cdot |H(f)|^2 \cdot e^{-\ |H(f)|^2} df, \tag{19}$$

где яв ляется параметром, характеризующим интенсивность замираний в канале связи.

Интенсивность замираний в канале связи связана со статистическими характеристиками огибающей принимаемого сигнала. Для релеевского закона распределения:

$$= \sqrt{\frac{\pi}{4}} \frac{\sigma_R}{\bar{R}}, \tag{20}$$

где $_R$ – среднеквадратическое отклонение огибающей; $\bar{R}$ – среднее значение огибающей. При этом параметр м ожет быть оценен через измеряемую глубину замираний:

$$\beta = \sqrt{-ln(1 - P_З) \cdot \frac{\pi}{4}}, \tag{21}$$

где $P_з$ – вероятность превышения заданного уровня замираний.

Энергетическая эффективность систем связи с ППРЧ. Существенным аспектом анализа систем с ППРЧ является оценка их энергетической эффективности [14]. Средние энергетические потери на перестройку частоты могут быть определены следующим выражением:

$$L_э = 10 \lg\left(1 + \frac{T_п}{T_{\text{пч}}} \right), \tag{22}$$

где $T_{\text{п}}$ представляет собой время перестройки синтезатора частоты.

При этом требуемое отношение сигнал/шум должно быть скорректировано с учетом этих потерь:

$$z_{\text{тр. эфф}} = z_{\text{тр}} + L_э. \tag{23}$$

Практические аспекты синхронизации систем ППРЧ и их теоретическое обоснование. Реализация систем синхронизации в ППРЧ представляет собой комплексную техническую задачу, требующую детального теоретического анализа [15]. Одним из ключевых параметров, определяющих эффективность синхронизации, является длина синхропоследовательности L, которая может быть определена через требуемую вероятность правильной синхронизации:

$$L = \frac{\log(1 - P_{\text{тр}})}{\log(P_{\text{ош}})}, \tag{24}$$

где $P_{\text{тр}}$ представляет собой требуемую вероятность правильной синхронизации, а $P_{\text{ош}}$ характеризует вероятность ошибки на бит в синхропоследовательности.

Существенное значение имеет также длительность окна синхронизации, определяемая с учетом максимально допустимого времени вхождения в синхронизм:

$$T_{\text{ос}} = \frac{T_{\text{макс}}}{K_{\text{зап}}}. \tag{25}$$

В данном выражении $K_{\text{зап}}$ представляет собой коэффициент запаса, учитывающий возможные нестабильности частоты опорных генераторов системы связи.

Комплексный анализ характеристик системы. Эффективность системы с ППРЧ может быть охарактеризована интегральным показателем качества:

$$Q = P_{\text{св. ППРЧ}} \cdot \frac{1}{L_{\text{э}}} \cdot \frac{T_{\text{пч}}}{T_n}. \tag{26}$$

Данный показатель учитывает вероятность связи, энергетические потери и временную эффективность системы. При этом оптимизация параметров системы должна проводиться с учетом максимизации данного показателя качества [16].

Теоретические основы адаптивного управления. В условиях изменяющейся помеховой обстановки особую значимость приобретает адаптивное управление параметрами системы [17, 18]. Вероятность связи при адаптивном управлении может быть представлена как:

$$P_{\text{св. адапт}} = \int_0 |H(f)|^2 \, P_{\text{ош. адапт}} df, \tag{27}$$

где $P_{\text{ош. адапт}}$ характеризует вероятность ошибки адаптивного управления, определяемую точностью оценки параметров канала связи:

$$P_{\text{ош. адапт}} = \frac{1}{{}_{\Delta}\sqrt{2}} \int_{-} \exp\left(- \frac{\left(\hat{} - \right)^2}{2 \, {}^{2}_{\Delta}} \right) d \ , \tag{28}$$

где h и $\hat{}$ представляют собой истинное и оценочное значения параметра канала соответственно, а ${}_{\Delta}$ характеризует дисперсию ошибки оценивания.

