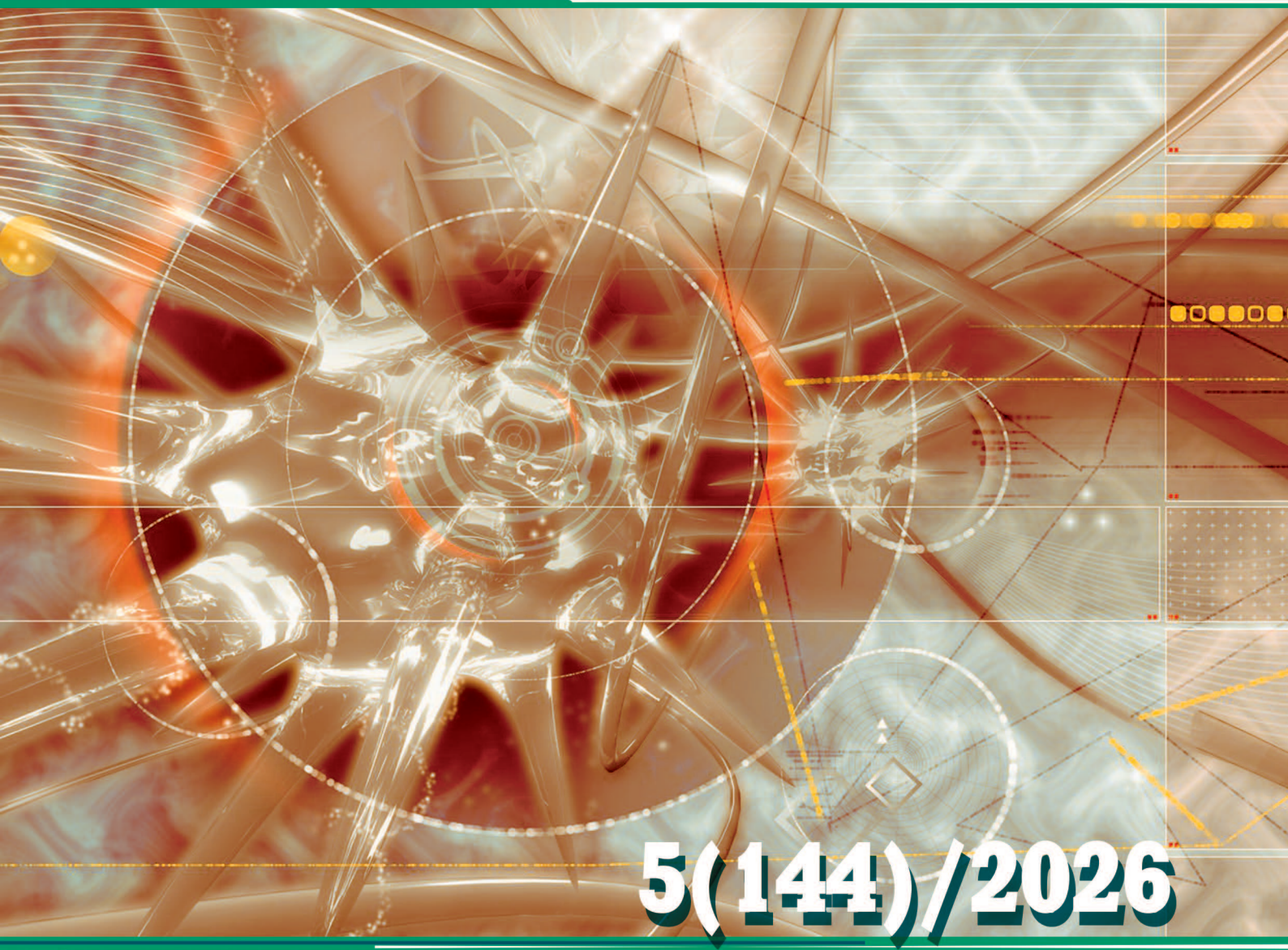
ISSN 1684-8853 (print); ISSN 2541-8610 (online)

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ



5(144)/2026

doi:10.31799/1684-8853-2026-5

ISSN 1684-8853 (print); ISSN 2541-8610 (online)

SCIENTIFIC JOURNAL

5(144)/2026

PEER REVIEWED JOURNAL

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

Founder
A. Vostrikov
Publisher
Saint Petersburg State University of Aerospace Instrumentation
Editor-in-Chief
E. Krouk
Dr. Sc., Professor, Moscow, Russia
Executive secretary
O. Muravtsova
Editorial Board
V. Anisimov
Dr. Sc., Professor, Saint Petersburg, Russia
B. Bezruchko
Dr. Sc., Professor, Saratov, Russia
N. Blaunstein
Dr. Sc., Professor, Beer-Sheva, Israel
M. Buzdalov,
PhD, Researcher, Saint Petersburg, Russia
C. Christodoulou
PhD, Professor, Albuquerque, New Mexico, USA
A. Dudin
Dr. Sc., Professor, Minsk, Belarus
I. Dumer
PhD, Professor, Riverside, USA
M. Favorskaya
Dr. Sc., Professor, Krasnoyarsk, Russia
L. Fortuna
PhD, Professor, Catania, Italy
A. Fradkov
Dr. Sc., Professor, Saint Petersburg, Russia
A. Hramov
Dr. Sc., Professor, Kaliningrad, Russia
L. Jain
PhD, Professor, Canberra, Australia
A. Myllari
PhD, Professor, Grenada, West Indies
K. Samouylov
Dr. Sc., Professor, Moscow, Russia
J. Seberry
PhD, Professor, Wollongong, Australia
M. Sergeev
Dr. Sc., Professor, Saint Petersburg, Russia
A. Shalyto
Dr. Sc., Professor, Saint Petersburg, Russia
A. Shepeta
Dr. Sc., Professor, Saint Petersburg, Russia
Yu. Shokin
RAS Academician, Dr. Sc., Novosibirsk, Russia
A. Smirnov
Dr. Sc., Professor, Saint Petersburg, Russia
T. Sutikno
PhD, Associate Professor, Yogyakarta, Indonesia
A. Tyugashev,
Dr. Sc., Professor, Samara, Russia
Z. Yuldashev
Dr. Sc., Professor, Saint Petersburg, Russia
A. Zeifman
Dr. Sc., Professor, Vologda, Russia
Editor: A. Larionova
Proofreader: T. Zvertanovskaia
Design: M. Chernenko, Yu. Umnitsyna
Layout and composition: I. Mosina

Contact information
The Editorial and Publishing Center, SUAI
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia
Website: http://i-us.ru/en, e-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

SYSTEM AND PROCESS MODELING

Kuzmenko A. A., Sergeev M. B.
Adaptive operation model for a remote patient monitoring system under communication channel degradation 2

Knyazev M. A., Gusev M. M.
Mathematical model and experimental robustness assessment of quantized DS-CNNs for TinyML keyword spotting 11

HARDWARE AND SOFTWARE RESOURCES

Nazarov V. A., Shalyto A. A.
Validation of automata specifications based on automata composition 21

INFORMATION SECURITY

Vulfin A. M., Vasilyev V. I., Lutskovich A. I., Kirillova A. D.
A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph 37

INFORMATION CODING AND TRANSMISSION

Shtanko S. V., Kryagin V. A., Topchiy P. N., Anikin D. A.
A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence 56

Krylov D. R., Bolotskikh U. A., Turlikov A. M.
Average age of information in distributed data storage systems with peer nodes 73

CONTROL IN MEDICAL AND BIOLOGICAL SYSTEMS

Chubich V. M., Kotselap E. S.
Application of the InceptionTime convolutional neural network to multi-label classification of electrocardiograms 85

INFORMATION ABOUT THE AUTHORS 96

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder A. Vostrikov,
PI № FS 77-82226 from November, 23, 2021
© A. Vostrikov, 2026

Submitted for publication 19.09.26. Passed for printing 30.10.26. Signed for printing: 05.11.26.
Format 60×84$_{1/8}$. Phototype CentSchbkCyrill BT. Digital printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia

The journal is indexed in Scopus.

Free distribution.

doi:10.31799/1684-8853-2026-5 ISSN 1684-8853 (print); ISSN 2541-8610 (online)
НАУЧНЫЙ ЖУРНАЛ

5(144)/2026

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
А. А. Востриков
Издатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Главный редактор
Е. А. Крук,
д-р техн. наук, проф., Москва, РФ
Ответственный секретарь
О. В. Муравцова
Редакционная коллегия:
В. Г. Анисимов,
д-р техн. наук, проф., Санкт-Петербург, РФ
Б. П. Безручко,
д-р физ.-мат. наук, проф., Саратов, РФ
Н. Блаунштейн,
д-р физ.-мат. наук, проф., Беэр-Шева, Израиль
М. В. Буздалов,
канд. техн. наук, научный сотрудник, Санкт-Петербург, РФ
Л. С. Джайн,
д-р наук, проф., Канберра, Австралия
А. Н. Дудин,
д-р физ.-мат. наук, проф., Минск, Беларусь
И. И. Думер,
д-р наук, проф., Риверсайд, США
А. И. Зейфман,
д-р физ.-мат. наук, проф., Вологда, РФ
К. Кристодолу,
д-р наук, проф., Альбукерке, Нью-Мексико, США
А. А. Мюлляри,
д-р наук, профессор, Гренада, Вест-Индия
К. Е. Самуйлов,
д-р техн. наук, проф., Москва, РФ
Д. Себерри,
д-р наук, проф., Волонгонг, Австралия
М. Б. Сергеев,
д-р техн. наук, проф., Санкт-Петербург, РФ
А. В. Смирнов,
д-р техн. наук, проф., Санкт-Петербург, РФ
Т. Сутикноу,
д-р наук, доцент, Джокьякарта, Индонезия
А. А. Тюгашев,
д-р техн. наук, проф., Самара, РФ
М. Н. Фаворская,
д-р техн. наук, проф., Красноярск, РФ
Л. Фортуна,
д-р наук, проф., Катания, Италия
А. Л. Фрадков,
д-р техн. наук, проф., Санкт-Петербург, РФ
А. Е. Храмов,
д-р физ.-мат. наук, Калининград, РФ
А. А. Шалыто,
д-р техн. наук, проф., Санкт-Петербург, РФ
А. П. Шепета,
д-р техн. наук, проф., Санкт-Петербург, РФ
Ю. И. Шокин,
акад. РАН, д-р физ.-мат. наук, проф., Новосибирск, РФ
З. М. Юлдашев,
д-р техн. наук, проф., Санкт-Петербург, РФ
Редактор: А. Г. Ларионова
Корректор: Т. В. Звертановская
Дизайн: М. Л. Черненко, Ю. В. Умницына
Компьютерная верстка: И. А. Мосина

Адрес редакции: 190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, ГУАП, РИЦ
Тел.: (812) 494-70-02, эл. адрес: ius.spb@gmail.com, сайт: http://i-us.ru

МОДЕЛИРОВАНИЕ СИСТЕМ И ПРОЦЕССОВ

Кузьменко А. А., Сергеев М. Б.
Модель адаптивного функционирования системы удаленного мониторинга пациентов при деградации канала связи **2**

Князев М. А., Гусев М. М.
Математическая модель и экспериментальная оценка устойчивости квантованных DS-CNN для TinyML-распознавания речевых команд 11

ПРОГРАММНЫЕ И АППАРАТНЫЕ СРЕДСТВА

Назаров В. А., Шалыто А. А.
Валидация автоматных спецификаций на основе перемножения автоматов 21

ЗАЩИТА ИНФОРМАЦИИ

Вульфин А. М., Васильев В. И., Луцкович А. И., Кириллова А. Д.
Модель и алгоритмы анализа данных кибер разведки на основе графа знаний 37

КОДИРОВАНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ

Штанько С. В., Крягин В. А., Топчий П. Н., Аникин Д. А.
Способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности 56

Крылов Д. Р., Болотских У. А., Тюрликов А. М.
Средний возраст информации в распределенных системах хранения данных с равноправными узлами 73

УПРАВЛЕНИЕ В МЕДИЦИНЕ И БИОЛОГИИ

Чубич В. М., Коцелап Е. С.
Применение сверточной нейронной сети InceptionTime для классификации электрокардиограмм с множественными метками 85

СВЕДЕНИЯ ОБ АВТОРАХ 96

Журнал входит в БД Scopus и 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.

Сдано в набор 19.09.26. Подписано в печать 30.10.26. Дата выхода в свет: 05.11.26.
Формат 60×841/8. Гарнитура CentSchbkCyrill BT. Печать цифровая.
Усл. печ. л. 11,7. Уч.-изд. л. 15,7. Тираж 1000 экз (1-й завод 40 экз.). Заказ № 369.
Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.
Отпечатано в редакционно-издательском центре ГУАП.
190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.
Распространяется бесплатно.

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-82226 от 23 ноября 2021 г.
© А. А. Востриков, 2026

УДК 681.518.3; 615.47:616-072.7
doi:10.31799/1684-8853-2026-5-2-10
EDN: DKDREI

Научные статьи
Articles

Модель адаптивного функционирования системы удаленного мониторинга пациентов при деградации канала связи

А. А. Кузьменко[a], *аспирант, orcid.org/0009-0006-9031-5082*
М. Б. Сергеев[a], *доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277, mbse@guap.ru*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *непрерывный удаленный мониторинг пациентов оказался чувствителен к снижению пропускной способности и разрывам связи: очередь необработанных данных увеличивала задержку доставки клинически значимого сообщения и могла исчерпать локальную память устройства.* ***Цель:*** *разработать модель адаптивного функционирования, сохранявшую приоритет критических данных при изменении характеристик канала и ограниченной емкости накопителя.* ***Методы:*** *состояние распределенной системы было формализовано через доступность соединения, подтвержденную скорость доставки, задержку, потери пакетов, заполнение очереди, клинический риск и качество сигнала. Управление представлено детерминированным автоматом с гистерезисом, временным подтверждением состояния и минимальным временем пребывания в режиме. Для сравнения сформирован протокол испытаний на потоке трехканального электрокардиографического сигнала с воспроизводимыми профилями ограничения скорости, задержки, потерь и разрыва соединения.* ***Результаты:*** *определены четыре режима: полная, сокращенная и событийная передача, а также автономное накопление с локальным оповещением. Данные разделены на пять приоритетных классов; тревожное сообщение и контекст события обслуживались раньше текущего и архивного некритического потока. Для критических записей выделена защищенная область памяти, а после восстановления связи установлена последовательность синхронизации. Условия допустимости заданы ограничениями на задержку тревоги, сохранность контекста и расчетный автономный интервал.* ***Практическая значимость:*** *модель позволила формировать требования к периферийному устройству, накопителю и каналу связи до выбора конкретной аппаратной платформы.* ***Обсуждение:*** *численные преимущества адаптивной стратегии не утверждались; предложенный протокол предназначался для их последующей экспериментальной проверки.*

Ключевые слова *— удаленный мониторинг пациентов, кардиомониторинг, электрокардиография, периферийная обработка, адаптивная передача данных, деградация канала связи, локальный накопитель, критическое событие.*

Для цитирования: Кузьменко А. А., Сергеев М. Б. Модель адаптивного функционирования системы удаленного мониторинга пациентов при деградации канала связи. *Информационно-управляющие системы*, 2026, № 5, с. 2–10. doi:10.31799/1684-8853-2026-5-2-10, EDN: DKDREI
For citation: Kuzmenko A. A., Sergeev M. B. Adaptive operation model for a remote patient monitoring system under communication channel degradation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2026-5-2-10, EDN: DKDREI

Введение

Носимые и домашние медицинские устройства сделали длительное наблюдение за пациентами доступным вне стационара. Их используют для контроля хронических заболеваний, наблюдения после выписки и раннего выявления ухудшения состояния, в том числе беременных [1]. Во время пандемии COVID-19 такие системы помогали уменьшить число очных контактов и выделять пациентов, которым требовалась госпитализация [2–5].

Типовая система включает датчик, периферийное устройство или домашний шлюз, канал связи, сервер и рабочее место медицинского специалиста. Серверная обработка удобна: алгоритмы обновляются централизованно, исходные записи доступны для повторного анализа, а данные разных устройств можно объединять. Цена этой простоты — зависимость от сети. Если подтвержденная скорость доставки становится ниже скорости формирования данных, очередь растет, задержка увеличивается, а локальный накопитель постепенно заполняется. В настоящей работе под деградацией канала связи понимается постепенное или резкое ухудшение его параметров: снижение подтвержденной скорости доставки, увеличение задержки и доли недоставленных пакетов — при сохранении соединения периферийного носимого устройства с сервером. Полный разрыв соединения рассматривается отдельно как предельное состояние недоступности канала.

Особенно уязвим непрерывный физиологический поток. Стабильный участок ЭКГ и фрагмент с потенциально опасным нарушением ритма имеют разную клиническую ценность, но при обычной потоковой передаче стоят в одной очереди. Уже накопленный массив способен задержать тревогу, хотя для первичного сообщения требуется лишь малая доля пропускной способности.

Периферийная обработка позволяет изменить этот порядок. Устройство может оценить качество сигнала, выделить простые признаки события и сформировать короткое приоритетное сообщение, не ожидая серверного анализа [6–9]. Для этого не обязательно использовать сложную модель машинного обучения: достаточно детерминированного алгоритма, если его выход имеет понятный клинический смысл и прошел отдельную валидацию. В этой работе точность медицинского классификатора не исследуется; рассматривается реакция системы на уже полученную оценку риска.

Цель исследования — разработать модель адаптивного функционирования системы удаленного мониторинга, которая при изменении характеристик связи сохраняет приоритет критических данных и управляет некритическим потоком с учетом ограниченной памяти. Научная новизна состоит в совместном использовании трех групп признаков: состояния канала, клинической значимости текущих данных и динамики заполнения локального накопителя. Результатом управления является не только выбор скорости передачи, но и порядок хранения, вытеснения и последующей синхронизации данных.

Постановка задачи

При устойчивой связи централизованная передача обеспечивает врачу наиболее полную запись. Локальное накопление сохраняет поток во время разрыва, однако сервер узнает о событии только после восстановления соединения. Событийная передача уменьшает трафик, но делает полноту данных зависимой от качества локального распознавания. Исследования адаптивной дискретизации, распределения вычислений и семантического сжатия показывают, что объем, например ЭКГ, можно менять на периферийном узле [10–16]. Отдельный механизм сжатия, однако, не определяет, какие записи важнее и что делать при заполнении памяти. Сравнение преимуществ и ограничений базовых стратегий приведено в табл. 1.

Систематические обзоры последних лет подтвердили клиническую востребованность удаленного мониторинга, но одновременно отметили неоднородность результатов, зависимость эффекта от организации процесса и требования к удобству использования [17–19]. Развитие носимой периферийной обработки позволяет оценивать сигналы непосредственно на устройстве и уменьшать объем передаваемых данных, однако сохраняет необходимость явного управления приоритетами и восстановлением потока после нарушения связи [20]. Методы объяснимого обнаружения и классификации событий в системах медицинского мониторинга развивают этот подход [21].

■ ***Таблица 1.*** Сравнение базовых стратегий
■ ***Table 1.*** Comparison of baseline strategies

Критерий	Полный поток	Накопление	Событийная передача
Полнота данных	Высокая при устойчивой связи	Восстанавливается после синхронизации	Зависит от локального анализа
Задержка тревоги	Растет вместе с очередью	Включает время разрыва	Мала при доступном канале
Нагрузка на сеть	Постоянно высокая	Переносится на период восстановления	Низкая
Работа без связи	Ограничена буфером	Сохранение до заполнения памяти	Локальный анализ и сохранение
Главный риск	Задержка критического фрагмента	Позднее оповещение	Потеря контекста или пропуск события

Для формализации используем непрерывный сигнал из n каналов с частотой дискретизации $f_д$ и разрядностью q. Скорость исходных данных и скорость полного сетевого потока равны

$$\lambda_{исх} = n \cdot f_д \cdot q/8;$$

$$\lambda_{полн} = k_{прот} \cdot \lambda_{исх}, \quad (1)$$

где $\lambda_{исх}$ — скорость исходных данных, байт/с; $\lambda_{полн}$ — скорость полного сетевого потока, байт/с; n — число каналов; $f_д$ — частота дискретизации одного канала, Гц; q — разрядность отсчета, бит; $k_{прот}$ — коэффициент протокольных накладных расходов ($k_{прот} \geq 1$). Деление на 8 переводит биты в байты.

Коэффициент $k_{прот}$ учитывает временные метки, идентификаторы, контрольные суммы, заголовки и подтверждения. В программной реализации полезнее измерять не номинальную пропускную способность, а объем данных $V_{подтв}$, подтвержденный сервером за интервал Δt:

$$\mu_{эф}(t) = V_{подтв}(t) / \Delta t, \quad (2)$$

где $\mu_{эф}(t)$ — эффективная скорость подтвержденной доставки, байт/с; $V_{подтв}(t)$ — объем данных, подтвержденный сервером за интервал наблюдения, байт; Δt — длительность интервала наблюдения, с.

Состояние системы описывает доступность соединения A, эффективную скорость доставки $\mu_{эф}$, задержку L, долю недоставленных пакетов p,

объем очереди Q, клинический риск R и качество сигнала S:

$$\mathbf{X}(t) = [A(t), \mu_{эф}(t), L(t), p(t), Q(t), R(t), S(t)], \quad (3)$$

где $\mathbf{X}(t)$ — вектор состояния системы; $A(t)$ — бинарный признак доступности соединения; $L(t)$ — задержка, с; $p(t)$ — доля недоставленных пакетов; $Q(t)$ — объем данных в локальной очереди, байт; $R(t)$ — нормированная оценка клинического риска; $S(t)$ — нормированная оценка качества сигнала.

Объем очереди меняется как разность поступивших и подтвержденно удаленных данных. Для накопителя емкостью $Q_{макс}$ получаем

$$Q(t + \Delta t) = \min\{Q_{макс};$$
$$\max[0; Q(t) + (\lambda_{вх}(t) - \lambda_{вых}(t)) \cdot \Delta t]\}, \quad (4)$$

где $Q(t)$ и $Q(t + \Delta t)$ — объем данных в очереди в начале и конце интервала, байт; $Q_{макс}$ — емкость очереди, байт; $\lambda_{вх}(t)$ и $\lambda_{вых}(t)$ — скорости поступления данных в очередь и подтвержденного удаления из нее, байт/с; Δt — длительность интервала, с.

Текущего значения Q недостаточно: одинаково заполненные накопители требуют разных действий, если в одном случае очередь уменьшается, а в другом быстро растет. Поэтому управляющая функция использует также dQ/dt и оценку времени до переполнения. Клинический риск задается нормированным показателем

$$R(t) = \Phi[\mathbf{Z}(t), S(t)], \ 0 \le R(t) \le 1, \quad (5)$$

где $R(t)$ — нормированная оценка клинического риска; Φ — внешний по отношению к модели алгоритм оценки риска; $\mathbf{Z}(t)$ — вектор признаков физиологического сигнала; $S(t)$ — нормированная оценка качества сигнала. Если $S(t) < S_{мин}$, устройство сообщает о плохом качестве записи и не трактует артефакт как подтвержденное клиническое событие; $S_{мин}$ — минимально допустимая оценка качества.

Критическое событие должно включать короткую тревогу и фрагмент сигнала до и после обнаружения. Для интервалов $T_{до}$ и $T_{после}$ размер такого контекста

$$V_{соб} = V_{служ} + c_{соб} \cdot n \cdot f_д \cdot q \cdot (T_{до} + T_{после})/8, \quad (6)$$

где $V_{соб}$ — объем записи события, байт; $V_{служ}$ — объем служебных данных события, байт; $c_{соб}$ — безразмерный коэффициент представления и сжатия записи ($c_{соб} = 1$ при отсутствии сжатия); $T_{до}$ и $T_{после}$ — длительности интервалов до и после события, с.

Модель должна выполнять ограничения по задержке тревоги, сохранности контекста и емкости накопителя. Уменьшение трафика рассматривается только среди решений, которые этим ограничениям удовлетворяют.

Модель адаптивного функционирования

Приоритеты данных и режимы функционирования

Данные разделены на пять классов. Приоритет описывает не медицинскую тяжесть состояния сам по себе, а порядок использования ограниченного канала и памяти. Составы классов данных и правила их обслуживания приведены в табл. 2.

■ ***Таблица 2.*** Классы данных
■ ***Table 2.*** Data classes

Класс	Содержание	Правило обслуживания
P1	Короткое сообщение о критическом событии	Передается первым
P2	Сигнал до и после события	Следует за данными класса P1; хранится в защищенной области
P3	Показатели состояния и качества	Передаются регулярно; допустима агрегация
P4	Текущий полный сигнал	Передается при достаточном ресурсе
P5	Архив некритических данных	Использует остаточную скорость канала

Короткое сообщение класса P1 формируется сразу после обнаружения события. Контекст данных класса P2 дополняется данными $T_{после}$ и передается отдельным объектом, поэтому ожидание полного фрагмента не увеличивает задержку первичной тревоги. Появление сообщения класса P1 приостанавливает передачу данных классов P4 и P5.

Управляющая функция выбирает один из четырех режимов. В режиме M0 передается полный поток; режим M1 уменьшает объем некритических данных; в режиме M2 остаются события, показатели состояния и контроль качества; режим M3 используется при отсутствии подтвержденного обмена и сочетает локальный анализ, накопление и оповещение пациента. Передаваемые данные и действия устройства для каждого режима представлены в табл. 3.

■ ***Таблица 3.*** Режимы адаптивной передачи
■ ***Table 3.*** Adaptive transmission modes

Режим	Состояние связи	Передаваемые данные	Действия устройства
M0	Устойчивый канал с резервом	P1–P4 и доступная часть P5	Полная регистрация и передача
M1	Ресурс ниже полного потока	P1–P3, сокращенный P4, часть P5	Снижение объема и освобождение очереди
M2	Канал пригоден в основном для коротких сообщений	P1–P3; P2 по доступности	Полный сигнал сохраняется локально
M3	Подтвержденная доставка отсутствует	Пробные и обязательные сообщения при появлении связи	Локальное оповещение и накопление

Выбор режима функционирования

Относительный коммуникационный ресурс определяется отношением подтвержденной скорости к скорости полного потока:

$$C(t) = \mu_{эф}(t) / \lambda_{полн}, \quad (7)$$

где $C(t)$ — безразмерный коэффициент достаточности канала; $\lambda_{полн}$ — скорость полного сетевого потока, байт/с.

Значение $C > 1$ указывает на возможный резерв, $0 < C < 1$ — на неизбежный рост очереди при передаче полного потока, а $C = 0$ — на отсутствие удаленной доставки. Одного C недостаточно: режим также зависит от L, p, Q, dQ/dt, R и S. Решение принимает детерминированный автомат

$$u(t) = F[A, C, L, p, Q/Q_{макс}, dQ/dt, R, S, u(t - \Delta t)], \quad (8)$$

где $u(t)$ — режим функционирования; F — детерминированное правило управления; A, C, L, p, $Q/Q_{макс}$, dQ/dt, R и S — учитываемые правилом доступность соединения, достаточность канала, задержка, доля недоставленных пакетов, относительное заполнение очереди, скорость ее изменения, клинический риск и качество сигнала; $u(t-\Delta t)$ — режим на предыдущем шаге управления.

При устойчивом канале и не растущей очереди выбирается режим M0. Недостаток ресурса для полного потока переводит систему в режим M1; дальнейшее ухудшение — в M2. Если подтверждений нет в течение $T_{пот}$, включается режим M3. После восстановления связь сначала используется в режиме M2 для передачи накопленных P1 и P2. Возврат к режимам M1 и M0 разрешается лишь после устойчивого улучшения.

Для каждой границы между соседними режимами по коммуникационному ресурсу C задаются два порога: $C_{ух\ i}$ для ухудшения и $C_{вос\ i}$ для восстановления, причем $C_{вос\ i} > C_{ух\ i}$. Переход в более экономичный режим разрешается при снижении C до $C_{ух\ i}$, а обратный переход — только после превышения $C_{вос\ i}$. Пока C находится между этими значениями, сохраняется текущий режим. Различие порогов образует гистерезис и исключает повторное переключение при малых колебаниях параметров сети.

Неблагоприятное состояние должно сохраняться в течение $T_{ух}$, благоприятное — в течение $T_{вос}$, причем $T_{вос} > T_{ух}$. После штатного перехода следующее переключение допускается не ранее, чем через $T_{реж}$. Таким образом, разные пороги, временное подтверждение состояния и минимальное время пребывания в режиме совместно ограничивают частые переключения. Эти задержки не применяются к критическому событию, потере подтвержденной связи и угрозе переполнения накопителя.

Задержка тревожного сообщения $D_{трев}$ включает обнаружение, формирование, ожидание в очереди, передачу и обработку сервером:

$$D_{трев} = D_{обн} + D_{форм} + D_{оч} + D_{пер} + D_{сер} \le D_{макс}, \quad (9)$$

где $D_{трев}$ — полная задержка доставки тревоги; $D_{обн}$ — задержка обнаружения события; $D_{форм}$ — задержка формирования тревожного сообщения; $D_{оч}$ — задержка в очереди; $D_{пер}$ — задержка передачи; $D_{сер}$ — задержка серверной обработки; $D_{макс}$ — максимально допустимая задержка. Все задержки измеряются в секундах.

Ограничение применимо только при физически доступной доставке. В режиме M3 оцениваются время локального оповещения $D_{лок}$ и сохранность P1–P2, а после восстановления — задержка первоочередной отправки накопленной тревоги.

Накопление и синхронизация данных

Некритический поток не должен занимать всю память до возникновения события. Объем памяти накопителя Q делится на обычную $Q_{обыч}$ и критическую $Q_{крит}$ области. Минимальный резерв определяется максимальным числом событий в расчетном автономном интервале:

$$Q_{крит} \ge Q_{крит.мин} = N_{соб.макс} \cdot V_{соб.макс}, \quad (10)$$

где $Q_{крит}$ — емкость защищенной области памяти, выделенной критическим записям, байт; $Q_{крит.мин}$ — минимально необходимая емкость этой области, байт; $N_{соб.макс}$ — максимальное

число событий, которые должны быть сохранены одновременно; $V_{\text{соб.макс}}$ — максимальный объем одной записи события, байт.

Все действия с памятью определяются достигнутыми порогами, определяющими их порядок и содержание. Порог $K1$ соответствует началу ограничения архива Р5: старые некритические записи агрегируются или удаляются. При достижении порога $K2$ дополнительно уменьшается детализация Р4. Порог $K3$ обозначает состояние, близкое к переполнению, и вызывает техническое предупреждение. Записи Р1 и Р2 не вытесняются некритическими данными. Если исчерпывается и критическая область памяти (резерв), устройство сообщает системе, что дальнейшая сохранность не гарантируется.

После восстановления соединения планировщик обслуживает классы в порядке Р1 > Р2 > Р3 > > Р4 > Р5. Крупные записи разбиваются на транспортные блоки, поэтому новое Р1 может прервать архив не позднее границы следующего блока. Архив получает только остаточный ресурс:

$$\lambda_{\text{арх}}(t) = \max\{0;\ \mu_{\text{эф}}(t) - \lambda_{\text{тек}}(t) - \lambda_{\text{сроч}}(t) - \lambda_{\text{рез}}\}, \quad (11)$$

где $\lambda_{\text{арх}}(t)$ — допустимая скорость выгрузки архива; $\lambda_{\text{тек}}(t)$ — скорость текущего формируемого потока; $\lambda_{\text{сроч}}(t)$ — скорость передачи срочных данных классов Р1–Р3; $\lambda_{\text{рез}}$ — резерв пропускной способности для новых критических сообщений. Все скорости измеряются в байт в секунду.

Ресурсная оптимизация выполняется после проверки обязательных ограничений. Среди допустимых решений можно минимизировать относительный трафик, энергию, время синхронизации и число переключений:

$$J_{\text{рес}} = \alpha K_{\text{траф}} + \beta K_{\text{эн}} + \gamma K_{\text{синхр}} + \delta K_{\text{перекл}}, \quad (12)$$

где $J_{\text{рес}}$ — значение ресурсного критерия; $K_{\text{траф}}$, $K_{\text{эн}}$, $K_{\text{синхр}}$ и $K_{\text{перекл}}$ — нормированные частные показатели сетевого трафика, энергопотребления, времени синхронизации и числа переключений режимов; α, β, γ и δ — неотрицательные весовые коэффициенты, для которых $\alpha + \beta + \gamma + \delta = 1$.

Никакая приоритизация не компенсирует неограниченный разрыв связи или поток обязательных данных, превышающий совокупную пропускную способность и память. Для временного интервала T потенциальная выполнимость требует

$$V_{\text{обяз}}(T) \le Q_{\text{дост}} + \int_0^T \mu_{\text{обяз}}(t)\mathrm{d}t, \quad (13)$$

где $V_{\text{обяз}}(T)$ — объем обязательных данных, сформированных за интервал T, байт; $Q_{\text{дост}}$ — доступная для них емкость накопителя, байт; $\mu_{\text{обяз}}(t)$ — часть эффективной скорости доставки, выделенная обязательным данным, байт/с; T — рассматриваемый интервал, с.

Нарушение этого условия не маскируется сокращением некритического трафика. Система сохраняет наиболее важные записи, рассчитывает время до переполнения и формирует техническое предупреждение.

Методика экспериментальной проверки

Проверку модели можно строить вокруг четырех компонентов: периферийного устройства, управляемого сетевого шлюза, сервера и контроллера эксперимента.

Периферийное устройство получает один и тот же записанный или синтетический сигнал, а шлюз воспроизводит заданные ограничения скорости, задержку, одиночные и групповые потери, а также полный разрыв соединения. Сервер подтверждает фрагменты, проверяет контрольные суммы, устраняет дубликаты и фиксирует время получения. Стратегия передачи подключается через единый интерфейс, поэтому смена алгоритма не меняет входной поток, формат пакетов, транспорт и емкость памяти.

Для сравнения выбираются четыре варианта сценария стратегии: $S_{\text{полн}}$ — непрерывная попытка передавать полный поток; $S_{\text{нак}}$ — накапливание потока при отсутствии связи; $S_{\text{соб}}$ — постоянная передача только события и показателей; $S_{\text{адапт}}$ — использование режимов М0–М3. Одни и те же моменты событий, профили качества и реализации случайных сетевых воздействий применяются ко всем стратегиям.

Параметры базовой конфигурации прототипа, использованные при формировании экспериментальных сценариев, приведены в табл. 4.

Значения $D_{\text{макс}}$ и $D_{\text{лок}}$ служат техническими критериями стенда, а не универсальными клиническими нормативами. Пороги переключения $C_{\text{ух}\ i}$ и $C_{\text{вос}\ i}$ определяются после пилотной настройки, фиксируются в протоколе конфигурации и не меняются в основной серии.

Коэффициенты $K1$, $K2$ и $K3$ являются безразмерными долями суммарного заполнения накопителя $b(t) = Q(t)/Q_{\text{макс}}$. Значения 0,60, 0,85 и 0,95 означают заполнение 60, 85 и 95 % от $Q_{\text{макс}}$; при $Q_{\text{макс}} = 128$ МиБ им соответствуют 76,8, 108,8 и 121,6 МиБ. Обычные данные при этом не могут занимать защищенную область $Q_{\text{крит}}$.

Например, при скорости полного профиля 42 Кбит/с и подтвержденной скорости доставки 28 Кбит/с работа в режиме М0 приводит к росту очереди со скоростью 14 Кбит/с. После перехода в режим М1 текущий поток уменьшается до 15 Кбит/с, поэтому он помещается в доступный канал, а оставшийся ресурс может использоваться для передачи накопленных данных.

Сетевые воздействия и проверяемые свойства модели представлены в табл. 5.

■ ***Таблица 4.*** Базовая конфигурация прототипа
■ ***Table 4.*** Baseline prototype configuration

Группа	Параметр	Значение	Назначение
Поток	ЭКГ	3 канала; 500 Гц; 24 бит	Полный полезный поток 36 Кбит/с
Передача	$\lambda 0/\lambda 1/\lambda 2$	42/15/1,5 Кбит/с	Полный, сокращенный и событийный профили
Событие	$T_{\text{до}}/T_{\text{после}}$	30/30 с	Контекст около 270 Кбайт
Память	$Q_{\text{макс}}/Q_{\text{крит}}$	128/16 МиБ	Общий и защищенный объем
Заполнение накопителя	$K1/K2/K3$	60/85/95 % $Q_{\text{макс}}$	Ограничение P5/сокращение P4/предупреждение
Переключение	$\Delta t/T_{\text{ух}}/T_{\text{вос}}$	1 с/5 с/30 с	Управляющий цикл/подтверждение ухудшения/ подтверждение восстановления
Переключение	$T_{\text{реж}}/T_{\text{пот}}$	20 с/10 с	Минимальное пребывание в режиме/потеря связи
Тревога	$D_{\text{макс}}/D_{\text{лок}}$	10 с/1 с	Технические критерии стенда

■ ***Таблица 5.*** Ключевые сетевые сценарии
■ ***Table 5.*** Key network scenarios

Сценарий	Условия	Проверяемое свойство
E0	128 Кбит/с; 50 мс; без потерь	Работа в режиме M0 без необоснованного сокращения
E1	28 Кбит/с; 100 мс; потери 1 %	Переход в режим M1
E2	4 Кбит/с; 400 мс; потери 2 %	Переход в режим M2 и доставка P1
E3	Связь отсутствует 4 ч	Режим M3, локальное оповещение и сохранность
E4	Разрыв и восстановление до 128 Кбит/с	Приоритетная синхронизация данных классов P1–P2
E5	Колебания 38–55 Кбит/с каждые 10 с	Работа в режиме «гистерезис»
E8	8 Кбит/с; начальное заполнение 85 %	Защита критического резерва
E9	Событие во время передачи архива	Прерывание данных классов P4–P5 новыми данными класса P1
E11	20 событий за 4 ч без связи	Достаточность $Q_{\text{крит}}$

Основными конечными показателями должны являться: максимальная и 99-процентильная задержка данных класса P1, число нарушений $D_{\text{макс}}$, доля подтвержденных тревог, полнота класса P2, максимальное заполнение накопителя, время доставки критического архива после восстановления, полное время синхронизации и фактический сетевой трафик. Дополнительно следует фиксировать переключения режимов, повторные передачи, объем агрегированных или вытесненных данных классов P3–P5, время управляющего цикла и загрузку процессора.

Конфигурация признается допустимой, если при физически доступной связи $D_{\text{трев}} \le D_{\text{макс}}$, записи данных классов P1–P2 не потеряны в пределах расчетного автономного интервала, после синхронизации контекст полон, а управляющий цикл завершается быстрее Δt. Сокращение трафика или времени синхронизации оценивается только после этой проверки.

Заключение

Предложенная модель рассматривает удаленный мониторинг как управляемую распределенную систему. Решение зависит от параметров канала, клинического приоритета и накопителя одновременно. При хорошем соединении устройство передает полный поток; при дефиците ресурса сокращает некритические данные; при глубокой деградации оставляет события и показатели; при разрыве продолжает локальную обработку и сохраняет обязательный контекст.

Разделение тревоги P1 и контекста P2 уменьшает время первичного оповещения, а защищенная область памяти не позволяет обычному потоку вытеснить критические записи. После восстановления связи новый и накопленный критический трафики обслуживаются раньше архива. Для ограничения частых переключений в модель введены разные пороги ухудшения и восстановления,

временное подтверждение состояния канала и минимальное время пребывания в режиме. Эффективность этого механизма оценивается в сценарии E5 по числу переключений режимов.

Модель не обещает гарантированную доставку при любом дефиците ресурсов. Гарантия ограничена расчетной продолжительностью автономной работы, числом событий и доступной памятью. Если обязательный поток превышает ресурс канала и накопителя, корректная реакция состоит в защите наиболее значимых данных и явном техническом предупреждении.

Результаты экспериментальной проверки модели могут быть использованы для обоснования технических параметров элементов системы, в частности периферийного носимого устройства.

Литература

1. **Корнеева И. П., Крамарь К. А., Семенова Е. А., Сергеев А. М., Юлдашев З. М.** Аппаратно-программный комплекс для удаленного мониторинга и контроля состояния беременных женщин. *Информационно-управляющие системы*, 2021, № 6, с. 21–30. doi:10.31799/1684-8853-2021-6-21-30
2. **Noah B., Keller M. S., Mosadeghi S., Stein L., Johl S., Delshad S., Tashjian V. C., Lew D., Kwan J. T., Jusufagic A., Spiegel B. M. R.** Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials. *npj Digital Medicine*, 2018, vol. 1, art. 20172. doi:10.1038/s41746-017-0002-4
3. **Vindrola-Padros C., Singh K., Sidhu M., Georghiou T., Sherlaw-Johnson C., Tomini S. M., Inada-Kim M., Kirkham K., Streetly A., Cohen N., Fulop N. J.** Remote home monitoring (virtual wards) for confirmed or suspected COVID-19 patients: A rapid systematic review. *EClinicalMedicine*, 2021, vol. 37, art. 100965. doi:10.1016/j.eclinm.2021.100965
4. **Annis T., Pleasants S., Hultman G., Lindemann E., Thompson J. A., Billecke S., Badlani S., Melton G. B.** Rapid implementation of a COVID-19 remote patient monitoring program. *Journal of the American Medical Informatics Association*, 2020, vol. 27, no. 8, pp. 1326–1330. doi:10.1093/jamia/ocaa097
5. **Gordon W. J., Henderson D., DeSharone A., Fisher H. N., Judge J., Levine D. M., MacLean L., Sousa D., Su M. Y., Boxer R.** Remote patient monitoring program for hospital discharged COVID-19 patients. *Applied Clinical Informatics*, 2020, vol. 11, no. 5, pp. 792–801. doi:10.1055/s-0040-1721039
6. **Shi W., Cao J., Zhang Q., Li Y., Xu L.** Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 2016, vol. 3, no. 5, pp. 637–646. doi:10.1109/JIOT.2016.2579198
7. **Satyanarayanan M.** The emergence of edge computing. *Computer*, 2017, vol. 50, no. 1, pp. 30–39. doi:10.1109/MC.2017.9
8. **Rahmani A. M., Gia T. N., Negash B., Anzanpour A., Azimi I., Jiang M., Liljeberg P.** Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 2018, vol. 78, pp. 641–658. doi:10.1016/j.future.2017.02.014
9. **Mutlag A. A., Abd Ghani M. K., Arunkumar N., Mohammed M. A., Mohd O.** Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, 2019, vol. 90, pp. 62–78. doi:10.1016/j.future.2018.07.049
10. **Serhani M. A., El Kassabi H. T., Ismail H., Nujum Navaz A.** ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, 2020, vol. 20, no. 6, art. 1796. doi:10.3390/s20061796
11. **Abo-Zahhad M., Ahmed S. M., Elnahas O.** A wireless emergency telemedicine system for patients monitoring and diagnosis. *International Journal of Telemedicine and Applications*, 2014, vol. 2014, art. 380787. doi:10.1155/2014/380787
12. **Augustyniak P.** Adaptive sampling of the electrocardiogram based on generalized perceptual features. *Sensors*, 2020, vol. 20, no. 2, art. 373. doi:10.3390/s20020373
13. **Bhattarai A., Peng D., Payne J., Sharif H.** Adaptive partition of ECG diagnosis between cloud and wearable sensor net using open-loop and closed-loop switch mode. *IEEE Access*, 2022, vol. 10, pp. 63684–63697. doi:10.1109/ACCESS.2022.3182704
14. **Amiri D., Takalo-Mattila J., Bedogni L., Levorato M., Dutt N.** SIC-EDGE: Semantic iterative ECG compression for edge-assisted wearable systems. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 377–385. doi:10.1109/WoWMoM54355.2022.00036
15. **Rancea A., Anghel I., Cioara T.** Edge computing in healthcare: Innovations, opportunities, and challenges. *Future Internet*, 2024, vol. 16, no. 9, art. 329. doi:10.3390/fi16090329
16. **Hizem M., Bousbia L., Ben Dhiab Y., Aoueileyine M. O.-E., Bouallegue R.** Reliable detection on edge devices for internet of medical things ECG anomaly applications. *Sensors*, 2025, vol. 25, no. 8, art. 2496. doi:10.3390/s25082496
17. **Taylor M. L., Thomas E. E., Snoswell C. L., Smith A. C., Caffery L. J.** Does remote patient monitoring reduce acute care use? A systematic review. *BMJ Open*, 2021, vol. 11, no. 3, art. e040232. doi:10.1136/bmjopen-2020-040232
18. **Leo D. G., Buckley B. J. R., Chowdhury M., Harrison S. L., Isanejad M., Lip G. Y. H., Wright D. J., Lane D. A., TAILOR investigators.** Interactive remote patient monitoring devices for managing chronic

health conditions: Systematic review and meta-analysis. *Journal of Medical Internet Research*, 2022, vol. 24, no. 11, art. e35508. doi:10.2196/35508
19. **Tan S. Y., Sumner J., Wang Y., Yip A. W.** A systematic review of the impacts of remote patient monitoring interventions on safety, adherence, quality-of-life and cost-related outcomes. *npj Digital Medicine*, 2024, vol. 7, art. 192. doi:10.1038/s41746-024-01182-w
20. **Shumba A.-T., Montanaro T., Sergi I., Bramanti A., Ciccarelli M., Rispoli A., Carrizzo A., De Vittorio M., Patrono L.** Wearable technologies and AI at the far edge for chronic heart failure prevention and management: A systematic review and prospects. *Sensors*, 2023, vol. 23, no. 15, art. 6896. doi:10.3390/s23156896
21. **Abououf M., Singh S., Mizouni R., Otrok H.** Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 2, pp. 3446–3457. doi:10.1109/JIOT.2023.3296809

UDC 681.518.3; 615.47:616-072.7
doi:10.31799/1684-8853-2026-5-2-10
EDN: DKDREI

Adaptive operation model for a remote patient monitoring system under communication channel degradation

A. A. Kuzmenko[a], Post-Graduate Student, orcid.org/0009-0006-9031-5082
M. B. Sergeev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277, mbse@guap.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Communication channel degradation has proved to reduce available bandwidth and increase latency or packet loss while the edge device has turned out to retain server connectivity; a growing queue then delaying clinically significant messages and exhausting local memory. Complete outages have created a separate autonomous-storage state. **Purpose:** To develop an adaptive operation model that preserves the priority of critical data under changing channel conditions and limited storage capacity. **Methods:** The study describes the distributed system by connection availability, acknowledged delivery rate, latency, packet loss, queue occupancy, clinical risk, and signal quality. A deterministic state machine controls data handling with hysteresis, temporal confirmation, and a minimum residence time in each mode. A reproducible validation protocol uses a three-channel electrocardiographic signal and controls profiles of bandwidth limitation, latency, packet loss, and complete disconnection. **Results:** The model defines four modes: full-stream transmission, reduced transmission, event-oriented transmission, and autonomous storage with local notification. It assigns data to five priority classes, so an alert and its event context pre-empt current and archive non-critical data. A protected storage area preserves critical records, while a specified synchronization order governs recovery after reconnection. Feasibility conditions constrain alert latency, event-context preservation, and the calculated autonomous operating interval. **Practical relevance:** The model supports engineering requirements for the edge device, storage subsystem, and communication channel before the selection of a hardware platform. **Discussion:** The study makes no numerical performance claim; the authors have designed the proposed protocol for subsequent experimental comparison of the adaptive and baseline strategies.

Keywords — remote patient monitoring, cardiac monitoring, electrocardiography, edge processing, adaptive data transmission, communication channel degradation, local buffer, critical event.

For citation: Kuzmenko A. A., Sergeev M. B. Adaptive operation model for a remote patient monitoring system under communication channel degradation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2026-5-2-10, EDN: DKDREI

References

1. Korneeva I. P., Kramar K. A., Semenova E. A., Sergeev A. M., Yuldashev Z. M. Hardware and software complex for remote monitoring and control of a pregnant woman's health state. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 6, pp. 21–30 (In Russian). doi:10.31799/1684-8853-2021-6-21-30
2. Noah B., Keller M. S., Mosadeghi S., Stein L., Johl S., Delshad S., Tashjian V. C., Lew D., Kwan J. T., Jusufagic A., Spiegel B. M. R. Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials. *npj Digital Medicine*, 2018, vol. 1, art. 20172. doi:10.1038/s41746-017-0002-4
3. Vindrola-Padros C., Singh K., Sidhu M., Georghiou T., Sherlaw-Johnson C., Tomini S. M., Inada-Kim M., Kirkham K., Streetly A., Cohen N., Fulop N. J. Remote home monitoring (virtual wards) for confirmed or suspected COVID-19 patients: A rapid systematic review. *EClinicalMedicine*, 2021, vol. 37, art. 100965. doi:10.1016/j.eclinm.2021.100965
4. Annis T., Pleasants S., Hultman G., Lindemann E., Thompson J. A., Billecke S., Badlani S., Melton G. B. Rapid implementation of A COVID-19 remote patient monitoring program. *Journal of the American Medical Informatics Association*, 2020, vol. 27, no. 8, pp. 1326–1330. doi:10.1093/jamia/ocaa097
5. Gordon W. J., Henderson D., DeSharone A., Fisher H. N., Judge J., Levine D. M., MacLean L., Sousa D., Su M. Y., Boxer R. Remote patient monitoring program for hospital discharged COVID-19 patients. *Applied Clinical Informatics*, 2020, vol. 11, no. 5, pp. 792–801. doi:10.1055/s-0040-1721039
6. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 2016, vol. 3, no. 5, pp. 637–646. doi:10.1109/JIOT.2016. 2579198
7. Satyanarayanan M. The emergence of edge computing. *Computer*, 2017, vol. 50, no. 1, pp. 30–39. doi:10.1109/MC.2017.9
8. Rahmani A. M., Gia T. N., Negash B., Anzanpour A., Azimi I., Jiang M., Liljeberg P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 2018, vol. 78, pp. 641–658. doi:10.1016/j.future.2017.02.014
9. Mutlag A. A., Abd Ghani M. K., Arunkumar N., Mohammed M. A., Mohd O. Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, 2019, vol. 90, pp. 62–78. doi:10.1016/j.future.2018.07.049