Истинное значение параметра канала h определяется в процессе калибровочных измерений:

$$= \frac{1}{T} \int_0^T |H(f,t)|^2 \, dt, \tag{29}$$

где T – интервал измерения, выбираемый исходя из требуемой точности оценки параметра канала.

Для повышения достоверности измерений используются эталонные сигналы:

$${}_{\text{эт}} = \frac{S_{\text{вых}}(f)}{S_{\text{эт}}(f)}, \tag{30}$$

где $S_{\text{вых}}(f)$ и $S_{\text{эт}}(f)$ – спектральные характеристики выходного и эталонного сигналов соответственно.

Оценочное значение параметра канала $\hat{}$ формируется в процессе работы системы на основе метода максимального правдоподобия:

$$\hat{} = \arg\max \left\{ \frac{1}{{}_{n}\sqrt{2}} \left(- \frac{|y(t) - \ \cdot s(t)|^2}{2 \, {}^{2}_{n}} \right) \right\}, \tag{31}$$

где $y(t)$ – принимаемый сигнал; $s(t)$ – передаваемый сигнал; σ_n^2 – дисперсия шума в канале связи [19].

Уточнение оценки производится с помощью рекурсивного фильтра:

$$\hat{}_{k+1} = \hat{}_k + K_k\left(y_k - H_k\,\hat{}_k\right) \quad (32)$$

с коэффициентом усиления:

$$K_k = P_k H_k^T (H_k P_k H_k^T + R_k)^{-1}, \quad (33)$$

где R_k – ковариационная матрица шума измерений.

Дисперсия ошибки оценивания определяется соотношением:

$$\overset{2}{\Delta} = \frac{1}{N}\sum_{i=1}^{N}\left(_i - \hat{}_i\right)^2, \quad (34)$$

где N – количество измерений, используемых для статистической оценки точности.

Данный математический аппарат позволяет обеспечить эффективное адаптивное управление параметрами системы ППРЧ с учетом изменяющихся условий функционирования канала связи.

Заключение. Теоретическое исследование вероятности связи в системах с ППРЧ позволяет сформулировать основные принципы построения таких систем и определить пути их оптимизации. Полученные математические выражения создают основу для проектирования высокоэффективных систем связи [20], способных функционировать в сложной помеховой обстановке.

Представленный теоретический аппарат может быть использован при разработке новых методов адаптивного управления параметрами системы ППРЧ и алгоритмов повышения энергетической эффективности передачи информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Сикорский А.Б.* Методы повышения помехоустойчивости систем подвижной сотовой связи в условиях преднамеренных помех // Проблемы информационной безопасности. Компьютерные системы. – 2001. – № 3.
2. *Макаренко С.И., Иванов М.С., Попов С.А.* Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты: монография. – СПб.: Свое издательство, 2013. – 166 с.
3. *Борисов В.И., Зинчук В.М., Лимарев А.Е.* Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / под ред. В.И. Борисова. –2-е изд., перераб. и доп. – М.: РадиоСофт, 2008. – 512 с.
4. *Борисов В.И., Зинчук В.М., Лимарев А.Е., Мухин Н.П., Нахмансон Г.С.* Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / под ред. В.И. Борисова. – М.: Радио и связь, 2003. – 640 с.
5. *Simon M.K., Omura J.K., Scholtz R.A., Levitt B.K.* Spread spectrum communication. – Vol. 3. – Rockwille, MD: Computer Science Press, 1985.
6. *Агеев А.В.* Исследование и разработка алгоритмов приема сигналов ППРЧ в каналах с памятью: дисс. … канд. техн. наук по спец. 05.12.13. – Самара: ПовГУТИ, 2009. – 122 с.
7. *Чуднов А.М.* Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации. – 1991. – Т. 27, № 3. – С. 57-65.
8. *Борисов В.И., Зинчук В.М., Мухин Н.П.* Помехоустойчивость систем радиосвязи с расширением спектра сигналов // Теория и техника радиосвязи. – 1993. – Вып. 1.
9. *Чуднов А.М.* Помехоустойчивость линий и сетей связи в условиях оптимизированных помех. – Л.: ВАС, 1986. – 84 с.
10. *Torrieri D.J.* The Information-Bit Error for Block Codes // IEEE Trans. – 1984. – Vol. COM-32, No. 4.
11. *Torrieri D.J.* Principles of Spread-Spectrum Communication Systems. – Publisher Springer US, 2005. – 444 p. – ISBN 978-0-387-22783-2.
12. *Борисов В.И.* Помехозащищенность систем радиосвязи: основы теории и принципы реализации. – М.: Наука, 2009. – 358 с. – ISBN 978-5-02036943-6 (в пер.).
13. *Богданов А.Е.* Разработка системы передачи информации для локальных сетей связи, работающих в сложной помеховой обстановке: дисс. … канд. техн. наук по спец. 05.12.13. – Владимир: ОАО «Владимирское КБ «Радиосвязи», 2005. – 144 с.
14. *Pickholtz R., Schilling D. and Milstein L.* Theory of Spread-Spectrum Communications - A Tutorial // IEEE Transactions on Communications. – 1982. – Vol. 30, No. 5. – P. 855-884.