10. Serhani M. A., El Kassabi H. T., Ismail H., Nujum Navaz A. ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, 2020, vol. 20, no. 6, art. 1796. doi:10.3390/s20061796
11. Abo-Zahhad M., Ahmed S. M., Elnahas O. A wireless emergency telemedicine system for patients monitoring and diagnosis. *International Journal of Telemedicine and Applications*, 2014, vol. 2014, art. 380787. doi:10.1155/2014/380787
12. Augustyniak P. Adaptive sampling of the electrocardiogram based on generalized perceptual features. *Sensors*, 2020, vol. 20, no. 2, art. 373. doi:10.3390/s20020373
13. Bhattarai A., Peng D., Payne J., Sharif H. Adaptive partition of ECG diagnosis between cloud and wearable sensor net using open-loop and closed-loop switch mode. *IEEE Access*, 2022, vol. 10, pp. 63684–63697. doi:10.1109/ACCESS.2022.3182704
14. Amiri D., Takalo-Mattila J., Bedogni L., Levorato M., Dutt N. SIC-EDGE: Semantic iterative ECG compression for edge-assisted wearable systems. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 377–385. doi:10.1109/WoWMoM54355.2022.00036
15. Rancea A., Anghel I., Cioara T. Edge computing in healthcare: Innovations, opportunities, and challenges. *Future Internet*, 2024, vol. 16, no. 9, art. 329. doi:10.3390/fi16090329
16. Hizem M., Bousbia L., Ben Dhiab Y., Aoueileyine M. O.-E., Bouallegue R. Reliable detection on edge devices for internet of medical things ECG anomaly applications. *Sensors*, 2025, vol. 25, no. 8, art. 2496. doi:10.3390/s25082496
17. Taylor M. L., Thomas E. E., Snoswell C. L., Smith A. C., Caffery L. J. Does remote patient monitoring reduce acute care use? A systematic review. *BMJ Open*, 2021, vol. 11, no. 3, art. e040232. doi:10.1136/bmjopen-2020-040232
18. Leo D. G., Buckley B. J. R., Chowdhury M., Harrison S. L., Isanejad M., Lip G. Y. H., Wright D. J., Lane D. A., TAILOR investigators. Interactive remote patient monitoring devices for managing chronic health conditions: Systematic review and meta-analysis. *Journal of Medical Internet Research*, 2022, vol. 24, no. 11, art. e35508. doi:10.2196/35508
19. Tan S. Y., Sumner J., Wang Y., Yip A. W. A systematic review of the impacts of remote patient monitoring interventions on safety, adherence, quality-of-life and cost-related outcomes. *npj Digital Medicine*, 2024, vol. 7, art. 192. doi:10.1038/s41746-024-01182-w
20. Shumba A.-T., Montanaro T., Sergi I., Bramanti A., Ciccarelli M., Rispoli A., Carrizzo A., De Vittorio M., Patrono L. Wearable technologies and AI at the far edge for chronic heart failure prevention and management: A systematic review and prospects. *Sensors*, 2023, vol. 23, no. 15, art. 6896. doi:10.3390/s23156896
21. Abououf M., Singh S., Mizouni R., Otrok H. Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 2, pp. 3446–3457. doi:10.1109/JIOT.2023.3296809

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая Scopus и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12 языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org

УДК 004.056
doi:10.31799/1684-8853-2026-5-11-20
EDN: AZRPYT

Научные статьи
Articles

Математическая модель и экспериментальная оценка устойчивости квантованных DS-CNN для TinyML-распознавания речевых команд

М. А. Князев[а], *аспирант, orcid.org/0009-0007-3931-7442, maxiknyaz@mail.ru*
М. М. Гусев[б], *магистрант, orcid.org/0009-0004-7023-4328*
[а]*МИРЭА — Российский технологический университет, Вернадского пр., 78, Москва, 119454, РФ*
[б]*Национальный исследовательский университет «Высшая школа экономики», Таллинская ул., 34, Москва, 123458, РФ*

Введение: *квантование позволяет размещать нейронные сети распознавания ключевых слов на микроконтроллерах, но дискретизация весов и активаций изменяет классификационный запас и чувствительность модели к возмущениям.* ***Цель:*** *разработать математическую модель, связывающую ошибку квантования, классификационный запас, локальную устойчивость и ограничения развертывания, и применить ее для сравнения режимов численного представления.* ***Методы:*** *на бинарной подзадаче "yes/no" набора Google Speech Commands v2 сравнивались сверточные сети с разделением по глубине: исходная сеть с 32-разрядными числами с плавающей точкой и сети с восьми- и четырехразрядным целочисленным квантованием после обучения либо с учетом квантования при обучении. Использовались адаптивные атаки проецируемого градиентного спуска в пространстве признаков, акустические искажения с контролем отношения сигнал/шум, пороговый допуск, парето-анализ и интегральный показатель.* ***Результаты:*** *восьмиразрядное квантование после обучения сохранило близкую к исходной точность на чистых данных (95,67 против 95,83 %) и при атаке (90,70 против 91,59 %). Обучение с учетом восьмиразрядного квантования обеспечило соответственно 95,87 и 90,78 % при коэффициенте сохранения точности 0,947. Четырехразрядное квантование после обучения снизило исходную точность до 63,31 %, а обучение с учетом квантования восстановило ее до 88,55 %. Максимальный интегральный показатель 0,5862 получен для восьмиразрядной сети, обученной с учетом квантования, при медиане задержки 41,53 мс на Arduino Nano 33 BLE Sense. При отношении сигнал/шум −5 дБ целевая аугментация этой сети повысила точность с 50,85 до 67,75 %, сократив долю ошибок на 34,4 %.* ***Практическая значимость:*** *предложенная модель позволяет количественно выбирать режим квантования с учетом измеренных показателей качества и задержки при отдельном контроле памяти всей прошивки.*

Ключевые слова *— TinyML, распознавание ключевых слов, DS-CNN, обучение с учетом квантования, квантование после обучения, INT8, INT4, состязательные атаки, PGD, акустические искажения, KWS.*

Для цитирования: Князев М. А., Гусев М. М. Математическая модель и экспериментальная оценка устойчивости квантованных DS-CNN для TinyML-распознавания речевых команд. *Информационно-управляющие системы*, 2026, № 5, с. 11–20. doi:10.31799/1684-8853-2026-5-11-20, EDN: AZRPYT

For citation: Knyazev M. A., Gusev M. M. Mathematical model and experimental robustness assessment of quantized DS-CNNs for TinyML keyword spotting. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 11–20 (In Russian). doi:10.31799/1684-8853-2026-5-11-20, EDN: AZRPYT

Введение

Локальное распознавание ключевых слов (Keyword Spotting, KWS) используется в голосовых интерфейсах носимых устройств, умных колонок и других компонентов персонального интернета вещей. Перенос обработки на устройство уменьшает сетевую задержку и объем передаваемых речевых данных, но требует одновременного соблюдения ограничений постоянной и оперативной памяти, времени вывода и энергопотребления. В машинном обучении на микроконтроллерах (Tiny Machine Learning, TinyML) эти требования обычно выполняются сочетанием компактной архитектуры и целочисленного представления модели [1–10].

Квантование влияет не только на размер модели. Округление весов и активаций распространяется через слои, изменяет логиты, классификационный запас и положение локальной границы решений. Кроме того, дискретность вычислений меняет градиент, используемый при построении состязательных примеров [11–14]. Поэтому вывод об устойчивости нельзя делать только по разрядности: требуется модель, одновременно учитывающая ошибку квантования, локальную чувствительность, тип атаки и аппаратный бюджет.

Метод быстрого знакового градиента (Fast Gradient Sign Method, FGSM) и проецируемый градиентный спуск (Projected Gradient Descent, PGD) остаются базовыми средствами оценки

устойчивости моделей белого ящика [15, 16]. Для сетей с недифференцируемыми или дискретными преобразованиями применяются адаптивные способы обратного прохода и независимые атаки, позволяющие отделить реальную устойчивость от эффекта скрытого градиента [12, 17–19]. Для аудиосистем к этому добавляется различие между воздействием в пространстве признаков и искажением исходного сигнала: одинаковое обозначение бюджета возмущения в этих пространствах не имеет единого физического смысла [20–24].

Методы распознавания речевых команд на устройствах с ограниченными ресурсами развиваются в направлении компактных сверточных, остаточных и импульсных архитектур [1–5, 9, 10]. TFLite Micro обеспечивает исполнение целочисленных моделей на встроенных платформах, а стандартные схемы INT8 (восьмиразрядного целочисленного квантования) используют квантованные веса и активации с накоплением произведений в расширенном целочисленном формате [7, 8]. PTQ (Post-Training Quantization) применяет квантование после обучения, тогда как QAT (Quantization-Aware Training) вводит имитацию квантования в обучающий цикл и позволяет параметрам адаптироваться к ошибкам дискретизации [8, 11].

Влияние квантования на состязательную устойчивость неоднозначно. При небольшом изменении логитов INT8-модель может сохранять границу решений FP32 (32-разрядной модели с плавающей точкой), но грубая дискретизация способна исчерпать классификационный запас. Одновременно ступенчатые активации могут затруднять обычную градиентную атаку, не меняя фактической уязвимости [12–14, 17]. По этой причине современные протоколы сочетают многошаговые атаки, адаптивный обратный проход и независимые алгоритмы проверки [18, 19, 25]. Российские исследования также рассматривают состязательные воздействия, перенос атак и механизмы защиты моделей машинного обучения [26–32].

В речевых системах цифровые атаки в пространстве признаков и акустические искажения отвечают разным моделям угроз [20, 21]. Белый шум, изменение высоты тона и темпа характеризуют эксплуатационную устойчивость, если параметры преобразования не оптимизируются по функции потерь. Запросные и переносимые атаки, напротив, моделируют нарушителя с неполным знанием целевой сети [23, 24]. Такое разделение используется далее при интерпретации результатов.

Цель работы заключается в том, чтобы разработать математическую модель оценки состязательной устойчивости квантованных TinyML-аудиосистем и применить ее для сравнения пяти конфигураций сверточной сети с разделением по глубине (Depthwise Separable Convolutional Neural Network, DS-CNN): FP32, INT8-PTQ, INT8-QAT, INT4-PTQ и INT4-QAT (INT4 — четырехразрядное целочисленное квантование). Научная новизна заключается в совместном использовании оценки классификационного запаса, эмпирических показателей устойчивости, порогового допуска и парето-анализа. Практический результат состоит в количественном сопоставлении точности, устойчивости и размера модели с учетом измеренной задержки на микроконтроллере.

Данные и методика оценки устойчивости

Данные, признаки и архитектура

Эксперимент проводился на бинарной подзадаче распознавания команд “yes” и “no” набора Google Speech Commands v2 [6]. Обучающая, валидационная и тестовая части включали соответственно 6358, 803 и 824 записей. Частота дискретизации составляла 16 кГц, длительность входа — 1 с. Из аудиосигнала строилась логарифмическая мел-спектрограмма с 40 фильтрами, окном 32 мс и шагом 16 мс. Использовалось разбиение без общих дикторов; нормализация рассчитывалась по обучающей части. Признаки поступали на вход компактной DS-CNN с 4514 параметрами.

Для исключения различий исходных FP32-моделей выполнена согласованная серия из трех запусков. Сеть обучалась 50 эпох оптимизатором Adam с начальной скоростью обучения 10^{-3}. В каждом из трех запусков FP32 и варианты с QAT инициализировались одним выбранным состоянием FP32 и дообучались по 10 эпох Adam с шагом 10^{-4} и одинаковым порядком примеров. PTQ применялось к итоговому FP32; состояния выбирались по точности валидации. При обучении и оценке устойчивости в PyTorch 2.8.0 INT8/INT4 обозначают сетки W8A8/W4A4 (8/4 бита для весов и активаций соответственно); свертки и накопление выполнялись в FP32. Для аппаратного измерения задержки использованы преобразованные модели TensorFlow Lite. INT8 и INT4 выполнялись целочисленными ядрами, а контрольная модель FP32 была выполнена с вещественной арифметикой.

Воздействия и показатели

Основной сценарий состязательного воздействия реализован в пространстве признаков. Использовался ансамбль PGD со случайной инициализацией, а именно 40/100 шагов с кросс-

энтропией и 100 шагов с разностью неверного и верного логитов; шаги ε/20, ε/10 и ε/4 соответственно, по три старта. Основное сравнение проводилось при ε = 0,03 в норме $L\infty$ без ограничения признаков интервалом [0, 1]. Прямой проход сохранял округление, обратный использовал сквозную оценку градиента (Straight-Through Estimator, STE) с единичной производной внутри диапазона квантования и нулевой вне его. Учитывалось объединение исходных ошибок и ошибок всех итераций. На общей стратифицированной подвыборке из 128 записей первого запуска (по 64 каждого класса) дополнительно проверялись обычный градиент, перенос с FP32 и стохастическая аппроксимация с одновременным возмущением (Simultaneous Perturbation Stochastic Approximation, SPSA) [12, 17–19]. Диагностические PGD-40/100 и перенос PGD-100 с FP32 использовали разность логитов, шаг ε/10 и три старта. SPSA выполнялась за 128 шагов по 32 двусторонних направления с радиусом ε/4 и шагом Adam ε/20: 8323 запроса на пример; учитывались ошибки всех пробных точек. Дополнительный блок в пространстве сигнала включал аддитивный белый гауссовский шум на сетке отношения сигнал/шум (Signal-to-Noise Ratio, SNR) от 30 до −5 дБ.

Для каждой конфигурации определялись точность на исходных данных Acc_{clean}, точность после атаки Acc_{adv}, абсолютное снижение точности ΔAcc и коэффициент сохранения R_{ret}. Ресурсная составляющая содержит полный размер контейнера параметров S, в том числе заголовок и задержку L. Размер контейнера не включает код прошивки и среды выполнения и не равен занятому объему Flash. На Arduino измерялось время полного вызова dscnn_run при пакете 1 и фиксированном тензоре признаков 1 × 40 × 61. После пяти прогревочных вызовов выполнялись 50 измеряемых; для каждого сохранялись отсчеты DWT_CYCCNT до и после вызова. При частоте 64 МГц задержка в миллисекундах равна ΔC/64 000; медиану см. в табл. 2. В интервал включены распаковка весов INT4, свертки, пулинг, классификатор и argmax. Загрузка модели при инициализации, извлечение признаков и обмен через Serial исключены; прерывания оставлены включенными. Сценарные бюджеты составляли $S_{\max} = 1024$ КиБ и $L_{\max} = 100$ мс.

Схема анализа

Сначала сравнивались исходная и состязательная точности. Затем вычислялись нормированные размер и задержка, интегральная полезность и пороговый допуск. Парето-анализ выполнялся по четырем критериям: максимизация Acc_{clean} и Acc_{adv} при минимизации S и L.

Математическая модель

Квантование и классификационный запас

Пусть $x \in \mathbb{R}^{T}$ — нормированный аудиосигнал, $\varphi(x)$ — его частотно-временное представление, а $F_b(x) \in \mathbb{R}^{K}$ — логиты сети в режиме b. Предсказание задается как

$$\hat{y}_b(x) = \arg\max_{k \in \{1, \ldots, K\}} [F_b(x)]_k. \quad (1)$$

Целочисленное кодирование и восстановление вещественного значения определяются раздельно:

$$q_b(r; s, z_0) = clip\left(\left[\frac{r}{s}\right] + z_0, q_{\min}, q_{\max}\right); \quad (2)$$

$$Q_b(r; s, z_0) = s\left(q_b(r; s, z_0) - z_0\right),$$
$$q_{\min} = -q_{\max}, q_{\max} = 2^{b-1} - 1. \quad (3)$$

Послойное распространение квантования имеет вид

$$h_0 = Q^a_{b,0}(\varphi(x)), W_l^{(b)} = Q^w_{b,l}(W_l); \quad (4)$$

$$h_l = Q^a_{b,l}\left[\sigma_l\left(W_l^{(b)} h_{l-1} + b_l^{(b)}\right)\right], F_b(x) = h_L. \quad (5)$$

Для размеченного объекта введем классификационный запас

$$m_b(x, y) = [F_b(x)]_y - \max_{k \neq y} [F_b(x)]_k \quad (6)$$

и ошибку квантования по логитам

$$e_b(x) = \left\| F_b(x) - F_{32}(x) \right\|_\infty. \quad (7)$$

В режиме FP32 квантователи тождественны. Для оценки e_b используется вещественная копия тех же итоговых весов; для QAT это дает возможность отделить квантование от изменения весов при дообучении. В опыте веса и вход использовали симметричные диапазоны кодов (3): [−127; 127] / [−7; 7], выходы ReLU (Rectified Linear Unit — функции выпрямления) и усреднения являются беззнаковыми [0; 255] / [0; 15]. Масштабы весов задавались по максимуму модуля в выходном канале, а масштабы активаций — по максимуму модуля на 512 обучающих примерах и затем фиксировались. В реализации (5) смещения и конечные логиты остаются FP32; активация и квантователь последнего слоя тождественны.

Из определения нормы следует $[F_b]_y \geq [F_{32}]_y - e_b$ и $[F_b]_k \leq [F_{32}]_k + e_b$. Поэтому

$$m_b(x, y) \geq m_{32}(x, y) - 2e_b(x). \quad (8)$$

Соотношение (8) задает механизм влияния разрядности на качество: пока $2e_b(x) < m_{32}(x, y)$, квантование не исчерпывает запас FP32-модели

для данного объекта; при нарушении этого условия класс может измениться уже без внешнего воздействия.

Локальная устойчивость

Обозначение $F_b(z)$ относится к классификатору без повторного извлечения признаков. Радиус $r_b(x)$ определяется в норме L_∞ пространства признаков. Пусть разности логитов $g_{b,yk}(z) = [F_b(z)]_y - [F_b(z)]_k$ локально липшицевы с константой не более $2L_b$:

$$\left|g_{b,yk}(z+\Delta) - g_{b,yk}(z)\right| \le 2L_b \left\|\Delta\right\|. \quad (9)$$

Тогда достаточное условие сохранения класса при $\|\Delta\| \le \varepsilon_z$ и нижняя оценка локального радиуса имеют вид

$$m_b(x, y) > 2L_b\varepsilon_z,\ r_b(x) \ge \frac{m_b(x, y)}{2L_b}. \quad (10)$$

Совместно с (8) получаем

$$r_b(x) \ge \frac{\max\{m_{32}(x, y) - 2e_b(x), 0\}}{2L_b}. \quad (11)$$

Оценки (10), (11) являются условными. При $L_b > 0$ неравенство (9) должно выполняться во всем шаре L_∞, содержащем оцениваемый радиус. Точное округление при пересечении порогов этого не гарантирует. Измеряемый максимум конечных отношений $\frac{|\Delta g|}{2\|\Delta z\|_\infty}$ по PGD-возмущению и случайным направлениям является выборочной оценкой чувствительности, а не ее верхней границей.

Если предварительная обработка локально удовлетворяет

$$\left\|\varphi(x+\delta) - \varphi(x)\right\| \le L_\varphi \left\|\delta\right\|, \quad (12)$$

то для бюджета ε_x в пространстве сигнала достаточно условия

$$m_b(x,y) > 2L_bL_\varphi\varepsilon_x. \quad (13)$$

Таким образом, эффект QAT может проявляться через увеличение запаса m_b, уменьшение локальной чувствительности L_b или их сочетание. Напротив, снижение качества INT4 может соответствовать ситуации, в которой ошибка e_b исчерпывает запас для значительной доли объектов.

Метрики устойчивости

PGD в пространстве признаков задается рекурсией

$$z^{(t+1)} = \Pi_{B_\infty(z,\varepsilon_z)}\left(z^{(t)} + \alpha\,\mathrm{sign}\nabla_z L(F_b(z^{(t)}), y)\right). \quad (14)$$

При атаке в пространстве признаков предсказание в (16) вычисляется непосредственно по атакованному тензору. Для набора из N объектов точности и их производные определяются как

$$Acc_{clean}(b) = \frac{1}{N}\sum_{i=1}^{N} 1[\hat{y}_b(x_i) = y_i]; \quad (15)$$

$$Acc_{adv}(b, A) = \frac{1}{N}\sum_{i=1}^{N} 1[\hat{y}_b(x_i^A) = y_i]; \quad (16)$$

$$\Delta Acc = Acc_{clean} - Acc_{adv},\ R_{ret} = \frac{Acc_{adv}}{Acc_{clean}}. \quad (17)$$

Для оценки аддитивного шума используется энергетическое отношение сигнал/шум

$$SNR_{dB}(x,\delta) = 10\log_{10}\frac{\|x\|_2^2}{\|\delta\|_2^2} = 20\log_{10}\frac{\|x\|_2}{\|\delta\|_2}. \quad (18)$$

Допуск и интегральный показатель

Допустимое множество моделей задается системой порогов

$$F = \left\{ b : \begin{matrix} Acc_{clean}(b) \ge A_{\min},\ R_{ret}(b) \ge R_{\min} \\ S(b) \le S_{\max},\ L(b) \le L_{\max} \end{matrix} \right\}. \quad (19)$$

В расчетах приняты $A_{\min} = 0{,}95$, $R_{\min} = 0{,}90$, $S_{\max} = 1024$ КиБ и $L_{\max} = 100$ мс. Для сравнительного ранжирования определен исходный показатель

$$U_0(b) = 0{,}30Acc_{clean}(b) + 0{,}40Acc_{adv}(b) - 0{,}15\frac{S(b)}{S_{\max}} - 0{,}15\frac{L(b)}{L_{\max}}. \quad (20)$$

Пороговый показатель принимает значение $U(b) = U_0(b)$ для $b \in F$ и $U(b) = -\infty$ в противном случае. Такое разделение не позволяет высокой суммарной оценке компенсировать нарушение обязательного ограничения.

Результаты

Точность и устойчивость в пространстве признаков

Результаты ансамбля PGD при $\varepsilon = 0{,}03$ приведены в табл. 1. Для точности и R_{ret} указаны среднее и стандартное отклонения трех запусков на одних 824 записях; ΔAcc и S представлены средними. INT8-PTQ сохранил близкую к FP32 исходную точность (95,67 против 95,83 %) и изменил точность при атаке на 0,89 п.п. Коэффициенты сохранения также близки: 0,948 и 0,956.

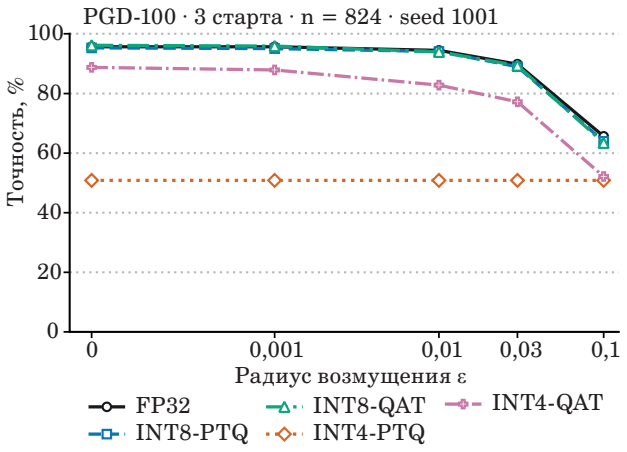
INT8-QAT показал точность при PGD 90,78 %, при этом снижение относительно исходных данных

■ ***Таблица 1.*** Точность DS-CNN при различных режимах квантования
■ ***Table 1.*** DS-CNN accuracy for different quantization modes

Модель	Acc_{clean}, %	Acc_{adv}, %	ΔAcc, п.п.	R_{ret}	Размер, КиБ
FP32	95,83 ± 0,25	91,59 ± 1,54	4,25	0,956 ± 0,014	21,20
INT8-PTQ	95,67 ± 0,37	90,70 ± 1,73	4,98	0,948 ± 0,015	14,91
INT8-QAT	95,87 ± 0,21	90,78 ± 1,58	5,10	0,947 ± 0,019	14,91
INT4-PTQ	63,31 ± 21,58	58,21 ± 12,86	5,10	0,942 ± 0,099	12,90
INT4-QAT	88,55 ± 2,79	75,24 ± 4,43	13,31	0,849 ± 0,023	12,90

составило 5,10 п.п. Парная разность Acc_{adv} между INT8-QAT и INT8-PTQ равна 0,08 ± 0,19 п.п. На общей подвыборке из 128 примеров INT8-QAT дает 99,22 % при обычной PGD-40 через округление и 91,41 % при STE-PGD-100; перенос с FP32 и SPSA дают 92,97 и 96,88 %. Прямые проходы с STE и точным округлением совпали. Для INT4-QAT STE-PGD-100 дает 82,03 %, для SPSA – 73,44 %, а объединение ошибок основного ансамбля и диагностических атак на той же подвыборке – 71,88 % (11 дополнительных ошибок относительно основного ансамбля). Следовательно, обычный градиент завышает устойчивость, а конечная STE-PGD не исчерпывает найденную уязвимость INT4; результаты подвыборки учитываются отдельно от табл. 1.

При INT4-PTQ исходная точность снизилась до 63,31 %. Большое значение R_{ret} = 0,942 в этом случае отражает сохранение уже низкой точности и не является признаком практической устойчивости. QAT восстановил исходную точность INT4 до 88,55 % и точность при PGD до 75,24 %. Прирост относительно INT4-PTQ составил соответственно 25,24 и 17,03 п.п., что демонстрирует способность обучения частично компенсировать ошибку грубой дискретизации.



■ Зависимость точности при состязательном воздействии от бюджета PGD-100
■ Accuracy under adversarial perturbations versus the PGD-100 budget

Зависимость от бюджета атаки показана на рисунке для первого запуска обучения (PGD-100 по разности логитов, шаг ε/10, три старта). INT8-конфигурации следуют близким траекториям, тогда как INT4-PTQ остается около 51 % вследствие потери качества еще на исходных данных. Кривая отдельной атаки не заменяет ансамбль табл. 1.

Расчет показателей ресурсов

Запуск выполнялся на Arduino Nano 33 BLE Sense с nRF52840, Cortex-M4F, 64 МГц, 1024 КиБ Flash и 256 КиБ оперативной памяти (RAM) (https://docs.arduino.cc/hardware/nano-33-ble-sense/; дата обращения: 15.09.2026). Использованы TensorFlow Lite for Microcontrollers (TFLM), CMSIS-NN (Common Microcontroller Software Interface Standard — Neural Network) 3.1.0 из CMSIS 5.9.0 и Arduino Mbed OS core 4.1.5 [7] (https://github.com/ARM-software/CMSIS-NN; дата обращения: 15.09.2026). Для INT8 применялись целочисленные ядра arm_convolve_s8, arm_depthwise_conv_s8 и arm_avgpool_s8 с накоплением в int32 и выходом int8. В INT4 веса диапазона [–7; 7] хранились по два в байте и распаковывались до int8 перед вызовом ядер; после сверток активации ограничивались 16 уровнями [0; 15] при хранении в int8 с теми же масштабами, что в PyTorch. FP32-конфигурация использует вещественный прямой проход.

Перед измерением на 824 исходных тестовых записях для INT8-PTQ, INT8-QAT, INT4-PTQ и INT4-QAT получено по 824/824 совпадения классов между платой и PyTorch. Максимальные абсолютные расхождения логитов составили $2{,}1 \cdot 10^{-3}$ для INT8 и $7{,}4 \cdot 10^{-3}$ для INT4. Эта проверка относится к исходным записям; оценки при PGD в табл. 1 получены в PyTorch. В табл. 2 приведены измеренные медианы задержки, нормированные показатели и значения U_0, рассчитанные по формуле (20) без промежуточного округления. Например, для INT8-QAT

$$U_0 = 0{,}30 \cdot 0{,}958738 + 0{,}40 \cdot 0{,}907767 - \\ - 0{,}15 \cdot \frac{14{,}9095}{1024} - 0{,}15 \cdot \frac{41{,}53}{100} \approx 0{,}5862. \quad (21)$$

■ ***Таблица 2.*** Задержка на Arduino и интегральная полезность конфигураций

■ ***Table 2.*** Arduino latency and composite utility of the configurations

Конфигурация	L, мс	S/S_{max}	L/L_{max}	U_0
FP32	72,43	0,0207	0,7243	0,542092
INT8-PTQ	41,87	0,0146	0,4187	0,584809
INT8-QAT	41,53	0,0146	0,4153	0,586249
INT4-PTQ	39,21	0,0126	0,3921	0,362070
INT4-QAT	38,96	0,0126	0,3896	0,506296

■ ***Таблица 3.*** Точность при акустических искажениях

■ ***Table 3.*** Accuracy under acoustic distortions

Условие	Контроль, %	Аугментация, %	Разность, п.п.
Исходные данные	95,95 ± 0,19	95,35 ± 0,14	–0,61 ± 0,21
SNR –5 дБ	50,85 ± 0,00	67,75 ± 3,65	16,90 ± 3,65
SNR 0 дБ	50,85 ± 0,00	79,18 ± 2,84	28,33 ± 2,84
SNR 10 дБ	51,17 ± 0,56	84,99 ± 5,80	33,82 ± 5,36
SNR 30 дБ	89,66 ± 3,26	93,50 ± 1,10	3,84 ± 2,22

Для S и точности использованы средние трех запусков обучения; L — медиана 50 запусков каждой конфигурации. Максимум U_0 получен для INT8-QAT: 0,586249 против 0,584809 у INT8-PTQ. Медиана INT8-QAT ниже FP32 на 42,66 %. По неокругленным значениям все пять конфигураций входят в парето-фронт; в каждой паре PTQ/QAT средние размеры контейнеров различаются лишь на 1,67 байта из-за заголовка, что не имеет самостоятельной практической значимости.

Для всех пяти конфигураций архитектурная сложность прохода составляет 2 618 944 операции умножения с накоплением (MAC) без учета активаций, квантования и обмена с памятью. Различия задержек характеризуют используемые реализации; уменьшение разрядности хранения весов не означает пропорционального уменьшения числа MAC.

Пороговый анализ дополняет интегральное ранжирование. Все пять медиан задержки ниже $L_{max} = 100$ мс. FP32, INT8-PTQ и INT8-QAT выполняют также пороги качества и размера и входят в F; INT4-конфигурации не достигают $A_{min} = 0,95$. Порог $S_{max} = 1024$ КиБ совпадает с полной емкостью Flash и используется для сравнения контейнеров, а не как измеренный свободный бюджет прошивки. Принадлежность F по этим показателям не подтверждает размещение всей прошивки в памяти или соблюдение предела задержки в каждом запуске.

Устойчивость к акустическим искажениям

Результаты в пространстве сигнала приведены в табл. 3. В отдельном парном опыте INT8-QAT контроль и аугментированная ветвь из общего FP32-состояния обучались ровно 10 эпох с одинаковыми остальными условиями. Сравнивались конечные состояния. Аугментация была представлена белым гауссовским шумом с вероятностью 0,5 и равномерным SNR от –5 до 10 дБ. Тестовые записи отделены по дикторам; шум совпадал по типу, но формировался независимо. При каждом SNR для каждой тестовой записи формировались три независимые реализации шума, одинаковые для контрольной и аугментированной модели. Точности трех реализаций усреднялись внутри каждого запуска, затем вычислялись среднее и стандартное отклонения трех запусков.

При –5 дБ точность выросла с 50,85 до 67,75 %, т. е. на 16,90 ± 3,65 п.п. Доля ошибок уменьшилась с 49,15 до 32,25 %, или на 34,4 %. Контрольная модель INT8-QAT при –5 дБ всегда выбирала команду “yes”, и 50,85 % соответствует доле этого класса (419/824). На исходных данных точность снизилась на 0,61 п.п. Этот результат показывает эффективность аугментации для исследованного белого шума; перенос на другие акустические условия не проверялся.

Ограничения исследования

Экспериментальная часть ограничена бинарной подзадачей “yes/no”, одной архитектурой DS-CNN и заданным ансамблем PGD-40/100. Перенос и SPSA дополнительно проверены на 128 примерах одного запуска. Поэтому численные границы не следует непосредственно переносить на полную 35-классовую задачу Speech Commands, другие архитектуры или иные нормы возмущения. Полученные значения характеризуют сравниваемые конфигурации в заданном протоколе, а не сертифицированный радиус устойчивости.

Сравнение включает в себя размеры контейнеров, число операций и медианы задержки на плате. Пиковая RAM и энергопотребление не измерялись. В целочисленных вариантах один тензор активаций $32 \times 20 \times 31$ занимает 19 840 байт при хранении в int8; это расчетный объем одного тензора, а не пиковая RAM с учетом арены TFLM, рабочих буферов ядер, распаковки весов и стека. Совпадение классов после конвертации на исходных данных не устанавливает совпадение устойчивости на атакованных входах.

Акустические результаты относятся к синтетическим искажениям сигнала; они описывают эксплуатационную устойчивость, но не полный тракт воспроизведения и записи в помещении.

Обсуждение

Математическая модель описывает различие между конфигурациями через два взаимосвязанных фактора: ошибку квантования e_b и локальную чувствительность L_b. Режим INT8-PTQ почти не изменил агрегированную исходную точность и приблизил кривую FP32 при PGD. Это согласуется с ситуацией, в которой ошибка квантования для большинства объектов меньше половины их исходного классификационного запаса. Следовательно, PTQ в данном режиме выступает прежде всего как средство уменьшения объема хранения, а не как самостоятельный механизм защиты.

Для проверки модели рассчитаны логиты на 824 записях трех запусков; объединенные наблюдения используются описательно. Для INT8-PTQ, INT8-QAT, INT4-PTQ и INT4-QAT медианы ошибки квантования по логитам относительно вещественной копии тех же весов равны 0,189; 0,195; 5,467 и 4,796; доли объектов с положительной правой частью (8) — 94,62; 94,54; 26,74 и 38,63 % соответственно. Среди первоначально правильно классифицированных объектов INT8-QAT медиана запаса равна 5,412 при сохранении класса под PGD и 0,830 при найденной атаке. Чувствительность оценивалась по сохраненному PGD-возмущению и трем случайным направлениям: по одному при радиусах 0,001; 0,01; 0,03 (генератор 31415). Медиана выборочной чувствительности равна 24,054 против 16,981 для FP32. Нарушений (8) при абсолютном допуске $2 \cdot 10^{-5}$ и относительном 10^{-6} к максимальному модулю логита вещественной копии не обнаружено.

Интегральный показатель и пороговый допуск решают разные задачи. U_0 задает ранжирование компромиссов, а множество F исключает конфигурации, нарушающие хотя бы одно обязательное требование. Поэтому большой R_{ret} INT4-PTQ не компенсирует низкую исходную точность. INT8-режимы позволяют уменьшить размер контейнера и медиану задержки при близком исходном качестве; в принятом сценарии максимум U_0 достигается у INT8-QAT.

Акустический блок дополняет оценку атак в пространстве признаков. Возмущение мелспектрограммы характеризует локальную геометрию классификатора, тогда как белый шум оценивает устойчивость всего тракта формирования признаков. Рост точности на 16,90 п.п. после целевой аугментации при –5 дБ подтверждает практическую ценность обучения на условиях, близких к границе эксплуатации. Такой подход совместим с TinyML, поскольку не увеличивает вычислительную сложность уже развернутой модели.

Заключение

Разработана математическая модель, связывающая ошибку квантования по логитам, классификационный запас и локальную чувствительность квантованной DS-CNN. Получена нижняя оценка $m_b \geq m_{32} - 2e_b$ и условная оценка локального радиуса при выполнении (9). Модель дополнена эмпирическими метриками, пороговым допуском и интегральным показателем развертывания.

Экспериментальное сравнение показало три характерных режима. INT8-PTQ сохранил близкую к FP32 исходную точность и близкое поведение при PGD. INT8-QAT обеспечил 95,87 % на исходных данных, 90,78 % при PGD и $R_{ret} = 0{,}947$. INT4-PTQ снизил исходную точность до 63,31 %, тогда как INT4-QAT частично восстановил ее до 88,55 %.

FP32 и обе INT8-конфигурации входят в F при принятых порогах качества, размера контейнера и медианы задержки. Максимальный $U_0 = 0{,}5862$ получен для INT8-QAT при $L = 41{,}53$ мс. INT8 сохраняет близкое к FP32 качество при меньших размере контейнера и медиане задержки; INT4-QAT применим при допустимости снижения исходной точности. Целевая аугментация при низком SNR дополняет квантование: при –5 дБ она повысила точность INT8-QAT на 16,90 п.п. и сократила долю ошибок на 34,4 %. Совместное применение математической модели, пороговых требований и парето-анализа позволяет выбирать режим квантования с учетом измеренных показателей качества и задержки при отдельном контроле памяти всей прошивки.

Литература

1. **Вольф Д. А., Туровский Я. А.** Распознавание речевых команд с применением сингулярного спектрального анализа в системах с ограниченными ресурсами. *Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1. Естественные и технические науки*, 2021, № 1, с. 3–11. doi:10.46418/2079-8199_2021_1_1, EDN: PNZXAY

2. **Левонович Н. И.** О методе распознавания голосовых команд с применением особого преобразования спектральных плотностей. *Моделирование и анализ данных*, 2022, т. 12, № 3, с. 49–57. https://psyjournals.ru/journals/mda/archive/2022_n3/Levonovich (дата обращения: 13.10.2026). doi:10.17759/mda.2022120304

3. **Сбоев А. Г., Рыбка Р. Б., Серенко А. В., Селиванов А. Г., Софонов А. О.** Классификация звука импульсной нейронной сетью, удовлетворяющей ограничениям нейропроцессора Алтай и при этом использующей полный динамический диапазон весов. *Вестник Военного инновационного технополиса «ЭРА»*, 2022, т. 3, № 3, с. 314–321. doi:10.56304/s2782375x22030093, EDN: HFEHPA
4. **Аксёнов А. А., Рюмина Е. В., Рюмин Д. А., Ивaнько Д. В., Карпов А. А.** Нейросетевой метод визуального распознавания голосовых команд водителя с использованием механизма внимания. *Научно-технический вестник информационных технологий, механики и оптики*, 2023, т. 23, № 4, с. 767–775. doi:10.17586/2226-1494-2023-23-4-767-775, EDN: ADSTLP
5. **Жолондковский В. В., Бочаров Ю. И., Бутузов В. А.** Нейросетевое устройство для распознавания речевых команд на базе аппаратных ускорителей семейства NeuroMatrix. *Безопасность информационных технологий*, 2024, т. 31, № 2, с. 134–141. doi:10.26583/bit.2024.2.09, EDN: MDJSMM
6. **Warden P.** Speech commands: A dataset for limited-vocabulary speech recognition, 2018. arXiv:1804.03209. https://arxiv.org/abs/1804.03209 (дата обращения: 13.10.2026). doi:10.48550/arXiv.1804.03209
7. **David R., Duke J., Jain A., Janapa Reddi V., Jeffries N., Li J., Kreeger N., Nappier I., Natraj M., Regev S., Rhodes R., Wang T., Warden P.** TensorFlow lite micro: Embedded machine learning on TinyML systems. *Proceedings of Machine Learning and Systems*, 2021, vol. 3, pp. 800–811.
8. **Jacob B., Kligys S., Chen B., Zhu M., Tang M., Howard A., Adam H., Kalenichenko D.** Quantization and training of neural networks for efficient integer-arithmetic-only inference. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018, pp. 2704–2713. doi:10.1109/cvpr.2018.00286
9. **Kim B., Chang S., Lee J., Sung D.** Broadcasted residual learning for efficient keyword spotting. *Interspeech 2021*, 2021, pp. 4538–4542. doi:10.21437/interspeech.2021-383
10. **López-Espejo I., Tan Z.-H., Hansen J. H. L., Jensen J.** Deep spoken keyword spotting: An overview. *IEEE Access*, 2022, vol. 10, pp. 4169–4199. doi:10.1109/access.2021.3139508
11. **Nahshan Y., Chmiel B., Baskin C., Zheltonozhskii E., Banner R., Bronstein A. M., Mendelson A.** Loss aware post-training quantization. *Machine Learning*, 2021, vol. 110, no. 11–12, pp. 3245–3262. doi:10.1007/s10994-021-06053-z
12. **Gupta K., Ajanthan T.** Improved gradient-based adversarial attacks for quantized networks. *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022, vol. 36, no. 6, pp. 6810–6818. doi:10.1609/aaai.v36i6.20637
13. **Xiao Y., Liu A., Zhang T., Qin H., Guo J., Liu X.** RobustMQ: benchmarking robustness of quantized models. *Visual Intelligence*, 2023, vol. 1, art. 30. doi:10.1007/s44267-023-00031-w
14. **Ayaz F., Zakariyya I., Cano J., Keoh S. L., Singer J., Pau D., Kharbouche-Harrari M.** Improving robustness against adversarial attacks with deeply quantized neural networks. *2023 International Joint Conference on Neural Networks (IJCNN)*, 2023, pp. 1–8. doi:10.1109/ijcnn54540.2023.10191429
15. **Goodfellow I. J., Shlens J., Szegedy C.** Explaining and harnessing adversarial examples. *International Conference on Learning Representations*, 2015. arXiv:1412.6572. https://arxiv.org/abs/1412.6572 (дата обращения: 13.10.2026).
16. **Madry A., Makelov A., Schmidt L., Tsipras D., Vladu A.** Towards deep learning models resistant to adversarial attacks. *International Conference on Learning Representations*, 2018. arXiv:1706.06083. https://arxiv.org/abs/1706.06083 (дата обращения: 13.10.2026).
17. **Athalye A., Carlini N., Wagner D.** Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. *Proceedings of the 35th International Conference on Machine Learning. Proceedings of Machine Learning Research*, 2018, vol. 80, pp. 274–283.
18. **Croce F., Hein M.** Reliable evaluation of adversarial robustness with an ensemble of diverse parameter-free attacks. *Proceedings of the 37th International Conference on Machine Learning. Proceedings of Machine Learning Research*, 2020, vol. 119, pp. 2206–2216.
19. **Carlini N., Athalye A., Papernot N., Brendel W., Rauber J., Tsipras D., Goodfellow I. J., Madry A., Kurakin A.** On evaluating adversarial robustness, 2019. arXiv:1902.06705. https://arxiv.org/abs/1902.06705 (дата обращения: 13.10.2026). doi:10.48550/arXiv.1902.06705
20. **Abdullah H., Warren K., Bindschaedler V., Papernot N., Traynor P.** SoK: The faults in our ASRs: An overview of attacks against Automatic Speech Recognition and speaker identification systems. *IEEE Symposium on Security and Privacy*, 2021, pp. 730–747. doi:10.1109/sp40001.2021.00014
21. **Bhanushali A. R., Mun H., Yun J.** Adversarial attacks on Automatic Speech Recognition (ASR): A survey. *IEEE Access*, 2024, vol. 12, pp. 88279–88302. doi:10.1109/access.2024.3416965
22. **López-Espejo I., Tan Z.-H., Jensen J.** A novel loss function and training strategy for noise-robust keyword spotting. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 2021, vol. 29, pp. 2254–2266. doi:10.1109/taslp.2021.3092567
23. **Wang Q., Zheng B., Li Q., Shen C., Ba Z.** Towards query-efficient adversarial attacks against Automatic Speech Recognition systems. *IEEE Transactions on Information Forensics and Security*, 2021, vol. 16, pp. 896–908. doi:10.1109/tifs.2020.3026543
24. **Tong C., Zheng X., Li J., Ma X., Gao L., Xiang Y.** Query-efficient black-box adversarial attacks on Automatic Speech Recognition. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 2023, vol. 31, pp. 3981–3992. doi:10.1109/taslp.2023.3304476

25. **Croce F., Andriushchenko M., Sehwag V., Debenedetti E., Flammarion N., Chiang M., Mittal P., Hein M.** RobustBench: A standardized adversarial robustness benchmark. *Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks*, 2021, vol. 1.
26. **Куликов Д. А., Платонов В. В.** Состязательные атаки на системы обнаружения вторжений, использующих LSTM-классификатор. *Проблемы информационной безопасности. Компьютерные системы*, 2021, № 2, с. 48–56. EDN: CLLJVV
27. **Парфёнов Д. И., Болодурина И. П., Гришина Л. С., Жигалов А. Ю., Толмачев С. В.** Исследование эффективности трансферного обучения при проведении состязательных атак. *Современные информационные технологии и ИТ-образование*, 2022, т. 18, № 4, с. 861–871. doi:10.25559/sitito.18.202204.861-871, EDN: DDZPSG
28. **Фомичева С. Г., Беззатеев С. В.** Механизмы защиты моделей машинного обучения от состязательных атак. *T-Comm: Телекоммуникации и транспорт*, 2023, т. 17, № 10, с. 28–42. doi:10.36724/2072-8735-2023-17-10-28-42
29. **Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А., Никольская А. Г.** Состязательные атаки против системы обнаружения вторжений, основанной на применении методов машинного обучения. *Проблемы информационной безопасности. Компьютерные системы*, 2023, № 4, с. 156–190. doi:10.48612/jisp/eatr-5pxb-akt8, EDN: XTMDJV
30. **Вершков Н. А., Бабенко М. Г., Кучукова Н. Н., Кучуков В. А., Кучеров Н. Н.** Поперечнослойное разделение искусственных нейронных сетей для классификации изображений. *Компьютерная оптика*, 2024, т. 48, № 2, с. 312–320. doi:10.18287/2412-6179-co-1278
31. **Баев А. В., Самонов А. В., Сафонов В. М., Краснов С. В., Малышев С. Р.** Методы защиты моделей нейронных сетей от состязательных атак уклонения и отравления. *Автоматизация процессов управления*, 2024, № 4 (78), с. 39–48. doi:10.35752/1991-2927_2024_4_78_39
32. **Котенко И. В., Саенко И. Б., Лаута О. С., Васильев Н. А., Садовников В. Е.** Метод противодействия состязательным атакам на системы классификации изображений. *Вопросы кибербезопасности*, 2025, № 2 (66), с. 114–123. doi:10.21681/2311-3456-2025-2-114-123, EDN: MKWZFT

UDC 004.056
doi:10.31799/1684-8853-2026-5-11-20
EDN: AZRPYT

Mathematical model and experimental robustness assessment of quantized DS-CNNs for TinyML keyword spotting

M. A. Knyazev[a], Post-Graduate Student, orcid.org/0009-0007-3931-7442, maxiknyaz@mail.ru
M. M. Gusev[b], Master Student, orcid.org/0009-0004-7023-4328
[a]MIREA — Russian Technological University, 78, Vernadsky Ave., 119454, Moscow, Russian Federation
[b]HSE University, 34, Tallinskaia St., 123458, Moscow, Russian Federation

Introduction: Quantization enables keyword-spotting networks to operate on microcontrollers, but alters classification margins and sensitivity to perturbations. **Purpose:** To develop a model linking quantization error, classification margin, local robustness, and deployment constraints, and compare numerical representations. **Methods:** Depthwise separable convolutional networks have been evaluated on the binary "yes/no" subset of Google Speech Commands v2: a 32-bit floating-point baseline and 8-bit and 4-bit integer networks obtained by post-training quantization or quantization-aware training. The evaluation has combined adaptive projected-gradient-descent attacks in feature space, acoustic distortions with controlled signal-to-noise ratios, threshold admission, Pareto analysis, and a composite score. **Results:** Eight-bit post-training quantization has retained clean accuracy close to the baseline (95.67% versus 95.83%) and similar accuracy under attack (90.70% versus 91.59%). Eight-bit quantization-aware training has achieved 95.87% clean accuracy and 90.78% accuracy under attack, with an accuracy retention coefficient of 0.947. Four-bit post-training quantization has reduced clean accuracy to 63.31%, whereas quantization-aware training has restored it to 88.55%. With latency measured on Arduino Nano 33 BLE Sense, the eight-bit network trained with quantization awareness has achieved the highest composite score, 0.5862, at a median latency of 41.53 milliseconds. At a signal-to-noise ratio of −5 decibels, targeted augmentation of this network has improved accuracy from 50.85% to 67.75% and reduced the error rate by 34.4%. **Practical relevance:** The proposed model supports quantitative selection of a quantization mode using measured quality and latency, subject to separate checks of full-firmware memory requirements.

Keywords – TinyML, keyword spotting, DS-CNN, post-training quantization, quantization-aware training, INT8, INT4, adversarial robustness, PGD, acoustic distortions, KWS.

For citation: Knyazev M. A., Gusev M. M. Mathematical model and experimental robustness assessment of quantized DS-CNNs for TinyML keyword spotting. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 11–20 (In Russian). doi:10.31799/1684-8853-2026-5-11-20, EDN: AZRPYT

References

1. Wolf D. A., Turovsky Ya. A. Recognition of speech commands based on singular spectral analysis in systems with limited resources. *Vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta tekhnologii i dizajna. Seriya 1. Estestvennye i tekhnicheskie nauki* [Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and Technical Sciences], 2021, no. 1, pp. 3–11 (In Russian). doi:10.46418/2079-8199_2021_1_1, EDN: PNZXAY
2. Levonovich N. I. Voice commands recognition method that uses special spectral density transform. *Modelirovanie i analiz dannyh* [Modelling and Data Analysis], 2022, vol. 12, no. 3, pp. 49–57. Available at: https://psyjournals.ru/en/journals/mda/archive/2022_n3/Levonovich (accessed 13 October 2026) (In Russian). doi:10.17759/mda.2022120304
3. Sboev A. G., Rybka R. B., Serenko A. V., Selivanov A. G., Sofonov A. O. Sound classification by a spiking neural network satisfying Altai neuroprocessor constraints. *Vestnik Voenno-*