15. *Mark K. Cornwall, Harry Price Haas.* Frequency hopping spread spectrum system with high sensitivity tracking and synchronization for frequency unstable signals. Patent US6934316B2, 23.08.2005.
16. *Simon M.K.* Spread Spectrum Communication. Electronic Edition. Inc., 2002. – 1115 p.
17. *Lee J., French R., Miller L.* Probability of Error Analyses of a BFSK Frequency-Hopping System with Diversity Under Partial-Band Jamming Interference – Part I: Performance of Square-Law Linear Combining Soft Decision Receiver // IEEE Transactions on Communications. – 1984. – Vol. 32, No. 6. – P. 645-653.
18. *Liu Y., Li X., Xu X.* A Broadband Transmission Technology Based on FFH-OFDM // 2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS). – 2018.
19. *Чуднов А.М.* О минимаксных алгоритмах формирования и приема сигналов // Проблемы передачи информации. – 1986. – Т. 22, № 4. – С. 49-54.
20. *Torrieri D.J.* Fundamental limitations on repeater jamming of frequency-hopping communications // IEEE Journal on Selected Areas in Communications. – 1989. – Vol. 7, No. 24. – P. 569-575.

REFERENCES

1. *Sikorskiy A.B.* Metody povysheniya pomekhoustoychivosti sistem podvizhnoy sotovoy svyazi v usloviyakh prednamerennykh pomekh [Methods for increasing the noise immunity of mobile cellular communication systems under deliberate interference], *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Problems of Information Security. Computer Systems], 2001, No. 3.
2. *Makarenko S.I., Ivanov M.S., Popov S.A.* Pomekhozashchishchennost' sistem svyazi s psevdosluchaynoy perestroykoy rabochey chastoty: monografiya [Noise immunity of communication systems with pseudo-random frequency hopping: monograph]. Saint Petersburg: Svoe izdatel'stvo, 2013, 166 p.
3. *Borisov V.I., Zinchuk V.M., Limarev A.E.* Pomekhozashchishchennost' sistem radiosvyazi s rasshireniem spektra signalov metodom psevdosluchaynoy perestroyki rabochey chastoty [Noise immunity of radio communication systems with signal spectrum expansion by the method of pseudo-random frequency tuning], ed. by V.I. Borisova. 2nd ed. Moscow: RadioSoft, 2008, 512 p.
4. *Borisov V.I., Zinchuk V.M., Limarev A.E., Mukhin N.P., Nakhmanson G.S.* Pomekhozashchishchennost' sistem radiosvyazi s rasshireniem spektra signalov modulyatsiey nesushchey psevdosluchaynoy posledovatel'nost'yu [Noise immunity of radio communication systems with signal spectrum expansion by carrier modulation with a pseudo-random sequence], ed. by V.I. Borisova. Moscow: Radio i svyaz', 2003, 640 p.
5. *Simon M.K., Omura J.K., Scholtz R.A., Levitt B.K.* Spread spectrum communication, Vol. 3. Rockwille, MD: Computer Science Press, 1985.
6. *Ageev A.V.* Issledovanie i razrabotka algoritmov priema signalov PPRCh v kanalakh s pamyat'yu: diss. … kand. tekhn. nauk po spets. 05.12.13 [Research and development of algorithms for receiving frequency hopping signals in channels with memory: cand. of eng. sc. diss. in specialty 05.12.13]. Samara: PovGUTI, 2009, 122 p.