go innovatsionnogo tekhnopolisa "ERA", 2022, vol. 3, no. 3, pp. 314–321 (In Russian). doi:10.56304/s2782375x22030093, EDN: HFEHPA
4. Axyonov A. A., Ryumina E. V., Ryumin D. A., Ivanko D. V., Karpov A. A. Neural network-based method for visual recognition of driver's voice commands using attention mechanism. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 4, pp. 767–775 (In Russian). doi:10.17586/2226-1494-2023-23-4-767-775, EDN: ADSTLP
5. Zholondkovskiy V. V., Bocharov Y. I., Butuzov V. A. Neural network device for recognizing speech commands based on hardware accelerators of the NEUROMATRIX family. *IT Security (Russia)*, 2024, vol. 31, no. 2, pp. 134–141 (In Russian). doi:10.26583/bit.2024.2.09, EDN: MDJSMM
6. Warden P. Speech commands: A dataset for limited-vocabulary speech recognition, 2018. arXiv:1804.03209. https://arxiv.org/abs/1804.03209 (accessed 13 October 2026). doi:10.48550/arXiv.1804.03209
7. David R., Duke J., Jain A., Janapa Reddi V., Jeffries N., Li J., Kreeger N., Nappier I., Natraj M., Regev S., Rhodes R., Wang T., Warden P. TensorFlow lite micro: Embedded machine learning on TinyML systems. *Proceedings of Machine Learning and Systems*, 2021, vol. 3, pp. 800–811.
8. Jacob B., Kligys S., Chen B., Zhu M., Tang M., Howard A., Adam H., Kalenichenko D. Quantization and training of neural networks for efficient integer-arithmetic-only inference. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018, pp. 2704–2713. doi:10.1109/cvpr.2018.00286
9. Kim B., Chang S., Lee J., Sung D. Broadcasted residual learning for efficient keyword spotting. *Interspeech 2021*, 2021, pp. 4538–4542. doi:10.21437/interspeech.2021-383
10. López-Espejo I., Tan Z.-H., Hansen J. H. L., Jensen J. Deep spoken keyword spotting: An overview. *IEEE Access*, 2022, vol. 10, pp. 4169–4199. doi:10.1109/access.2021.3139508
11. Nahshan Y., Chmiel B., Baskin C., Zheltonozhskii E., Banner R., Bronstein A. M., Mendelson A. Loss aware post-training quantization. *Machine Learning*, 2021, vol. 110, no. 11–12, pp. 3245–3262. doi:10.1007/s10994-021-06053-z
12. Gupta K., Ajanthan T. Improved gradient-based adversarial attacks for quantized networks. *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022, vol. 36, no. 6, pp. 6810–6818. doi:10.1609/aaai.v36i6.20637
13. Xiao Y., Liu A., Zhang T., Qin H., Guo J., Liu X. RobustMQ: benchmarking robustness of quantized models. *Visual Intelligence*, 2023, vol. 1, art. 30. doi:10.1007/s44267-023-00031-w
14. Ayaz F., Zakariyya I., Cano J., Keoh S. L., Singer J., Pau D., Kharbouche-Harrari M. Improving robustness against adversarial attacks with deeply quantized neural networks. *2023 International Joint Conference on Neural Networks (IJCNN)*, 2023, pp. 1–8. doi:10.1109/ijcnn54540.2023.10191429
15. Goodfellow I. J., Shlens J., Szegedy C. Explaining and harnessing adversarial examples. *International Conference on Learning Representations*, 2015. arXiv:1412.6572. https://arxiv.org/abs/1412.6572 (accessed 13 October 2026).
16. Madry A., Makelov A., Schmidt L., Tsipras D., Vladu A. Towards deep learning models resistant to adversarial attacks. *International Conference on Learning Representations*, 2018. arXiv:1706.06083. https://arxiv.org/abs/1706.06083 (accessed 13 October 2026).
17. Athalye A., Carlini N., Wagner D. Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. *Proceedings of the 35th International Conference on Machine Learning. Proceedings of Machine Learning Research*, 2018, vol. 80, pp. 274–283.
18. Croce F., Hein M. Reliable evaluation of adversarial robustness with an ensemble of diverse parameter-free attacks. *Proceedings of the 37th International Conference on Machine Learning. Proceedings of Machine Learning Research*, 2020, vol. 119, pp. 2206–2216.
19. Carlini N., Athalye A., Papernot N., Brendel W., Rauber J., Tsipras D., Goodfellow I. J., Madry A., Kurakin A. On evaluating adversarial robustness, 2019. arXiv:1902.06705. https://arxiv.org/abs/1902.06705 (accessed 13 October 2026). doi:10.48550/arXiv.1902.06705
20. Abdullah H., Warren K., Bindschaedler V., Papernot N., Traynor P. SoK: The faults in our ASRs: An overview of attacks against Automatic Speech Recognition and speaker identification systems. *IEEE Symposium on Security and Privacy*, 2021, pp. 730–747. doi:10.1109/sp40001.2021.00014
21. Bhanushali A. R., Mun H., Yun J. Adversarial attacks on Automatic Speech Recognition (ASR): A survey. *IEEE Access*, 2024, vol. 12, pp. 88279–88302. doi:10.1109/access.2024.3416965
22. López-Espejo I., Tan Z.-H., Jensen J. A novel loss function and training strategy for noise-robust keyword spotting. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 2021, vol. 29, pp. 2254–2266. doi:10.1109/taslp.2021.3092567
23. Wang Q., Zheng B., Li Q., Shen C., Ba Z. Towards query-efficient adversarial attacks against Automatic Speech Recognition systems. *IEEE Transactions on Information Forensics and Security*, 2021, vol. 16, pp. 896–908. doi:10.1109/tifs.2020.3026543
24. Tong C., Zheng X., Li J., Ma X., Gao L., Xiang Y. Query-efficient black-box adversarial attacks on Automatic Speech Recognition. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 2023, vol. 31, pp. 3981–3992. doi:10.1109/taslp.2023.3304476
25. Croce F., Andriushchenko M., Sehwag V., Debenedetti E., Flammarion N., Chiang M., Mittal P., Hein M. RobustBench: A standardized adversarial robustness benchmark. *Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks*, 2021, vol. 1.
26. Kulikov D. A., Platonov V. V. Adversarial attacks on intrusion detection systems using LSTM classifier. *Problems of Information Security. Computer Systems*, 2021, no. 2, pp. 48–56 (In Russian). EDN: CLLJVV
27. Parfenov D. I., Bolodurina I. P., Grishina L. S., Zhigalov A. Yu., Tolmachev S. V. Investigation of transfer learning efficiency in adversarial attacks. *Modern Information Technologies and IT-Education*, 2022, vol. 18, no. 4, pp. 861–871 (In Russian). doi:10.25559/sitito.18.202204.861-871, EDN: DDZPSG
28. Fomicheva S. G., Bezzateev S. V. Defenses for machine learning models from adversarial attacks. *T-Comm*, 2023, vol. 17, no. 10, pp. 28–42 (In Russian). doi:10.36724/2072-8735-2023-17-10-28-42
29. Getman A. I., Goryunov M. N., Matskevich A. G., Rybolovlev D. A., Nikolskaya A. G. Adversarial attacks against a machine learning based intrusion detection system. *Problems of Information Security. Computer Systems*, 2023, no. 4, pp. 156–190 (In Russian). doi:10.48612/jisp/eatr-5pxb-akt8, EDN: XTMDJV
30. Vershkov N. A., Babenko M. G., Kuchukova N. N., Kuchukov V. A., Kucherov N. N. Transverse-layer partitioning of artificial neural networks for image classification. *Computer Optics*, 2024, vol. 48, no. 2, pp. 312–320 (In Russian). doi:10.18287/2412-6179-co-1278
31. Baev A. V., Samonov A. V., Safonov V. M., Krasnov S. V., Malyshev S. R. Methods for protecting neural network models from evasion and poisoning attacks. *Automation of Control Processes*, 2024, no. 4(78), pp. 39–48 (In Russian). doi:10.35752/1991-2927_2024_4_78_39
32. Kotenko I. V., Saenko I. B., Lauta O. S., Vasiliev N. A., Sadovnikov V. E. A method of countering adversarial attacks on image classification systems. *Voprosy kiberbezopasnosti*, 2025, no. 2(66), pp. 114–123 (In Russian). doi:10.21681/2311-3456-2025-2-114-123, EDN: MKWZFT

УДК 621.396
doi:10.31799/1684-8853-2026-5-21-36
EDN: IBKLIO

Научные статьи
Articles

Валидация автоматных спецификаций на основе перемножения автоматов

В. А. Назаров[a], *бакалавр, orcid.org/0009-0000-0352-7885*
А. А. Шалыто[a], *доктор техн. наук, профессор, orcid.org/0000-0002-2723-2077, anatoly.shalyto@gmail.com*
[a]*Университет ИТМО, Кронверкский пр., 49, Санкт-Петербург, 197101, РФ*

Введение: *при разработке ответственных систем все чаще применяются автоматные спецификации. При этом особую важность и актуальность представляет их валидация. Тестирование и верификация не решают эту проблему, особенно при использовании вложенных конечных автоматов.* ***Цель:*** *разработать метод построения автомата-произведения для рассматриваемого класса спецификаций на основе перемножения графов переходов, в том числе для вложенных автоматов, для упрощения эвристической процедуры его последующей валидации.* ***Методы:*** *в работе применяется построение достижимой части пространства состояний, обход графа в ширину и имитационная проверка выходных последовательностей событий.* ***Результаты:*** *предлагаемый метод формирует автомат-произведение с множеством достижимых пар состояний и отображением переходов, что позволяет при визуальном анализе обнаружить и вручную исключить тупиковые (дедлоки) и другие некорректные состояния и переходы. Последовательное перемножение нескольких автоматов обеспечивает пошаговую проверку корректности всей системы. В рассмотренном примере расхождений выходных последовательностей событий между откорректированной системой и автоматом-произведением на использованных входных последовательностях событий не обнаружено.* ***Практическая значимость:*** *представленный метод позволяет расширить арсенал средств для обеспечения валидации автоматных спецификаций, содержащих, в том числе, вложенные автоматы, однако не гарантирует упрощения автомата-произведения по сравнению с исходной системой.* ***Обсуждение:*** *метод особенно полезен при анализе автоматически построенных или модифицированных систем автоматов, поскольку помогает обнаруживать скрытые логические противоречия, которые трудно выявить тестированием, верификацией или имитационным моделированием.*

Ключевые слова *— автоматы, вложенные автоматы, перемножение автоматов, валидация.*

Для цитирования: Назаров В. А., Шалыто А. А. Валидация автоматных спецификаций на основе перемножения автоматов. *Информационно-управляющие системы*, 2026, № 5, с. 21–36. doi:10.31799/1684-8853-2026-5-21-36, EDN: IBKLIO
For citation: Nazarov V. A., Shalyto A. A. Validation of automata specifications based on automata composition. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 21–36 (In Russian). doi:10.31799/1684-8853-2026-5-21-36, EDN: IBKLIO

Введение

Программное обеспечение (ПО) для управления ответственными объектами обычно представляет собой системы со сложным поведением, зависящим от предыстории [1]. Цена ошибки в таких системах может быть очень высока, поэтому к ним применяют строгие методы формальной верификации [2, 3]. Одним из подходов к созданию ПО для таких объектов является автоматное программирование.

В рамках парадигмы автоматного программирования [1] ключевыми компонентами программы считаются конечные автоматы, совокупность которых представляет собой спецификацию и ее поведение. Среди достоинств конечных автоматов можно отметить наглядность их представления в виде графов переходов, удобство и естественность их верификации [4], которая может дополнять тестирование, применяемое обычно при отладке программ. По мнению Л. Лэмпорта, код не предназначен для размышлений о поведении системы, графы переходов для этой цели подходят значительно лучше. При использовании инструментальных средств, таких как Stateflow [5], графы переходов являются также и сверхвысоким языком программирования. Современные работы продолжают развивать формальную верификацию таких моделей, в том числе Stateflow [6] и автоматных спецификаций на основе теории автоматов [7]. Поэтому автоматные спецификации все шире используются на практике, однако и они требуют валидации.

Как в свое время заметил Э. Дейкстра, отсутствие ошибок при тестировании не гарантирует их отсутствия. Верификация также не дает полной гарантии: известны случаи, когда автоматная спецификация успешно проходила значительное число тестов и проверку многих темпоральных свойств, однако ошибка обнаруживалась лишь при добавлении дополнительного свойства. Таким образом, ни число тестов, ни число проверяемых свойств заранее не известны, а тестирование и верификацию следует рассматривать как составляющие валидации [8] наряду с имитационным моделированием и эвристическими проверками. Валидации автоматных и statechart-спецификаций посвящены и современные работы, например [9].

Особое значение валидация приобретает при использовании для управления ответственными объектами систем взаимосвязанных автоматов, в том числе вложенных, каждый из которых задается графом переходов. Корректность таких систем исследуют методами проверки на моделях и автоматного анализа [10, 11], в том числе для систем взаимодействующих конечных автоматов [12, 13]. В настоящей работе предлагается новый подход к валидации таких графов переходов, состоящий в их замене одним эквивалентным графом. Метод позволяет обнаруживать дефекты в исходной системе, в том числе тупиковые достижимые состояния. Подход, который при наличии более двух автоматов применяется многократно, состоит из двух стадий: построения эквивалентного графа для двух автоматов и последующего эвристического анализа полученного результата.

Известно, что задача построения одного автомата по системе автоматов может быть решена их перемножением. В работе «Автоматное программирование: определение, модель, реализация» (https://habr.com/ru/articles/682422/) рассматривается перемножение схем структурных автоматов, а не графов переходов автоматов, что предлагается в данной работе. Перемножение графов переходов автоматов рассмотрено в классической литературе по теории автоматов, где эта задача сформулирована как построение «системы в целом как автомата» (https://www.klex.ru/1q56). Однако излагаемый там метод не позволяет перемножать вложенные графы переходов, что чрезвычайно важно при их применении на практике. В настоящей работе эта проблема решается за счет разработки метода перемножения таких графов переходов. Отметим, что близкие задачи активно исследуются как в отечественных, так и в зарубежных работах. Конформному тестированию конечных автоматов и синтезу проверяющих тестов с гарантированной полнотой посвящен ряд работ [14–17]. Методы построения, активного обучения и тестирования автоматных моделей, в том числе недетерминированных и взаимодействующих автоматов, развиваются в [18–23]. Современные подходы к верификации, проверке на моделях и поведенческой эквивалентности автоматных спецификаций изложены в [24–28].

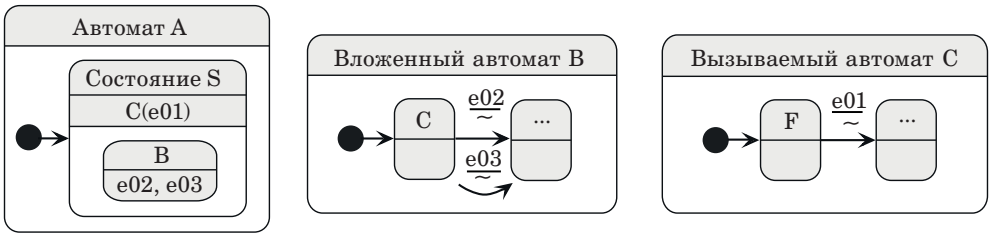
Обозначения и определения. Постановка задачи

В данной работе конечные автоматы рассматриваются как графы переходов. Автомат Ai задается кортежем $(Si, s_0i, Ei, \delta i, Ni)$, где Si — конечное множество состояний, $s_0i \in Si$ — начальное состояние, Ei — множество входных воздействий, δi: $Si \times Ei \rightharpoonup Si$ — частичная функция переходов, Ni: $Si \to 2^{Id}$ — функция вложенности, сопоставляющая каждому состоянию множество идентификаторов вложенных автоматов. Переход содержит событие, условие v, выходные воздействия. Вершины также могут иметь выходные воздействия, генерируемые при входе в них. На графах переходов дуга записывается в виде e [& v] / z, где слева от «/» указываются событие и условие, справа — выходные воздействия (символ «~» означает их отсутствие, что используется на рисунках данной работы). Если из одного состояния по одному событию существует несколько переходов, срабатывает тот, условие v которого истинно. Если подходящего перехода нет, состояние автомата не изменяется.

Глобальное состояние системы автоматов — это кортеж текущих состояний всех автоматов. В отличие от классического перемножения графов, где одно входное событие адресуется всем автоматам одновременно, в рассматриваемой системе внешнее входное воздействие адресуется конкретному автомату системы. Этот автомат может изменить свое состояние и породить внешние выходные воздействия или межавтоматные вызовы. В нотации переходов используются следующие обозначения: e — входное событие; v — условие перехода (булева формула над x и yi), где x — входная переменная, yi — номер текущей вершины автомата i; z — внешнее выходное воздействие; $Ai(e)$ — вызов автомата i с событием e как выходное воздействие. Запись $yi = j$ означает проверку того, что автомат i находится в вершине с номером j; запись $yi! = j$ означает обратное. Знак «=» для компактности заменяет знак «==» языка С. Знак «!» в булевых формулах заменяет отрицание.

Под межавтоматным взаимодействием понимаются два механизма: вызов другого автомата $Ai(e)$ и условие на переходе, зависящее от состояния другого автомата, например $yi = j$. Вызов выполняется синхронно: вызываемый автомат обрабатывает переданное событие в рамках того же вызова. В рассматриваемой реализации предполагается, что один переход или вход в состояние порождает не более одного межавтоматного вызова, адресованного одному из двух перемножаемых автоматов.

Вложенный автомат B — это автомат, указанный в одном или нескольких состояниях автомата A. Если A получает входное воздействие, находясь в таком состоянии, воздействие сначала передается вложенному автомату B, а затем обрабатывается самим автоматом A. В данной работе рассматриваются случаи с не более чем одним автоматом, вложенным в состояние другого автомата. Дополнительным ограничением является запрет обратного вызова: автомат не может в рамках одного шага вызвать автомат, который уже вызвал его. Это ограничение предотвращает циклическое распространение межавтоматных воздействий.



■ ***Рис. 1.*** Пример системы с вложенным и вызываемым автоматом
■ ***Fig. 1.*** An example of a system with a nested and a called automaton

Вложенный в вершину автомат обозначается дробью: в числителе — его имя, в знаменателе — события, на которые он реагирует. Рассмотрим используемую в дальнейшем нотацию на примере. На графе переходов (рис. 1) в состоянии S автомата A присутствуют два вида межавтоматного взаимодействия. Первое — межавтоматное воздействие $C(e01)$: при входе A в состояние S вызывается автомат C с событием $e01$. Второе — вложенный автомат B, который реагирует только на два воздействия: $e02$, $e03$. Автомат может одновременно быть вложенным для одного автомата и вызываемым другим автоматом.

Задача состоит в построении автомата-произведения, состояния которого соответствуют достижимым глобальным состояниям перемножаемых автоматов. Такой автомат используется для последующего анализа спецификации: поиска запрещенных комбинаций состояний, некорректных переходов и тупиковых состояний, — а также последующей модификации исходной системы автоматов на основе данного преобразования.

Под поведенческой эквивалентностью будем понимать совпадение последовательностей внешних выходных воздействий исходной системы и автомата-произведения для любой в инженерном смысле этого слова конечной последовательности внешних входных воздействий. В программной реализации это свойство проверяется имитационным моделированием на конечном наборе последовательностей событий.

Описание подхода, основанного на методе перемножения автоматов

Процесс последовательного перемножения и валидации системы конечных автоматов ($A1$, $A2$, $A3$, …) включает следующие шаги.

Шаг 1. Выбор пары автоматов. Из исходной системы выбираются два конечных автомата Ai и Aj, для которых требуется построить автомат-произведение.

Шаг 2. Инициализация обхода. Формируется очередь Q, содержащая пары вершин. Изначально она содержит пару стартовых вершин автоматов Ai и Aj. Дополнительно вводится множество посещенных вершин V и отображение переходов T, в котором для каждой пары вершин и входного воздействия фиксируется переход в соответствующую пару вершин.

Шаг 3. Итеративное построение множества вершин. Пока очередь Q не пуста, выполняются следующие действия, представленные в виде псевдокода:

```
while Q is not empty:
  (a, b) = Q.pop()
  for each input event e in events(a, b):
    for each (c, d, out) in imitate(a, b, e):
      T[(a, b)][e].add(c, d, out)
      if (c, d) not in V:
        V.add(c, d)
        Q.push(c, d)
```

Здесь a, b — текущие вершины автоматов; $\text{events}(a, b) = \{e \in Eenv \mid \delta i(a, e) \neq \varnothing\} \cup \{e \in Eenv \mid \delta j(b, e) \neq \varnothing\}$ — множество входных воздействий, на которые реагирует хотя бы один из автоматов в текущих вершинах; $\text{imitate}(a, b, e)$ — функция имитации, возвращающая множество результатов (c, d, out): по одному для каждого перехода, применимого при событии e. Если из одной вершины по одному событию существует несколько переходов с разными условиями x, каждый порождает отдельный результат и отдельную дугу в итоговом графе.

Шаг 4. Формирование автомата-произведения. По завершении обхода множество посещенных пар вершин образует множество состояний автомата-произведения $Ai * Aj$, а сформированное отображение T определяет его функцию переходов.

Шаг 5. Валидация результата. Полученный автомат эвристически анализируется относительно явно заданных ограничений корректности: отсутствия запрещенных комбинаций состояний, некорректных переходов и тупиковых достижимых состояний. В случае обнаружения несоответствий исходные автоматы Ai, Aj модифицируются, после чего процедура перемножения повторяется.

Шаг 6. Последовательное перемножение системы автоматов. Если система содержит более двух автоматов, построенный автомат-произведение *Ai* * *Aj* считается новым автоматом *Ai*, а следующий автомат системы принимается за новый *Aj*. После этого метод вновь начинает работу с шага 1.

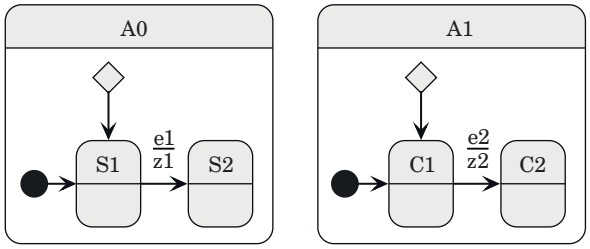
Далее подробно рассматриваются шаги 2, 3 и 4 предложенного метода, тогда как этапы валидации будут продемонстрированы на примере в следующем разделе.

Шаг 2. Инициализация обхода. До начала обхода оба автомата *A*0, *A*1 (рис. 2) находятся в начальных состояниях *S*1, *C*1 соответственно.

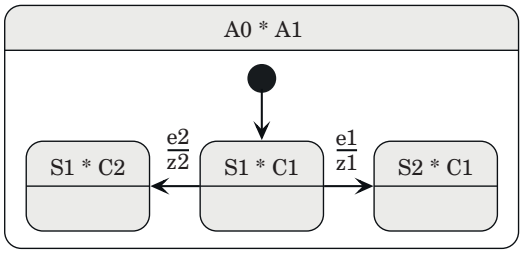
Далее на представленных графах в данной работе черной точкой отмечены стартовые вершины, а ромбом — вершины, в которых автоматы находятся в текущий момент.

Шаг 3. Итеративное построение множества вершин. Метод основан на вызове конкретного конечного автомата системы с заданным входным событием (воздействием). При его обработке автомат выполняет не более одного перехода и может вызвать другой автомат, передав ему межавтоматное воздействие. Такой процесс распространения воздействий и изменения состояний автоматов назовем имитацией (imitate(*a*, *b*, *e*)) *входного события* (рис. 3, *а* и *б*). Результат каждой имитации отражается в итоговом графе переходов: определяется соответствующая комбинация вершин, которая либо уже присутствует в графе, либо добавляется в него, а после этого проводится дуга от предыдущей пары вершин с пометкой *входного* и возникших *выходных воздействий* (рис. 4).

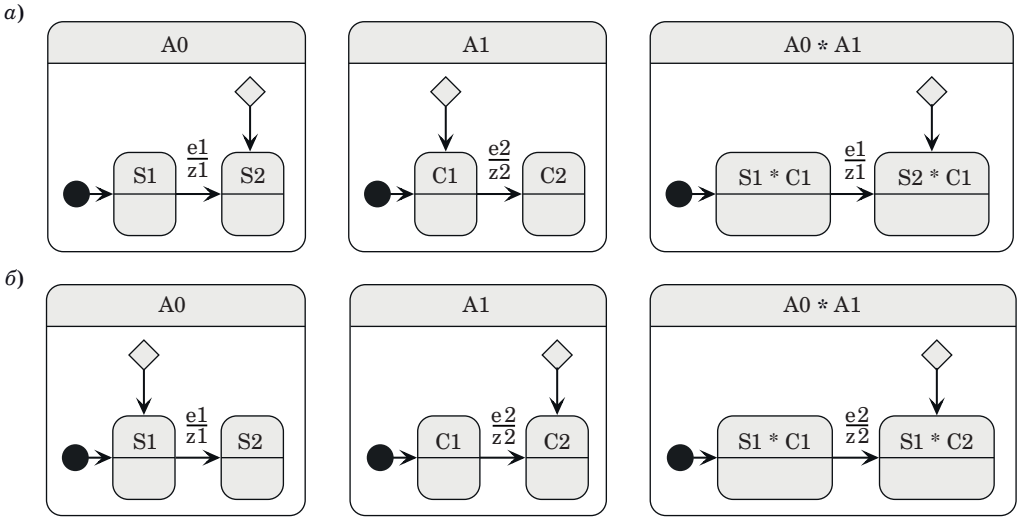
В процессе имитации выходное воздействие считается межавтоматным только в том случае, если оно адресовано второму автомату из данной пары. В случае, когда в процессе имитации автомат вызывает второй из текущей пары (рис. 5), переход затрагивает состояния обоих автоматов одновременно, и результирующая пара рассматривается как единая комбинация, в отличие от случая без межавтоматного взаимодействия (рис. 6, *а* и *б*, рис. 7). Воздействия, адресованные автоматам вне текущей пары, на данном шаге не учитываются. Они будут обработаны при последующем перемножении автомата-произведения с остальными автоматами системы.



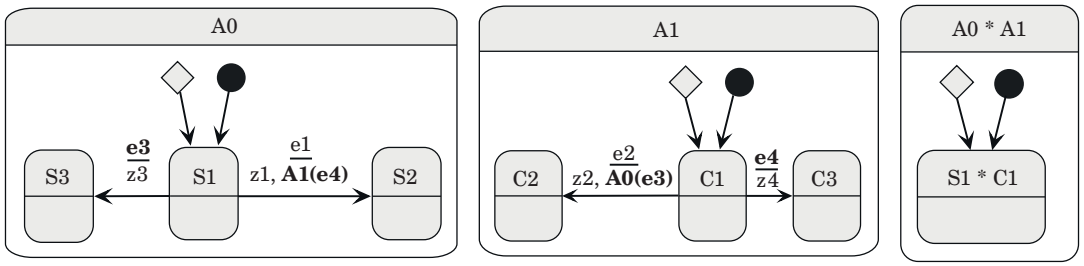
■ ***Рис. 2.*** Система графов в начальных состояниях
■ ***Fig. 2.*** The system of graphs in their initial states



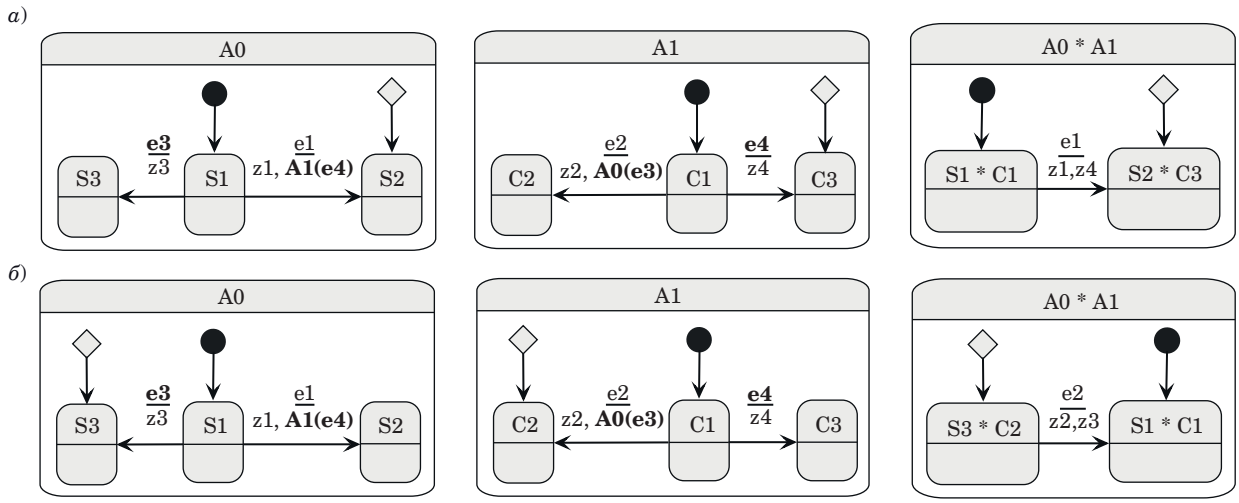
■ ***Рис. 4.*** Граф переходов после двух вызовов
■ ***Fig. 4.*** The transition graph after two calls



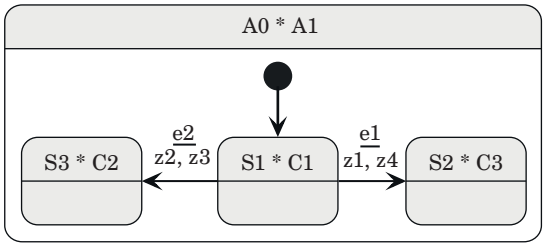
■ ***Рис. 3.*** Результат вызова автомата *A*0 с событием *e*1 (*а*) и *A*1 с событием *e*2 (*б*)
■ ***Fig. 3.*** The result of calling automaton *A*0 with event *e*1 (*а*) and *A*1 with event *e*2 (*б*)



■ ***Рис. 5.*** Система конечных автоматов, содержащая межавтоматные воздействия
■ ***Fig. 5.*** A system of finite automata containing inter-automata actions

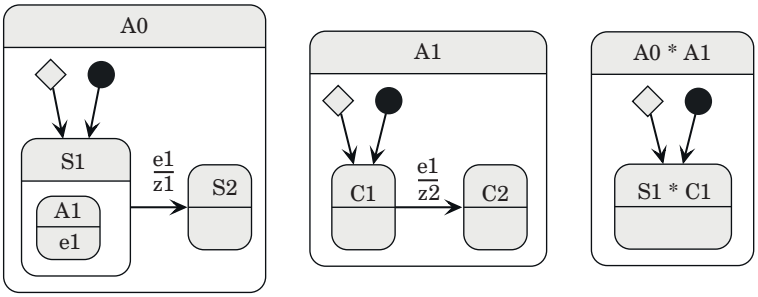


■ ***Рис. 6.*** Результат вызова с межавтоматным воздействием автомата $A0$ с событием $e1$ (*а*) и $A1$ с событием $e2$ (*б*)
■ ***Fig. 6.*** The result of calling with inter-automata actions between automaton $A0$ with event $e1$ (*а*) and $A1$ with event $e2$ (*б*)

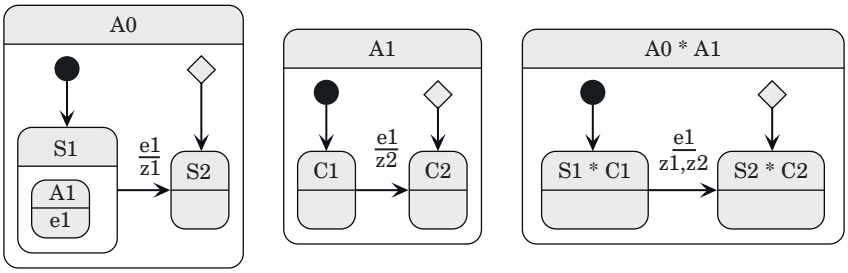


■ ***Рис. 7.*** Граф переходов автомата-произведения
■ ***Fig. 7.*** The transition graph of the product automaton

Входное воздействие всегда поступает из внешней среды — межавтоматные вызовы $Ai(e)$ выполняются при имитации и в итоговом графе как входные события не фигурируют. Вложенные автоматы также учитываются в процессе имитации (рис. 8, 9): воздействие сначала передается вложенному автомату $A1$, затем обрабатывается автоматом $A0$. Также, если перемножение в данном шаге выполняется с другим автоматом, вложенный автомат в имитации не участвует — ссылка на него в состояниях сохраняется и будет учтена при последующем перемножении с ним.



■ ***Рис. 8.*** Система конечных автоматов, содержащая вложенный автомат $A1$
■ ***Fig. 8.*** A system of finite automata containing a nested automaton $A1$

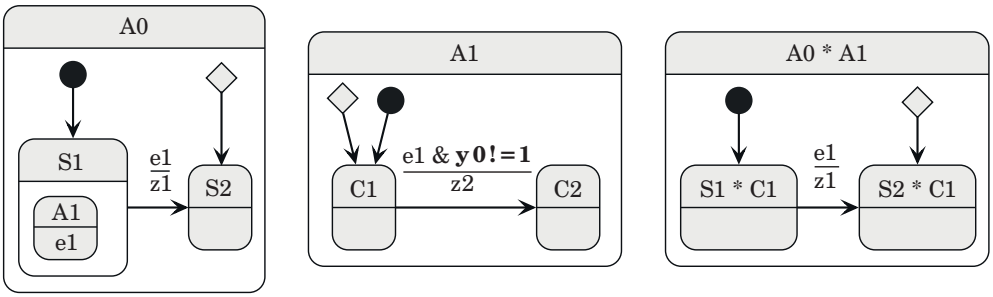


■ ***Рис. 9.*** Результат вызова автомата $A0$ (с вложенным автоматом $A1$) с событием $e1$
■ ***Fig. 9.*** The result of calling automaton $A0$ (with nested automaton $A1$) with event $e1$

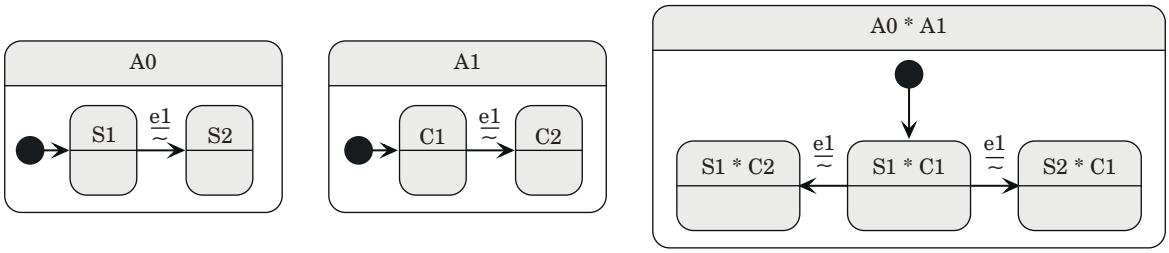
На первый взгляд, обработка вложенного автомата напоминает стандартное перемножение, где каждый автомат независимо реагирует на воздействие. Разница в порядке: управление передается сначала вложенному автомату, затем возвращается обратно «внешнему» автомату. Условия на переходах вида x вычисляются в момент выбора перехода и не зависят от состояния другого автомата. Условие $yi = j$, напротив, обращается к текущему состоянию автомата, j — это межавтоматное взаимодействие, которое влияет на выбор перехода (рис. 10).

Отметим, что если оба автомата независимо реагируют на одно и то же внешнее воздействие, в автомате-произведении из одного состояния возникают два перехода с одинаковым входным воздействием (рис. 11). Автомат-произведение становится недетерминированным: из одного состояния по одному входному воздействию невозможно однозначно выбрать переход. Условия детерминизма для систем автоматов исследованы в [12].

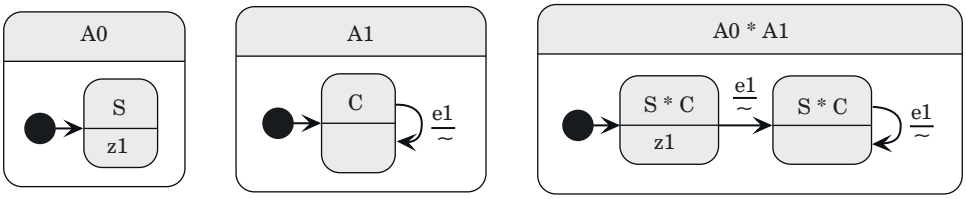
Шаг 4. Формирование автомата-произведения. Метод оперирует состояниями и условиями переходов исходных автоматов. Он позволяет итеративно рассматривать все возможные входные воздействия для пар вершин, с помощью процесса имитации определять достижимые вершины и добавлять их в множество вершин итогового графа. Для каждой вновь полученной пары вершин процесс имитации повторяется. Таким образом, результирующий автомат формируется как граф достижимых состояний системы автоматов, а не как декартово произведение автоматов.



■ ***Рис. 10.*** Результат вызова автомата $A0$ (с условием $y0!=1$) с событием $e1$
■ ***Fig. 10.*** The result of calling automaton $A0$ (with condition $y0!=1$) with event $e1$



■ ***Рис. 11.*** Система конечных автоматов, не допускающая корректного перемножения
■ ***Fig. 11.*** A system of finite automata that does not admit a correct composition



■ ***Рис. 12.*** Пример перемножения автоматов с выходными воздействиями в вершинах
■ ***Fig. 12.*** An example of automata composition with output actions in the vertices

В результирующем графе возможно появление вершин, соответствующих одной и той же паре базовых состояний, но различающихся выходными воздействиями, связанными с входом в вершину (рис. 12). В этом случае происходит дублирование вершин в итоговом графе. Поэтому размер автомата-произведения определяется не только числом пар базовых состояний, но и числом различимых наборов таких выходных воздействий. В общем случае метод не гарантирует уменьшения числа состояний.

Межавтоматные взаимодействия связывают переходы двух автоматов в один и тем самым могут сокращать число состояний и переходов в автомате-произведении.

Пример. Рассмотрим систему конечных автоматов из работы «Имитатор игрового автомата класса “Однорукий бандит”» [29].

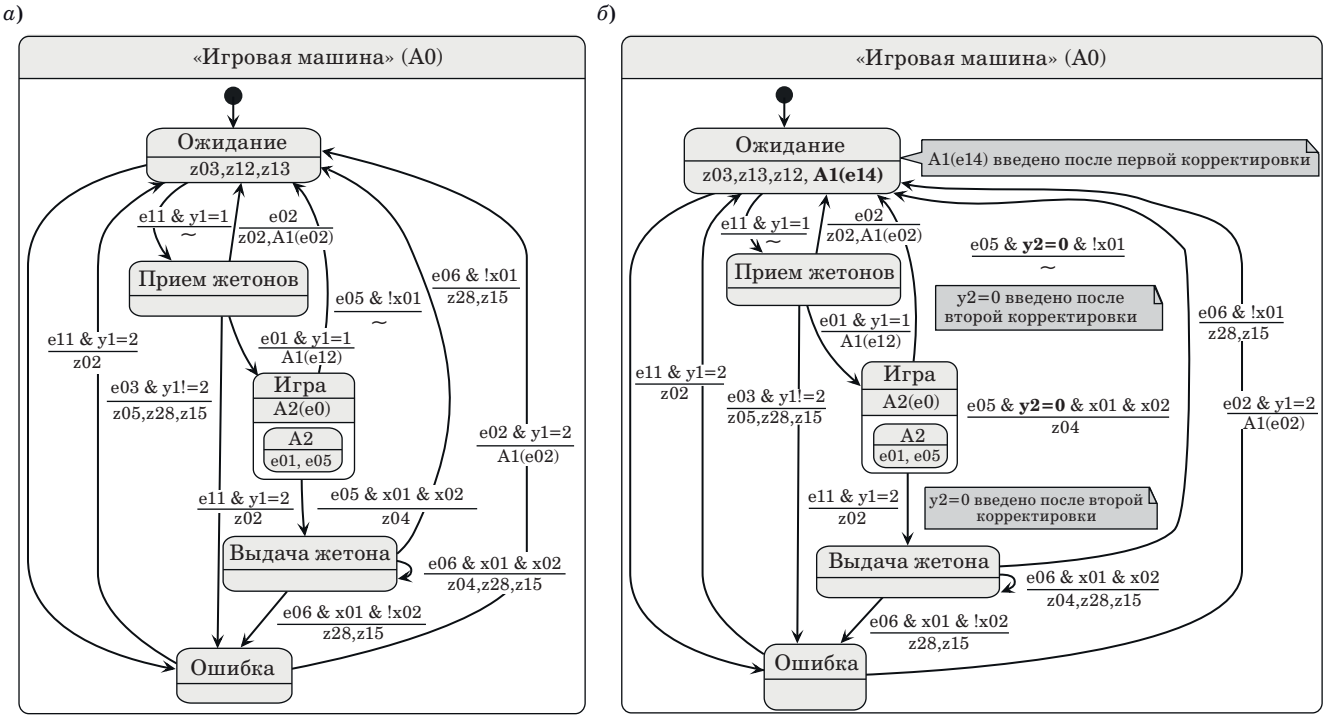
Система состоит из трех автоматов с суммарным числом состояний 12. Автомат 0 «Игровая машина» (*A*0) — пять состояний: «Ожидание», «Прием жетонов», «Игра», «Ошибка», «Выдача жетона». Схема связей, определяющая интерфейс автомата *A*0, и его граф переходов приведены на рис. 13 и 14, *а*. Графы переходов из [29] были уточнены и приведены к единообразной нотации.

Особенность графа переходов автомата *A*0 на рис. 14 состоит в том, что в вершине «Игра» автомат *A*2 упоминается два раза. Вверху вершины он изображен как автомат, вызываемый с событием *e*0; это означает, что *A*0 вызовет *A*2 при входе в состояние «Игра». Снизу автомат *A*2 изображен как вложенный согласно введенной нотации, в числителе которой приведено его обозначение, в знаменателе — события *e*01 и *e*05, на которые он реагирует. На рис. 14, *б* представлен итоговый граф переходов автомата *A*0, включающий корректировки, обоснование которых приводится в последующих разделах.

Автомат 1 «Монетоприемник» (*A*1) — три состояния: «Монетоприемник пуст», «Жетон принят», «Жетон не распознан». Схема связей, определяющая интерфейс автомата *A*1, и его граф переходов приведены на рис. 15 и 16, *а*. Автомат *A*1, находясь в состояниях «Жетон принят» и «Жетон не распознан», вызывает автомат *A*0 с событием *e*11. Исходное выходное воздействие *z*13 «Поместить жетоны в банк» в автомате *A*1 из [29] заменено на *z*16, так как оно конфликтовало с *z*13 «Сбросить ставку» в автомате *A*0. Итоговый граф переходов автомата *A*1, включающий корректировки, которые рассматриваются далее, представлен на рис. 16, *б*.

		A0			
Среда	Нажата кнопка «Игра»	e01	z02	Закрыть монетоприемник	Среда
	Нажата кнопка «Возврат»	e02	z03	Открыть монетоприемник	
	Нажата кнопка «Тех. сброс»	e03	z04	Выдать жетон из банка	
	Сработал таймер третьего барабана	e05	z05	Сбросить сумму выигрыша	
	Выдан жетон из банка	e06	z12	Обновить индикатор «Ставка»	
	Сумма выдачи выигрыша больше нуля	x01	z13	Сбросить ставку	
	В банке есть жетоны	x02	z15	Обновить индикатор «Банк»	
			z28	Обновить индикатор «Выигрыш»	
A1	Опущен жетон	e11			
	Жетон принят	y1=1	e02	Нажата кнопка «Возврат»	A1
	Жетон не распознан	y1=2	e12	Необходимо перевести жетоны в банк	
			e14	**Открыть монетоприемник**	
A2	**Барабаны прокручены**	**y2=0**			
			e0	Начало игры	A2
			e01	Нажата кнопка «Игра»	
			e05	Сработал таймер третьего барабана	

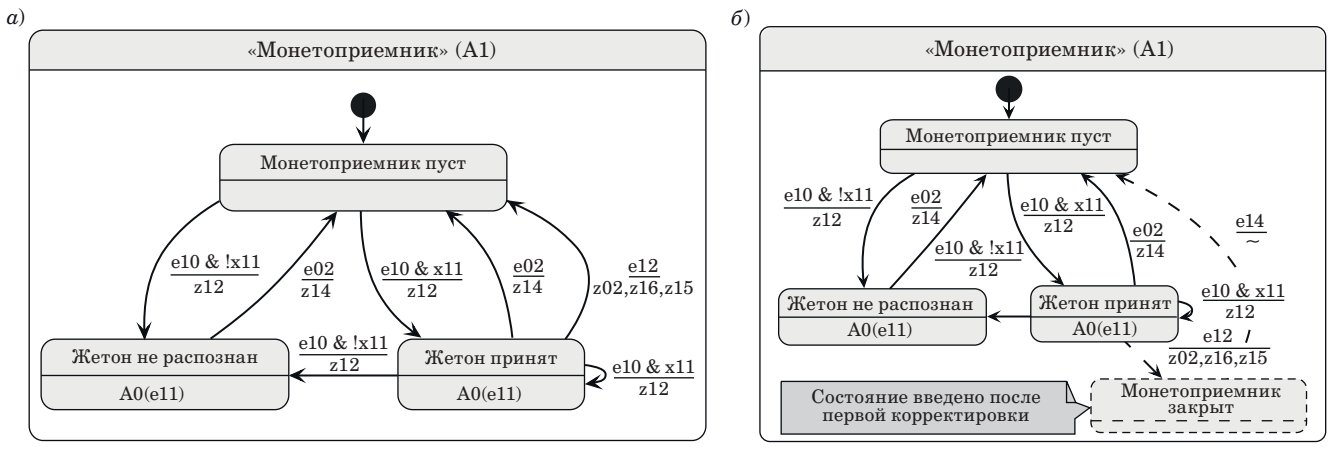
■ ***Рис. 13.*** Интерфейс автомата «Игровая машина» (*A*0)
■ ***Fig. 13.*** The interface of the “Gaming machine” automaton (*A*0)



■ ***Рис. 14.*** Граф переходов автомата «Игровая машина» (*A*0) до (*а*) и после двух корректировок (*б*)
■ ***Fig. 14.*** The transition graph of the “Gaming machine” automaton (*A*0) before (*a*) and after two corrections (*б*)

		A1			
Среда	Опущен жетон	e10	z02	Закрыть монетоприемник	Среда
	Жетон подлинный	x11	z12	Обновить индикатор «Ставка»	
			z14	Вернуть деньги	
A0	Нажата кнопка «Возврат»	e02	z15	Обновить индикатор «Банк»	
	Необходимо перевести жетоны в банк	e12	z16	Поместить жетоны в банк	
	Открыть монетоприемник	**e14**			
			e11	Опущен жетон	A0

■ ***Рис. 15.*** Интерфейс автомата «Монетоприемник» (*A*1)
■ ***Fig. 15.*** The interface of the “Coin acceptor” automaton (*A*1)



■ ***Рис. 16.*** Граф переходов автомата «Монетоприемник» (*A*1) до (*а*) и после одной корректировки (*б*)
■ ***Fig. 16.*** The transition graph of the “Coin acceptor” automaton (*A*1) before (*a*) and after one correction (*б*)

Автомат 2 «Игровые барабаны» (*A*2) — четыре состояния: «Барабаны остановлены», «Барабаны запущены», «Первый барабан остановлен», «Второй барабан остановлен». Схема связей, определяющая интерфейс автомата *A*2, и его граф переходов приведены на рис. 17, *а* и *б*.

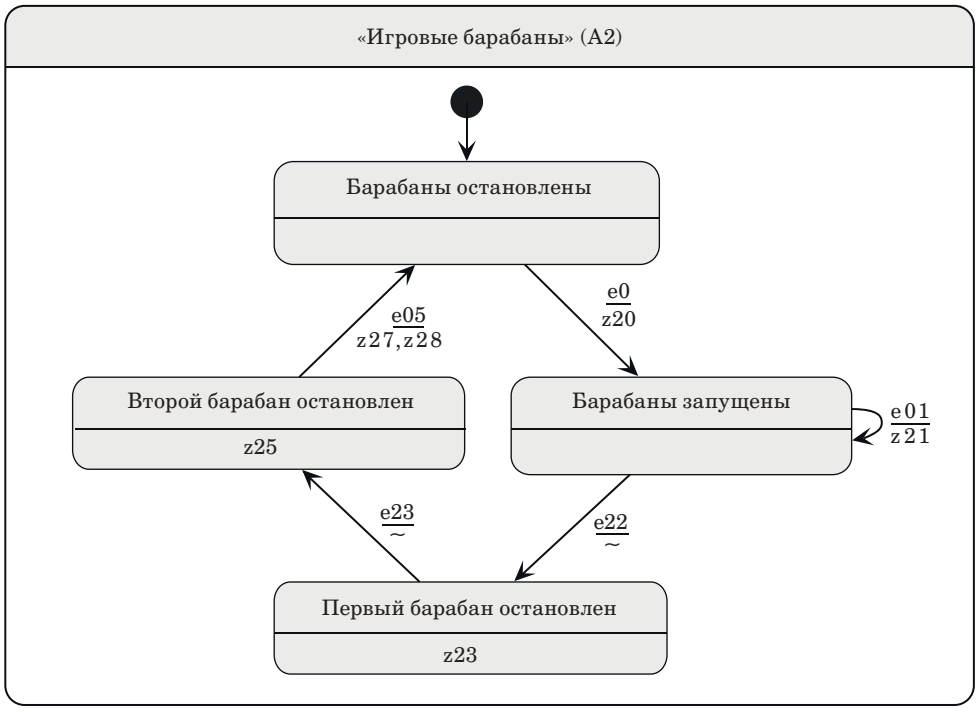
Краткое описание функционирования системы: автомат *A*0 разделяет работу на несколько фаз. Первая соответствует состояниям «Ожидание» и «Прием жетонов» автомата *A*0 и описывает процесс приема жетонов. В этой фазе задействованы автоматы *A*0 и *A*1, тогда как *A*2 не получает входных событий. Далее пользователь нажимает кнопку «Игра», и начинается следующая фаза, соответствующая состояниям «Игра» и «Выдача жетона» автомата *A*0, которая описывает процесс прокрутки барабанов, подсчета и выдачи выигрыша. В этой фазе задействованы автоматы *A*0 и *A*2, тогда как *A*1 не получает входных событий до завершения игры. Данное разделение на фазы определяет порядок перемножения: сначала *A*0 * *A*1, что соответствует первой фазе, а затем результат перемножается с *A*2 в соответствии со второй фазой.

Для анализа результата в спецификацию работы были добавлены два ограничения корректности. Они не сформулированы явно в исходной работе, однако логически вытекают из постановки задачи: их нарушение способно нарушить корректность работы системы в целом. Во-первых, прием жетонов разрешен только в состояниях «Ожидание» и «Прием жетонов» автомата *A*0; во время игры монетоприемник должен быть закрыт. Во-вторых, автомат *A*0 не должен выходить из состояния «Игра» по событию *e*05 до тех пор, пока автомат *A*2 не перешел в состояние «Барабаны остановлены».

а)

		A2			
Среда	Сработал таймер первого барабана	e22	z20	Запустить барабаны	Среда
	Сработал таймер второго барабана	e23	z21	Запустить таймер первого барабана	
			z23	Запустить таймер второго барабана	
A0	Начало игры	e0	z25	Запустить таймер третьего барабана	
	Нажата кнопка «Игра»	e01	z27	Установить сумму выигрыша	
	Сработал таймер третьего барабана	e05	z28	Обновить индикатор «Выигрыш»	

б)



■ ***Рис. 17.*** Интерфейс (*а*) и граф переходов (*б*) автомата «Игровые барабаны» (*A*2)

■ ***Fig. 17.*** The interface (*а*) and the transition graph (*б*) of the “Game reels” automaton (*A*2)

Предложенный метод был применен к рассматриваемой системе. Перемножение автоматов $A0$ и $A1$ привело к автомату, содержащему 13 состояний (рис. 18, *а*). Анализ полученного автомата показал, что он содержит состояния и переходы, нарушающие первое ограничение корректности (они выделены пунктиром). Состояние «Ожидание * Жетон не распознан» является тупиковым достижимым состоянием: оно достижимо в автомате-произведении, но из него не следует допустимое продолжение, соответствующее логике системы.

Из спецификации работы системы следует, что прием жетонов разрешен только в состояниях «Ожидание» и «Прием жетонов» автомата $A0$. В автомате-произведении есть состояния, нарушающие это ограничение. В состояниях «Игра», «Выдача жетона» и «Ошибка» автомата $A0$ обнаружена возможность вносить жетоны. Программа запрещает такое поведение пользователю за счет физической блокировки монетоприемника на программном уровне, хотя сама система конечных автоматов допускает неправильные состояния, которые приведены на рис. 18, *а*. При этом отметим, что в автоматной спецификации из работы «Однорукий бандит» [29], которая валидируется в данной работе, это не оговаривалось. Полагаться на внешнюю программу как на единственный механизм защиты от некорректного поведения небезопасно: спецификация автоматов должна явно исключать недопустимые состояния, а не перекладывать ответственность на внешние факторы.

Для устранения этой проблемы в автомат $A1$ было добавлено состояние «Монетоприемник закрыт» (см. рис. 16, *б*), а в $A0$ — событие $e14$ для явного открытия монетоприемника при возврате автомата $A0$ в состояние «Ожидание» (см. рис. 14, *б*). Тем самым запрет приема жетонов во время игры был перенесен из внешней среды в саму автоматную спецификацию, что исключает зависимость корректности от конкретной реализации физической блокировки монетоприемника.

Откорректированные конечные автоматы $A0$ и $A1$ были вновь перемножены. Внесенные изменения позволили сократить размер перемноженного автомата $A0 * A1$ с 13 до шести состояний (рис. 18, *б*).

Далее было произведено перемножение откорректированного автомата $A0 * A1$ (см. рис. 18, *б*) с автоматом $A2$ (см. рис. 17, *б*), что привело к автомату-произведению с 35 состояниями (рис. 19). В состояниях-группах, отмеченных на рисунке пунктиром, скрыты соответствующие состояния и переходы.

При анализе графа нет необходимости рассматривать его целиком, достаточно анализировать состояния в отдельности: «Выдача жетона * * Монетоприемник закрыт * Барабаны запущены», «Ожидание * Монетоприемник пуст * Барабаны запущены», «Прием жетонов * Жетон принят * * Барабаны запущены», «Ошибка * Монетоприемник закрыт * Барабаны запущены» и другие. Все эти состояния нарушают второе ограничение корректности: при запущенных барабанах невозможно начать прием новых жетонов, а автомат $A0$ не должен переходить в состояние «Ожидание» до завершения прокрутки всех барабанов.

На графе (см. рис. 19) также были найдены некорректные переходы: из состояний «Игра * * Монетоприемник закрыт * Барабаны запущены» и «Игра * Монетоприемник закрыт * Первый барабан остановлен» с событием $e05$ (сработал таймер третьего барабана). Они порождали все остальные некорректные состояния и переходы.