7. *Chudnov A.M.* Teoretiko-igrovye zadachi sinteza algoritmov formirovaniya i priema signalov [Game-theoretic problems of synthesizing algorithms for generating and receiving signals], *Problemy peredachi informatsii* [Problems of Information Transmission], 1991, Vol. 27, No. 3, pp. 57-65.
8. *Borisov V.I., Zinchuk V.M., Mukhin N.P.* Pomekhoustoychivost' sistem radiosvyazi s rasshireniem spektra signalov [Noise immunity of radio communication systems with signal spectrum expansion], *Teoriya i tekhnika radiosvyazi* [Theory and Technology of Radio Communication], 1993, Issue 1.
9. *Chudnov A.M.* Pomekhoustoychivost' liniy i setey svyazi v usloviyakh optimizirovannykh pomekh [Noise immunity of communication lines and networks under optimized noise conditions]. L.: VAS, 1986, 84 p.
10. *Torrieri D.J.* The Information-Bit Error for Block Codes, *IEEE Trans*., 1984, Vol. COM-32, No. 4.
11. *Torrieri D.J.* Principles of Spread-Spectrum Communication Systems. Publisher Springer US, 2005, 444 p. ISBN 978-0-387-22783-2.
12. *Borisov V.I.* Pomekhozashchishchennost' sistem radiosvyazi: osnovy teorii i printsipy realizatsii [Interference immunity of radio communication systems: fundamentals of theory and principles of implementation]. Moscow: Nauka, 2009, 358 p. ISBN 978-5-02036943-6 (v per.).
13. *Bogdanov A.E.* Razrabotka sistemy peredachi informatsii dlya lokal'nykh setey svyazi, rabotayushchikh v slozhnoy pomekhovoy obstanovke: diss. … kand. tekhn. nauk po spets. 05.12.13 [Development of an information transmission system for local communication networks operating in a complex interference environment: cand. of eng. sc. diss. in specialty 05.12.13]. Vladimir: OAO «Vladimirskoe KB «Radiosvyazi», 2005, 144 p.

14. *Pickholtz R., Schilling D. and Milstein L.* Theory of Spread-Spectrum Communications - A Tutorial, *IEEE Transactions on Communications,* 1982, Vol. 30, No. 5, pp. 855-884.
15. *Mark K. Cornwall, Harry Price Haas.* Frequency hopping spread spectrum system with high sensitivity tracking and synchronization for frequency unstable signals. Patent US6934316B2, 23.08.2005.
16. *Simon M.K.* Spread Spectrum Communication. Electronic Edition. Inc., 2002, 1115 p.
17. *Lee J., French R., Miller L.* Probability of Error Analyses of a BFSK Frequency-Hopping System with Diversity Under Partial-Band Jamming Interference – Part I: Performance of Square-Law Linear Combining Soft Decision Receiver, *IEEE Transactions on Communications,* 1984, Vol. 32, No. 6, pp. 645-653.
18. *Liu Y., Li X., Xu X.* A Broadband Transmission Technology Based on FFH-OFDM, *2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS),* 2018.
19. *Chudnov A.M.* O minimaksnykh algoritmakh formirovaniya i priema signalov [On minimax algorithms for signal generation and reception], *Problemy peredachi informatsii* [Problems of Information Transmission], 1986, Vol. 22, No. 4, pp. 49-54.
20. *Torrieri D.J.* Fundamental limitations on repeater jamming of frequency-hopping communications, *IEEE Journal on Selected Areas in Communications,* 1989, Vol. 7, No. 24, pp. 569-575.

Коньков Денис Иванович – Научно-исследовательский цент Военной академии связи; e-mail: den/konkov/94@mail.ru; г. Санкт-Петербург, Россия; тел.: +79537321643; адъюнкт.