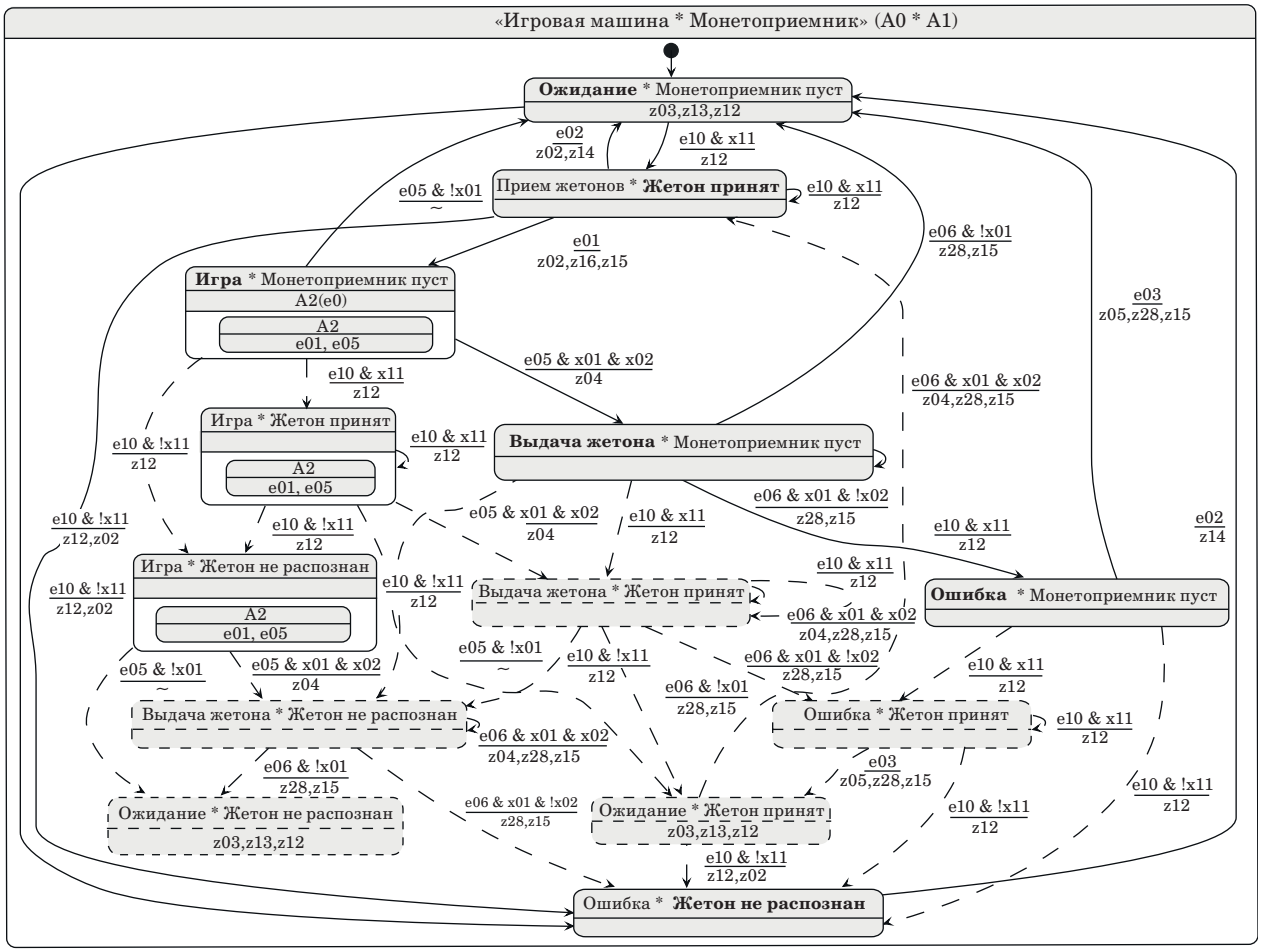
В процессе игры среда вызывает автомат $A2$ с событиями $e22$, $e23$ и автомат $A0$ с событием $e05$. Эти события описывают поочередную остановку барабанов по таймеру, при этом при наступлении события $e05$ автомат $A0$ выходит из состояния «Игра». Предполагается, что среда соблюдает строгий порядок этих событий. Однако в системе автоматов это не учитывается, и допускается переход в некорректное состояние в случае, если автомат $A0$ будет вызван с событием $e05$ без вызовов автомата $A2$ с событиями $e22$ и $e23$. Для того чтобы $A0$ не выходил из состояния «Игра» до остановки барабанов, к переходам из этого состояния по событию $e05$ добавлено условие $y2 = 0$ (см. рис. 14, *б*), которое явно проверяет остановку всех барабанов.

Отметим, что после внесения изменений в автомат $A0$ изменяется результат произведения $A0 * A1$. Поэтому схема, представленная на рис. 15, становится неактуальной и требует повторного перемножения откорректированного автомата $A0$ с автоматом $A1$. При этом изменения в автомате-произведении $A0 * A1$ являются незначительными и сводятся к добавлению условия $y2 = 0$ на переходы из состояния «Игра * Монетоприемник закрыт». При этом условия этих переходов станут следующими: $e05$ & $(y2 = 0)$ & $!x01$ и $e05$ & $(y2 = 0)$ & $x01$ & $x02$ / $z04$ (где $x01$, $x02$ — входные переменные автомата $A0$, см. рис. 14, *б*).

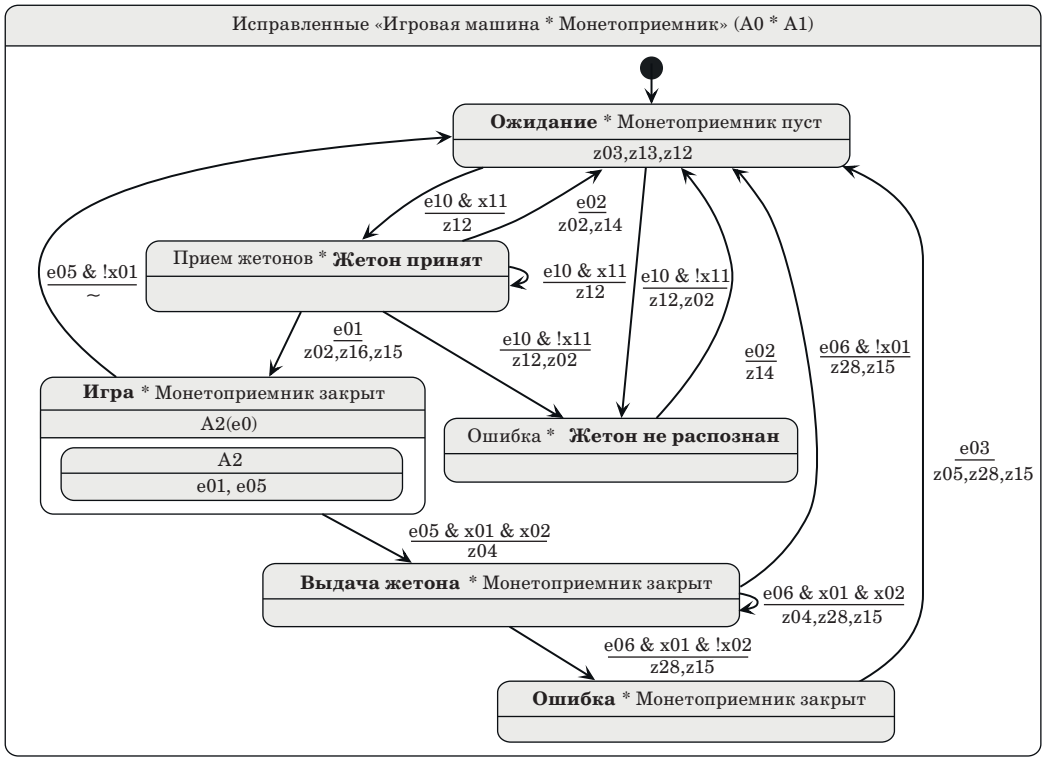
В результате интерфейс автомата-произведения $A0 * A1 * A2$ не содержит события $e0$ (рис. 20, *а*), а его граф переходов имеет всего лишь восемь состояний (рис. 20, *б*). Отсутствие события $e0$ связано с тем, что в исходной системе данное событие участвует только в межавтоматных взаимодействиях и не имеет связи с внешней средой.

После этих изменений в автомате-произведении не осталось выявленных ранее недопустимых состояний и переходов относительно двух сформулированных ограничений. При этом часть проверок во внешней программе стала избыточной, поскольку соответствующие ограничения были перенесены в автоматную спецификацию.

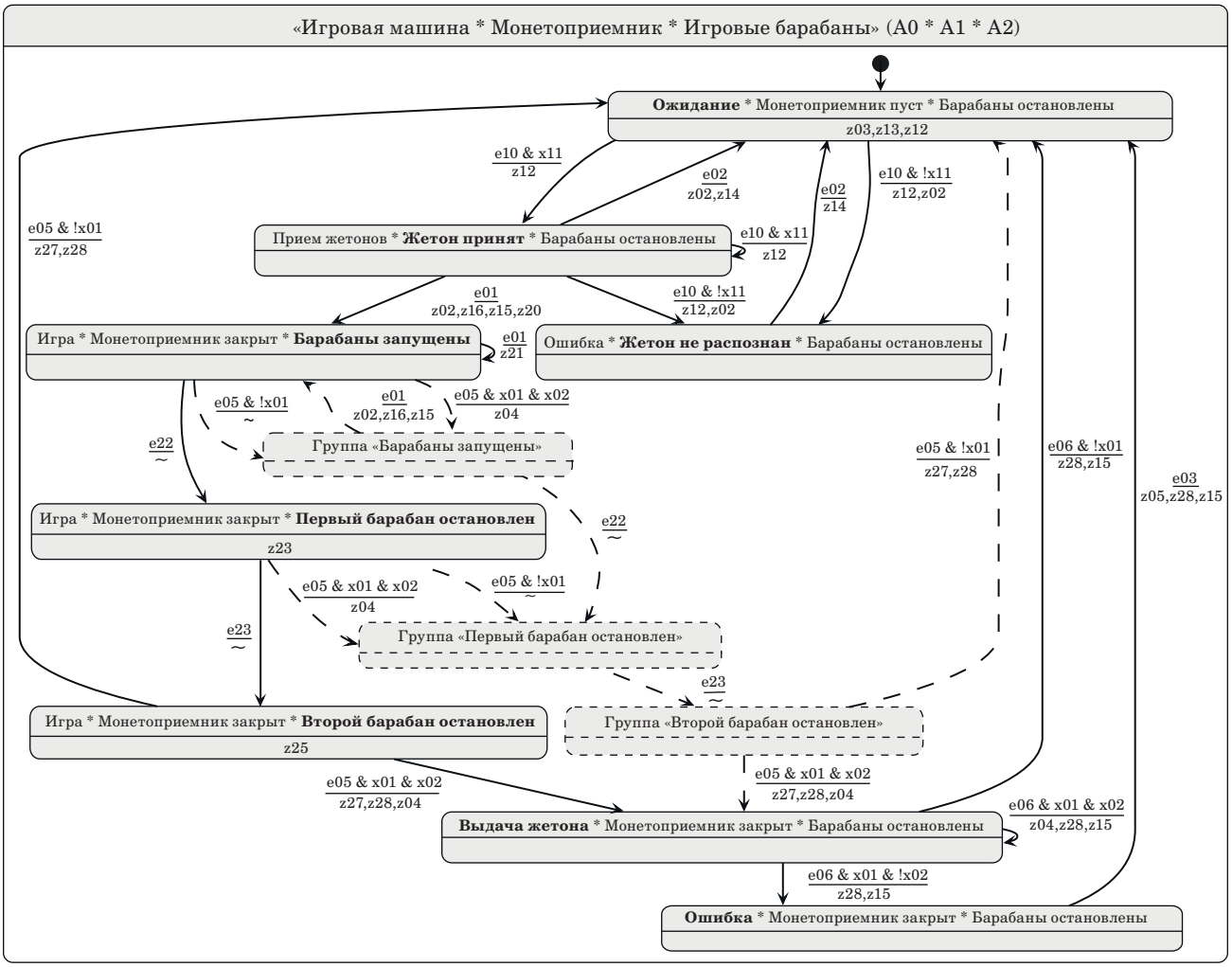
а)



б)



■ ***Рис. 18.*** Граф переходов перемноженного автомата *A*0 * *A*1 до (*а*) и после корректировок (*б*)
■ ***Fig. 18.*** The transition graph of the product automaton *A*0 * *A*1 before (*а*) and after corrections (*б*)



■ ***Рис. 19.*** Граф переходов автомата-произведения *A*0 * *A*1 * *A*2
■ ***Fig. 19.*** The transition graph of the product automaton *A*0 * *A*1 * *A*2

Заключение

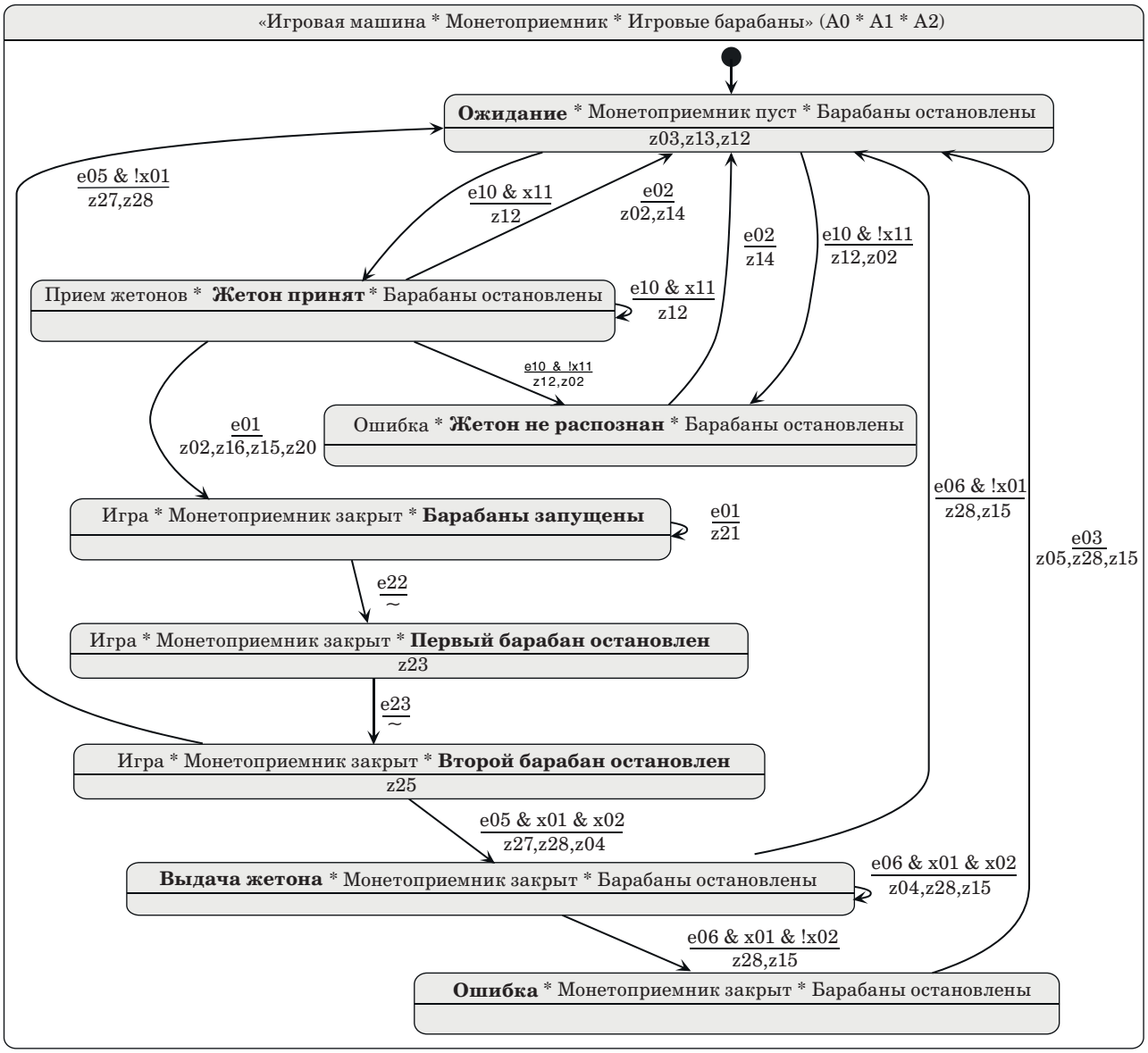
Полученные результаты показывают преимущества предложенного метода по сравнению с современными подходами к валидации автоматных спецификаций. В отличие от методов формальной верификации и проверки на моделях [6–10], требующих построения полной формальной модели и явной формулировки проверяемых свойств, предложенный подход выявляет дефекты (в том числе тупиковые достижимые состояния) на основе эвристического анализа автомата-произведения, построенного перемножением исходных графов переходов, включая вложенные. В отличие от методов активного обучения и тестирования автоматных моделей [17–28], требующих построения тестовых наборов или обучающих последовательностей и зависящих от их полноты, предложенный метод применяется непосредственно к уже заданной системе автоматов и не требует построения таких последовательностей.

Метод перемножения реализован программно (https://github.com/PhoenixNazarov/fsm-multiply). Там же реализован модуль имитационного моделирования (имитационной проверки): откорректированная система автоматов и автомат-произведение исполняются на одинаковых последовательностях внешних входных воздействий, после чего сравниваются последовательности внешних выходных воздействий (экспериментальный стенд с исходной, откорректированной и перемноженной реализациями автомата «Однорукий бандит» доступен по адресу https://github.com/PhoenixNazarov/fsm-slot-machine). Проверка включала полный перебор до глубины 20 и 1000 псевдослучайных последовательностей длиной 100. Расхождений обнаружено не было. Этот результат подтверждает согласованность программной реализации с построенным автоматом-произведением на указанных входных последовательностях событий.

а)

		A0 * A1 * A2			
Среда	Нажата кнопка «Игра»	e01	z02	Закрыть монетоприемник	Среда
	Нажата кнопка «Возврат»	e02	z03	Открыть монетоприемник	
	Нажата кнопка «Тех. сброс»	e03	z04	Выдать жетон из банка	
	Сработал таймер третьего барабана	e05	z05	Сбросить сумму выигрыша	
	Выдан жетон из банка	e06	z12	Обновить индикатор «Ставка»	
	Опущен жетон	e10	z13	Сбросить ставку	
	Сработал таймер первого барабана	e22	z14	Вернуть деньги	
	Сработал таймер второго барабана	e23	z15	Обновить индикатор «Банк»	
	Сумма выдачи выигрыша больше нуля	x01	z16	Поместить жетоны в банк	
	В банке есть жетоны	x02	z20	Запустить барабаны	
	Жетон подлинный	x11	z21	Запустить таймер первого барабана	
			z23	Запустить таймер второго барабана	
			z25	Запустить таймер третьего барабана	
			z27	Установить сумму выигрыша	
			z28	Обновить индикатор «Выигрыш»	

б)



■ ***Рис. 20.*** Интерфейс (*а*) и граф переходов (*б*) автомата-произведения откорректированных *A*0 * *A*1 * *A*2
■ ***Рис. 20.*** The interface (*а*) and the transition graph (*б*) of the product automaton of the corrected *A*0 * *A*1 * *A*2

Из изложенного следует, что предложенный подход является полуавтоматическим. После каждого автоматического перемножения пары автоматов специалист анализирует полученный автомат-произведение относительно заданных ограничений корректности. При обнаружении нарушений исходные автоматы корректируются. После этого перемножение автоматов повторяется. Процедура может выполняться многократно.

Приведенный пример показывает, что на первый взгляд корректно работающая система автоматов может содержать неточности, которые трудно обнаружить только имитационным моделированием. Так, в построенной системе из трех автоматов (формальной спецификации поведения программы) из [29] такие неточности на основе моделирования обнаружены не были. Поэтому предложенный метод следует рассматривать как дополнительный инструмент валидации автоматных спецификаций, особенно в случаях, когда система строится или модифицируется автоматически. В заключение отметим, что в работе [30] показано, как итеративные, а в других работах — рекурсивные алгоритмы могут быть преобразованы в графы переходов автоматов. Поэтому авторы предполагают обобщить предложенный метод валидации на указанные классы алгоритмов.

Выявленная в работе закономерность состоит в том, что небольшое изменение межавтоматного взаимодействия может существенно повлиять на размер автомата-произведения. В рассмотренном примере после устранения ошибок автомат $A0 * A1$ сократился с 13 до шести состояний, и потом $A0 * A1 * A2$ — с 35 до восьми состояний. Это позволяет высказать гипотезу: значительное увеличение размера автомата-произведения по отношению к сумме размеров исходных автоматов может служить эвристическим признаком наличия ошибок в спецификации, а после их устранения автомат-произведение нередко становится более компактным. Предлагаемый метод не гарантирует упрощения автомата-произведения, но является еще одним инженерным средством для обеспечения возможности повышения качества автоматных спецификаций.

Дальнейшее развитие метода связано с его расширением на случай нескольких автоматов, вложенных (в том числе и друг в друга) в состояние другого автомата.

Литература

1. **Поликарпова Н. И., Шалыто А. А.** *Автоматное программирование*. СПб., Питер, 2008, 167 с. http://is.ifmo.ru/books/_book.pdf (дата обращения: 22.03.2026).
2. **Adhikary S., Gurung A., Thakkar J., Bruto da Costa A. A., Dey S., Hazra A., Dasgupta P.** SMT-based verification of safety-critical embedded control software. *IEEE Embedded Systems Letters*, 2021, vol. 13, no. 3, pp. 138–141. doi:10.1109/LES.2020.3035560
3. **André É., Liu S., Liu Y., Choppy C., Sun J., Dong J. S.** Formalizing UML state machines for automated verification — A survey. *ACM Computing Surveys*, 2023, vol. 55, no. 13s, art. 277. doi:10.1145/3579821
4. **Вельдер С. Э., Лукин М. А., Шалыто А. А., Яминов Б. Р.** *Верификация автоматных программ*. СПб., Наука, 2011. 244 с.
5. **Янкин Ю. Ю., Шалыто А. А.** Автоматное программирование ПЛИС в задачах управления электроприводом. *Информационно-управляющие системы*, 2011, № 1, с. 50–56. EDN: NEKQXX
6. **Filipovikj P., Ung G., Gurov D., Nyberg M.** Bounded invariant checking for Stateflow. *Electronic Proceedings in Theoretical Computer Science (EPTCS)*, 2022, vol. 371, pp. 38–52. doi:10.4204/EPTCS.371.3
7. **Xiao M., Xu Y., Zhang Y., Yang K., Yan S., Cen L.** Formal verification of solidity smart contracts via automata theory. *Symmetry*, 2025, vol. 17, no. 8, art. 1275. doi:10.3390/sym17081275
8. **Шалыто А. А.** Валидация автоматных спецификаций. *Научно-технический вестник информационных технологий, механики и оптики*, 2023, т. 23, № 2, с. 436–438. https://ntv.ifmo.ru/file/article/21921.pdf (дата обращения: 20.05.2026). doi:10.17586/2226-1494-2023-23-2-436-438, EDN: YHATJW
9. **Wu R., Du Y., Li M.** A model transformation method based on Simulink/Stateflow for validation of UML statechart diagrams. *Mathematics*, 2025, vol. 13, no. 5, art. 724. doi:10.3390/math13050724
10. **Barth M., Jakobs M.-C.** Test-case generation with automata-based software model checking. *Model Checking Software (SPIN 2024)*, *LNCS*, vol. 14624, Springer, 2024, pp. 248–267. doi:10.1007/978-3-031-66149-5_14
11. **Sankur O.** Timed automata verification and synthesis via finite automata learning. *Journal of Automated Reasoning*, 2025, vol. 69, art. 15. doi:10.1007/s10817-025-09730-z
12. **Бурдонов И. Б., Косачев А. С.** Система автоматов: условия детерминизма и тестирование. *Труды Института системного программирования РАН*, 2016, т. 28, № 1, с. 151–184. doi:10.15514/ISPRAS-2016-28(1)-9, EDN: WAPNTP
13. **Бурдонов И. Б., Косачев А. С.** Тестирование системы автоматов с буферизацией сообщений. *Труды Института системного программирования РАН*, 2016, т. 28, № 1, с. 103–130. doi:10.15514/ISPRAS-2016-28(1)-7, EDN: WAPNQX
14. **Бурдонов И. Б., Косачев А. С.** Развитие теории конформности: семантики, формальные модели, алгоритмы. *Труды Института системного программирования РАН*, 2014, т. 26, № 1, с. 27–72. doi:10.15514/ISPRAS-2014-26(1)-2, EDN: RUMWWB

15. **Ермаков А. Д., Евтушенко Н. В.** К синтезу адаптивных проверяющих последовательностей для недетерминированных автоматов. *Труды Института системного программирования РАН*, 2016, т. 28, № 3, с. 123–144. doi:10.15514/ISPRAS-2016- 28(3)-8, EDN: WKFGUV
16. **Петрухнова Г. В., Усачев М. Г., Попова Е. В.** Тестовый контроль конечных автоматов. *Вестник Воронежского государственного технического университета*, 2023, т. 19, № 6, с. 47–52. doi:10.36622/VSTU.2023.19.6.007, EDN: ENHULJ
17. **Turker U. C., Hierons R. M., El-Fakih K., Mousavi M. R., Tyukin I. Y.** Accelerating finite state machine-based testing using reinforcement learning. *IEEE Transactions on Software Engineering*, 2024, vol. 50, no. 3, pp. 574–597. doi:10.1109/TSE.2024.3358416
18. **Kruger L., Junges S., Rot J.** Small test suites for active automata learning. *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2024), LNCS,* vol. 14571, Springer, 2024, pp. 109–129. doi:10.1007/978-3-031-57249-4_6
19. **Borsotti A., Breveglieri L., Crespi Reghizzi S., Morzenti A.** Multientry DFA with reduced initial states to speed-up parallel recognition. *Implementation and Application of Automata (CIAA 2025), LNCS,* vol. 15981. Springer, 2025, pp. 55–72. doi:10.1007/978-3-032-02602-6_5
20. **Vaandrager F., Melse I.** New fault domains for conformance testing of finite state machines. *36th International Conference on Concurrency Theory (CONCUR 2025), LIPIcs*, vol. 348, Schloss Dagstuhl — Leibniz-Zentrum für Informatik, 2025, art. 34, pp. 34:1–34:22. doi:10.4230/LIPIcs.CONCUR.2025.34
21. **Ferreira D., Lima L.** Verifying integrated designs of UML state machines and activities using CSP. *Formal Methods: Foundations and Applications (SBMF 2024), LNCS,* Springer, 2024, pp. 68–85. doi:10.1007/978-3-031-78116-2_5
22. **Rahaman H., Chattopadhyay S., Sengupta I.** Conformance testing for finite state machines guided by deep neural network. *Journal of Circuits, Systems and Computers*, 2022, vol. 31, iss. 09, art. 2250156, pp. 1–19. doi:10.1142/S0218126622501560
23. **Muškardin E., Tappler M., Aichernig B. K., Pill I.** Active model learning of stochastic reactive systems. *Software and Systems Modeling*, 2024, vol. 23, no. 2, pp. 503–524. doi:10.1007/s10270-024-01158-0
24. **Fortz S., Ghassemi F., Henry L., Howar F., Neele T., Rot J., Suilen M.** A research agenda for active automata learning. *International Journal on Software Tools for Technology Transfer*, 2026. doi:10.1007/s10009-026-00839-z
25. **Marksteiner S., Schögler D., Sirjani M., Sjödin M.** Learning single and compound-protocol automata and checking behavioral equivalences. *International Journal on Software Tools for Technology Transfer*, 2025, vol. 27, pp. 35–52. doi:10.1007/s10009-025-00797-y
26. **Henry L., Mousavi M. R., Neele T., Sammartino M.** Compositional active learning of synchronizing systems through automated alphabet refinement. *CONCUR 2025, LIPIcs*, vol. 348, Schloss Dagstuhl, 2025, pp. 20:1–20:22. doi:10.4230/LIPIcs.CONCUR.2025.20
27. **Manini A., Rossi M., San Pietro P.** Random testing of model checkers for timed automata with automated oracle generation. *TASE 2025, LNCS,* vol. 15841, Springer, 2025, pp. 343–360. doi:10.1007/978-3-031-98208-8_20
28. **Grobelna I.** Formal verification of control modules in cyber-physical systems. *Sensors*, 2020, vol. 20, no. 18, art. 5154. doi:10.3390/s20185154
29. **Хокканен А. В., Шалыто А. А.** Имитатор игрового автомата класса «Однорукий бандит». СПб., ИТМО, 2003. 44 с. https://is.ifmo.ru/download/SlotMachine_Report.pdf (дата обращения: 20.05.2026).
30. **Шалыто А. А., Туккель Н. И.** Преобразование итеративных алгоритмов в автоматные. *Программирование*, 2002, № 5, с. 12–26. http://is.ifmo.ru/works/iter/ (дата обращения: 20.05.2026).