Шмидт Артур Андреевич – Научно-исследовательский цент Военной академии связи; e-mail: shmidt.artur2011@yandex.ru; г. Санкт-Петербург, Россия; тел.: +79500479274; адъюнкт.

Поляков Дмитрий Николаевич – Научно-исследовательский цент Военной академии связи; e-mail: bryanik51@mail.ru; г. Санкт-Петербург, Россия; тел.: +79113045069; адъюнкт.

Бикбулатов Владислав Родионович – Научно-исследовательский цент Военной академии связи; e-mail: vlaad.bik@icloud.com; г. Санкт-Петербург; тел.: +79953062642; адъюнкт.

Konkov Denis Ivanovich – Research Center of the Military Academy of Communications; e-mail: den/konkov/94@mail.ru; St. Petersburg, Russia; phone: +79537321643; adjunct.

Schmidt Artur Andreyevich – Research Center of the Military Academy of Communications; e-mail: shmidt.artur2011@yandex.ru; St. Petersburg, Russia; phone: +79500479274; adjunct.

Polyakov Dmitry Nikolaevich – Research Center of the Military Academy of Communications; e-mail: bryanik51@mail.ru; St. Petersburg, Russia; phone: +79113045069; adjunct.

Bikbulatov Vladislav Rodionovich – Research Center of the Military Academy of Communications; e-mail: vlaad.bik@icloud.com; St. Petersburg, Russia; phone: +79953062642; adjunct.

ПРАВИЛА ОФОРМЛЕНИЯ РУКОПИСЕЙ

1. Объем статьи должен быть не менее 12 и не более 18 страниц. Формат (А 4). Редактор ***Word 7 for Windows***, шрифт Times New Roman, размер 14, интервал 1,5. Авторы представляют в редакцию 1 экз. статьи и идентичный электронный вариант.

2. Названию статьи предшествует индекс УДК, соответствующий заявленной теме.

3. Текст статьи начинается с названия статьи (на русском и английском языках), фамилии, имени и отчества автора (полностью) и снабжается аннотацией на русском и английском языках объёмом ***не менее 250-300 слов***. В тексте аннотации указывается цель, задачи исследования и краткие выводы. В аннотации ***не следует*** давать ссылки на номер публикации в списке литературы к статье. После аннотаций приводятся ключевые слова (словосочетания), несущие в тексте основную смысловую нагрузку (на русском и английском языках).

4. В тексте статьи следует использовать минимальное количество таблиц и иллюстраций. Рисунок должен иметь объяснения значений всех компонентов, порядковый номер, название, расположенное под рисунком. В тексте на рисунок дается ссылка. Таблица должна иметь порядковый номер, заголовок, расположенный над ней. Данные таблиц и рисунков не должны дублировать текст. Формулы должны быть набраны ***в редакторе формул Word 7 for Windows.***

5. Цитаты тщательно сверяются с первоисточником и визируются автором на обратной стороне последней страницы: "Цитаты и фактический материал сверены". Подпись, дата.

6. Наличие пристатейного библиографического списка на русском и английском языках обязательно. ***Ссылок должно быть не менее 20-ти,*** из них на зарубежные источники – не менее 35 %. В тексте ссылки должны быть в квадратных скобках.

Примеры оформления литературы: а) для книг: фамилия, инициалы автора(ов), полное название книги, место, год издания, страницы; б) для статей: фамилия и инициалы автора(ов), полное название сборника, книги, газеты, журнала, где опубликована статья, место и год издания (сборника, книги), номер (для журнала), год и дата (для газеты), выпуск, часть (для сборника), страницы, на которых опубликована статья. Иностранная литература оформляется по тем же правилам.

Ссылки на неопубликованные работы не допускаются.

7. Рукопись должна быть тщательно вычитана. Редакционная коллегия оставляет за собой право при необходимости сокращать статьи, редактировать и отсылать авторам на доработку.

8. Статьи сопровождаются сведениями об авторе(ах) (фамилия, имя, отчество, ученое звание, должность, место работы, адрес, электронный адрес и номер телефона) на русском и английском языках.

9. Плата с аспирантов за публикацию рукописей не взымается.

Адрес журнала в Интернете: http://izv-tn.tti.sfedu.ru/.