UDC 621.396
doi:10.31799/1684-8853-2026-5-21-36
EDN: IBKLIO

Validation of automata specifications based on automata composition

V. A. Nazarov[a], Bachelor, orcid.org/0009-0000-0352-7885
A. A. Shalyto[a], Dr. Sc., Tech, Professor, orcid.org/0000-0002-2723-2077, anatoly.shalyto@gmail.com
[a]ITMO University, 49, Kronverksky Pr., 197101, Saint-Petersburg, Russian Federation

Introduction: As automata-based specifications are increasingly used in the development of safety-critical systems, their validation is of particular importance and relevance. Testing and verification do not solve this problem, especially when nested finite automata are used. **Purpose:** To develop a method for constructing a product automaton for the class of specifications under consideration, based on the product of transition graphs and applicable to nested automata, in order to simplify the heuristic procedure for its subsequent validation. **Methods:** The study employs the construction of the reachable part of the state space, breadth-first graph traversal, and simulation-based checking of output event sequences. **Results:** The method forms a product automaton with a set of reachable state pairs and a transition mapping, which allows detecting with visual analysis and manually eliminating deadlocks and other incorrect states and transitions. Sequential composition of several automata provides step-by-step verification of the correctness of the entire system. In the example considered, no discrepancies have been found in the output event sequences between the corrected system and the product automaton on the used input event sequences. **Practical relevance:** The proposed method extends the range of tools available for validating automata-based specifications, including those containing nested automata, although it does not guarantee that the product automaton will be simpler than the original system. **Discussion:** The method is particularly useful for analyzing automatically constructed or modified systems of automata, since it helps detect hidden logical contradictions that are difficult to reveal by testing or simulation alone.

Keywords – automata, nested automata, automata composition, validation.

For citation: Nazarov V. A., Shalyto A. A. Validation of automata specifications based on automata composition. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 21–36 (In Russian). doi:10.31799/1684-8853-2026-5-21-36, EDN: IBKLIO

Reference

1. Polikarpova N. I., Shalyto A. A. *Avtomatnoe programmirovanie* [Automata-based programming]. Saint Petersburg, Piter Publ., 2008, 167 p. Available at: http://is.ifmo.ru/books/_book.pdf (accessed 22 March 2026) (In Russian).
2. Adhikary S., Gurung A., Thakkar J., Bruto da Costa A. A., Dey S., Hazra A., Dasgupta P. SMT-based verification of safety-critical embedded control software. *IEEE Embedded Systems Letters*, 2021, vol. 13, no. 3, pp. 138–141. doi:10.1109/LES.2020.3035560
3. André É., Liu S., Liu Y., Choppy C., Sun J., Dong J. S. Formalizing UML state machines for automated verification — A survey. *ACM Computing Surveys*, 2023, vol. 55, no. 13s, art. 277. doi:10.1145/3579821
4. Velder S. E., Lukin M. A., Shalyto A. A., Iaminov B. R. *Verifikatsiia avtomatnykh programm* [Verification of automata-based programs]. Saint Petersburg, Nauka Publ., 2011, 244 p. (In Russian).
5. Yankin Y. Y., Shalyto A. A. A method of finite-state machine realization in electric motor drives control. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2011, no. 1, pp. 50–56 (In Russian). EDN: NEKQXX
6. Filipovikj P., Ung G., Gurov D., Nyberg M. Bounded invariant checking for Stateflow. *Electronic Proceedings in Theoretical Computer Science (EPTCS)*, 2022, vol. 371, pp. 38–52. doi:10.4204/EPTCS.371.3
7. Xiao M., Xu Y., Zhang Y., Yang K., Yan S., Cen L. Formal verification of solidity smart contracts via automata theory. *Symmetry*, 2025, vol. 17, no. 8, art. 1275. doi:10.3390/sym17081275
8. Shalyto A. A. Validation of state machine specifications. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2023, vol. 23, no. 2, pp. 436–438 (In Russian). doi:10.17586/2226-1494-2023-23-2-436-438, EDN: YHATJW
9. Wu R., Du Y., Li M. A model transformation method based on Simulink/Stateflow for validation of UML statechart diagrams. *Mathematics*, 2025, vol. 13, no. 5, art. 724. doi:10.3390/math13050724
10. Barth M., Jakobs M.-C. Test-case generation with automata-based software model checking. *Model Checking Software (SPIN 2024), LNCS*. Springer, vol. 14624, 2024, pp. 248–267. doi:10.1007/978-3-031-66149-5_14
11. Sankur O. Timed automata verification and synthesis via finite automata learning. *Journal of Automated Reasoning*, 2025, vol. 69, art. 15. doi:10.1007/s10817-025-09730-z
12. Burdonov I. B., Kossatchev A. S. Automata system: determinism conditions and testing. *Proceedings of the Institute for System Programming of the RAS,* 2016, vol. 28, no. 1, pp. 151–184 (In Russian). doi:10.15514/ISPRAS-2016-28(1)-9, EDN: WAPNTP
13. Burdonov I. B., Kossatchev A. S. Testing of automata system. *Proceedings of the Institute for System Programming of the RAS,* 2016, vol. 28, no. 1, pp. 103–130 (In Russian). doi:10.15514/ISPRAS-2016-28(1)-7, EDN: WAPNQX
14. Burdonov I. B., Kossatchev A. S. Conformance theory development: semantics, formal models, algorithms. *Proceedings of the Institute for System Programming of the RAS,* 2014, vol. 26, no. 1, pp. 27–72 (In Russian). doi:10.15514/ISPRAS-2014-26(1)-2, EDN: RUMWWB
15. Ermakov A. D., Yevtushenko N. V. Deriving adaptive checking sequence for nondeterministic Finite State Machines. *Proceedings of the Institute for System Programming of the RAS,* 2016, vol. 28, no. 3, pp. 123–144 (In Russian). doi:10.15514/ISPRAS-2016-28(3)-8, EDN: WKFGUV
16. Petrukhnova G. V., Usachev M. G., Popova E. V. Test control of finite state machines. *The Bulletin of Voronezh State Technical University*, 2023, vol. 19, no. 6, pp. 47–52 (In Russian). doi:10.36622/VSTU.2023.19.6.007, EDN: ENHULJ
17. Turker U. C., Hierons R. M., El-Fakih K., Mousavi M. R., Tyukin I. Y. Accelerating finite state machine-based testing using reinforcement learning. *IEEE Transactions on Software Engineering*, 2024, vol. 50, no. 3, pp. 574–597. doi:10.1109/TSE.2024.3358416
18. Kruger L., Junges S., Rot J. Small test suites for active automata learning. *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2024), LNCS,* vol. 14571, Springer, 2024, pp. 109–129. doi:10.1007/978-3-031-57249-4_6
19. Borsotti A., Breveglieri L., Crespi Reghizzi S., Morzenti A. Multi-entry DFA with reduced initial states to speedup parallel recognition. *Implementation and Application of Automata (CIAA 2025), LNCS*, vol. 15981. Springer, 2025, pp. 55–72. doi:10.1007/978-3-032-02602-6_5
20. Vaandrager F., Melse I. New fault domains for conformance testing of finite state machines. *36th International Conference on Concurrency Theory (CONCUR 2025), LIPIcs*, vol. 348, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025, art. 34, pp. 34:1–34:22. doi:10.4230/LIPIcs.CONCUR.2025.34
21. Ferreira D., Lima L. Verifying integrated designs of UML state machines and activities using CSP. *Formal Methods: Foundations and Applications (SBMF 2024), LNCS*, Springer, 2024, pp. 68–85. doi:10.1007/978-3-031-78116-2_5
22. Rahaman H., Chattopadhyay S., Sengupta I. Conformance testing for finite state machines guided by deep neural network. *Journal of Circuits, Systems and Computers*, 2022, vol. 31, iss. 09, art. 2250156, pp. 1–19. doi:10.1142/S0218126622501560
23. Muškardin E., Tappler M., Aichernig B. K., Pill I. Active model learning of stochastic reactive systems. *Software and Systems Modeling*, 2024, vol. 23, no. 2, pp. 503–524. doi:10.1007/s10270-024-01158-0
24. Fortz S., Ghassemi F., Henry L., Howar F., Neele T., Rot J., Suilen M. A research agenda for active automata learning. *International Journal on Software Tools for Technology Transfer*, 2026. doi:10.1007/s10009-026-00839-z
25. Marksteiner S., Schögler D., Sirjani M., Sjödin M. Learning single and compound-protocol automata and checking behavioral equivalences. *International Journal on Software Tools for Technology Transfer*, 2025, vol. 27, pp. 35–52. doi:10.1007/s10009-025-00797-y
26. Henry L., Mousavi M. R., Neele T., Sammartino M. Compositional active learning of synchronizing systems through automated alphabet refinement. *CONCUR 2025, LIPIcs*, vol. 348, Schloss Dagstuhl, 2025, pp. 20:1–20:22. doi:10.4230/LIPIcs.CONCUR.2025.20
27. Manini A., Rossi M., San Pietro P. Random testing of model checkers for timed automata with automated oracle generation. *TASE 2025, LNCS,* vol. 15841, Springer, 2025, pp. 343–360. doi:10.1007/978-3-031-98208-8_20
28. Grobelna I. Formal verification of control modules in cyber-physical systems. *Sensors*, 2020, vol. 20, no. 18, art. 5154. doi:10.3390/s20185154
29. Khokkanen A. V., Shalyto A. A. *Imitator igrovogo avtomata klassa "Odnorukii bandit"* [Simulator of the slot machine of the "One-armed bandit" class]. Saint Petersburg, ITMO Publ., 2003, 44 p. Available at: https://is.ifmo.ru/download/SlotMachine_Report.pdf (accessed 20 May 2026) (In Russian).
30. Shalyto A. A., Tukkel N. I. Translating iterative algorithms into automaton ones. *Programming and Computer Software,* 2002, vol. 28, no. 5, pp. 250–260. doi:10.1023/A:1020208127964

УДК 004.056.53
doi:10.31799/1684-8853-2026-5-37-55
EDN: IULELD

Научные статьи
Articles

Модель и алгоритмы анализа данных киберразведки на основе графа знаний

А. М. Вульфин[a], *доктор техн. наук, профессор, orcid.org/0000-0001-5857-2413, vulfin.alexey@yandex.ru*
В. И. Васильев[a], *доктор техн. наук, профессор, orcid.org/0000-0002-6105-5481*
А. И. Луцкович[a], *старший преподаватель, orcid.org/0009-0000-7257-6947*
А. Д. Кириллова[a], *канд. техн. наук, доцент, orcid.org/0009-0000-4164-2526*
[a] *Уфимский университет науки и технологий, К. Маркса ул., 12, Уфа, 450008, РФ*

Введение: *традиционные системы генерации ответов с расширенным поиском, основанные на векторном поиске по текстовым фрагментам, ограниченно эффективны при многошаговом сопоставлении отчетов киберразведки, национальных классификаторов угроз и международных баз знаний.* ***Цель:*** *разработать и экспериментально оценить модель графа знаний, алгоритмов межонтологического выравнивания и двухконтурного извлечения контекста в ходе анализа данных киберразведки.* ***Методы:*** *модель реализована как ориентированный типизированный граф свойств с набором атрибутов, объединяющий национальный банк данных угроз, международные базы знаний о тактиках и техниках атак, защитных мерах, реестры уязвимостей, классификаторы слабостей программного обеспечения, каталоги шаблонов атак и корпус отчетов киберразведки. Достижение цели оценивается количественными метриками при построении межонтологических связей и анализе возможностей вопросно-ответной системы.* ***Результаты:*** *разработан алгоритм построения межонтологических связей с проверкой по семантическому сходству, доменным ограничениям и выравниванием с контролем корректности с помощью больших языковых моделей. Реализован двухконтурный алгоритм извлечения контекста, объединяющий граф знаний и доказательный слой текстовых фрагментов. Предложен метод анализа данных киберразведки на основе модели графа знаний, алгоритмов построения межонтологических связей и извлечения контекста. На тестовой выборке обучаемый классификатор межонтологических связей достиг значения метрики F_1 = 0,83. Вводимые экспертные связи повысили значение метрики EM полного совпадения предсказанного и эталонного множества идентификаторов с 0,34 до 0,63, автоматические связи обеспечили значение метрики EM = 0,56. Получен значимый прирост значения метрики Entity Recall@50 относительно текстового поиска – 0,5225, и после сокрытия идентификаторов тактик и техник прирост составил 0,5467.* ***Практическая значимость:*** *метод предназначен для поддержки принятия решений аналитиками центра мониторинга информационной безопасности при сопоставлении отчетов киберразведки с национальными и международными базами знаний.* ***Обсуждение:*** *межонтологические связи повышают проверяемость ответа за счет выравнивания с контролем корректности, а слой сводных описаний сообществ графа увеличивает согласованность ответа с извлеченным контекстом при умеренном снижении точности.*

Ключевые слова *— граф знаний, графовая генерация с расширенным поиском, данные киберразведки, тактики и техники, сопоставление онтологий, выравнивание сущностей, большие языковые модели, MITRE ATT & CK, MITRE D3FEND, БДУ ФСТЭК.*

Для цитирования: Вульфин А. М., Васильев В. И., Луцкович А. И., Кириллова А. Д. Модель и алгоритмы анализа данных киберразведки на основе графа знаний. *Информационно-управляющие системы*, 2026, № 5, с. 37–55. doi:10.31799/1684-8853-2026-5-37-55, EDN: IULELD

For citation: Vulfin A. M., Vasilyev V. I., Lutskovich A. I., Kirillova A. D. A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 37–55 (In Russian). doi:10.31799/1684-8853-2026-5-37-55, EDN: IULELD

Введение

Действенную роль в реализации проактивной защиты информационных систем играют методы анализа данных отчетов киберразведки (Cyber Threat Intelligence, CTI) о тактиках, техниках и процедурах (Tactics, Techniques and Procedures, TTP), применяемых злоумышленниками в ходе реализации компьютерных атак [1]. CTI-отчеты обычно представляют собой аналитические или технические документы, содержащие сведения о действиях злоумышленников, применяемом вредоносном программном обеспечении, инфраструктуре атак, индикаторах компрометации и мерах противодействия. Извлечение полезной (структурированной) информации из указанных «сырых» данных в форме некоторых признаков — индикаторов компрометации (Indicators of Compromise, IoC) — является актуальной задачей [2]. IoC рассматриваются как формализуемые признаки инцидента информационной безопасности (ИБ), например сетевые адреса, домены, хеш-суммы файлов, адреса электронной почты и другие наблюдаемые артефакты.

Для решения задач обработки данных CTI-отчетов о TTP злоумышленников все чаще применяются методы искусственного интеллекта, связанные с использованием больших языковых моделей (Large Language Models, LLM) [3, 4]. На практике применение LLM для анализа данных TTP может сталкиваться с рядом ограничений [4, 5]:

— LLM дает ложные сведения, если не знает правильного ответа («галлюцинации»);

— сообщает пользователю устаревшую информацию, в то время как от нее ждут актуальных данных;

— неправильно или неточно обрабатывает запрос из-за нарушения терминологии.

Одним из подходов к уменьшению числа необоснованных ответов LLM является генерация с расширенным поиском (Retrieval-Augmented Generation, RAG) [6]. В RAG-системе перед генерацией ответа выполняется извлечение релевантных фрагментов из внешнего хранилища знаний, далее эти фрагменты передаются в генеративную модель как контекст. Архитектура RAG-системы в общем виде включает модуль извлечения контекста (retriever) и модуль генерации ответа (generator). Примеры применения RAG-систем в задачах обработки слабоструктурированных данных в домене ИБ приводятся в публикациях (см., например, [7, 8]), а также в работе авторов [9].

В то же время, как отмечается, например, в [9], стандартный RAG также не лишен определенных недостатков, таких как:

— потеря контекста (при увеличении фрагментов информации может быть потеряна важная взаимосвязь между ними, что приводит к неполным или неточным ответам);

— сложность работы с многошаговыми вопросами (в случаях, когда требуется объединение информации из нескольких источников или выполнение логических выводов);

— неэффективность при работе с неструктурированными данными (извлечение релевантной информации из неструктурированных данных может быть сложным и неточным).

Для преодоления указанных ограничений развивается направление GraphRAG — графовая генерация ответов с расширенным поиском, при которой извлечение контекста опирается на граф сущностей и отношений. Граф знаний в настоящей работе рассматривается как ориентированный типизированный граф с заданием атрибутов, позволяющий явно представлять угрозы, тактики и техники атак, уязвимости, меры защиты и доказательные фрагменты CTI-отчетов. Графовое представление может повысить связность контекста и обеспечить прослеживаемость использованных фактов, однако эффект зависит от качества исходных данных, формируемых междоменных связей и правил извлечения [10, 11]. Анализ современного состояния исследований позволяет выделить следующие нерешенные проблемы.

Во-первых, существующие GraphRAG-системы для анализа данных CTI-отчетов ориентированы преимущественно на англоязычные источники и международные базы знаний. Интеграция национальных баз знаний, в частности банка данных угроз безопасности информации (БДУ) ФСТЭК России, в графовые структуры RAG-систем исследована недостаточно. Это ограничивает применимость существующих решений для организаций, деятельность которых регулируется российским законодательством в области ИБ и требует соответствия национальным классификаторам угроз.

Во-вторых, методология построения межонтологических связей между гетерогенными базами знаний в области ИБ остается недостаточно формализованной. Базы знаний используют различные таксономии, уровни абстракции и языки описания. Отсутствуют систематизированные подходы к установлению семантических соответствий между угрозами национального классификатора и техниками международных фреймворков, что препятствует формированию единого пространства знаний для комплексного анализа.

В-третьих, вопросы мультиязычного поиска и генерации в GraphRAG-системах для анализа CTI-отчетов исследованы фрагментарно. В рассматриваемом корпусе преобладают англоязычные документы, БДУ ФСТЭК России и запросы аналитиков отечественных центров мониторинга ИБ (Security Operations Center, SOC) представлены преимущественно на русском языке. Используемые многоязычные векторные представления (embeddings) обеспечивают техническую возможность кросс-язычного поиска, однако отдельная оценка режимов RU-RU, EN-EN, RU-EN и EN-RU в настоящем исследовании не проводилась.

Цель работы состоит в разработке и экспериментальной оценке модели графа знаний BDU-KG, алгоритма построения межонтологических связей и алгоритма двухконтурного извлечения контекста. Проверяется гипотеза о том, что включение типизированных графовых фактов и межонтологических связей повышает точное совпадение ответа с эталоном и полноту извлечения сущностей по сравнению с текстовым поиском в многошаговых сценариях. Практическим критерием достижения цели является повышение полноты контекста при контролируемом изменении метрики оценки релевантности извлеченного контекста с учетом его ранжирования (Context Precision) и снижении доли утверждений, не поддержанных переданным контекстом.

Анализ применения графов знаний в области ИБ с помощью GraphRAG-систем

Проблема автоматизации построения графов знаний в области ИБ, предназначенных для анализа и защиты сетевой инфраструктуры, обсуждается во многих публикациях (например, [12, 13]).

Оригинальная двухэтапная процедура генерации графов знаний из текстов домена знаний, где на первом этапе с помощью LLM осуществляется построение непосредственно графов знаний в виде совокупности взаимосвязанных триплетов («субъект» — «отношение» — «объект»), а на втором этапе производится проверка достоверности полученных графовых моделей с использованием онтологий, предложена в [14].

В [15] исследуются вопросы применения LLM с открытым исходным кодом (и весовыми коэффициентами) для извлечения и структурирования знаний в форме триплетов из текстов в области ИБ. Полученные триплеты используются при построении графов знаний, интегрированных с LLM для решения задач перевода, суммаризации текстов и извлечения сущностей. Качество решений оценивалось с помощью метрик ROUGE, предназначенных для сравнения сгенерированного текста с эталонным текстом.

В [16] разработана программная среда Knowledge Graph Verifier для оценки качества данных о TTP, основанная на объединении интерпретируемых графов знаний и LLM как носителей контекстных априорных знаний. В работе предложены критерии, позволяющие автоматически извлекать ключевые утверждения из открытых баз данных о TTP и проверять достоверность этих утверждений.

Общие вопросы архитектуры и применения GraphRAG-систем рассмотрены в [17]. Графовое расширение позволяет учитывать связи между фрагментами и повышать связность контекста, однако само по себе не гарантирует устранения необоснованных ответов или снижения вычислительных затрат.

В [18] обсуждается подход к интеграции графов знаний и RAG-технологии в области кибербезопасности, названный авторами средой CyKG-RAG Framework. Рассмотрены основные этапы проектирования проблемно-ориентированной Graph-RAG-системы. Вначале осуществляется построение графа знаний с использованием двух типов источников: локальных данных логов и событий ИБ, отражающих специфику обеспечения ИБ конкретной организации, и внешних данных из публичных источников и предметных баз знаний.

Графы знаний для предметной области TTP часто строятся путем автоматического извлечения знаний из специализированных текстов на основе правил (rule-based approach) и LLM-ориентированных подходов (LLM-based approach). Однако необработанные знания, извлеченные из CTI-документов, могут быть неточными и неполными. Для минимизации таких ошибок применяются онтологии: они обеспечивают семантическую совместимость данных из разных источников и задают априорные ограничения, повышающие надежность анализа.

Интеграция гетерогенных источников данных предметной области приводит к задаче сопоставления онтологий и выравнивания сущностей (ontology matching / entity alignment, OM/EA). Эта задача заключается в установлении соответствий между концептами, атрибутами и отношениями в разных схемах представления знаний. В отличие от построения графа знаний только на основе текстов, построение межонтологических связей предполагает наличие как минимум двух уже существующих онтологий и необходимость контролировать семантическую корректность связей.

Сущности типа «уязвимости» (CVE), «слабости» (CWE), «шаблоны атак» (CAPEC) и «тактики» злоумышленника могут быть представлены как узлы графа знаний. Каждая сущность ассоциируется со специфическими свойствами, описывающими ее атрибуты, такие как идентификатор, описание, оценка воздействия и возможность эксплуатации. Подобная интеграция позволяет создавать комплексные системы анализа угроз безопасности информации (УБИ).

Извлечение сведений о действиях злоумышленников из CTI-текстов рассмотрено в [19], применение графов знаний при формировании гипотез о реализуемых атаках — в [20]. База MITRE D3FEND представляет граф знаний защитных техник (репозиторий онтологии: https://github.com/d3fend/d3fend-ontology). База CVE2CAPEC используется как источник соответствий между записями CVE, CWE, CAPEC и техниками ATT & CK/D3FEND (https://github.com/Galeax/CVE2CAPEC).

Методы автоматического построения графов знаний предметной области ИБ достигли высокой зрелости. CTIKG [21] демонстрирует 91,89 % точности и 89,39 % полноты при извлечении триплетов, CTINexus [22] обеспечивает гибкую адаптацию к различным онтологиям без обширного дообучения моделей, LLM-TIKG [23] эффективно использует обучение на ограниченном количестве примеров для минимизации ручной разметки.

При переходе от единственного доменного графа знаний к составному графу знаний критическим становится вопрос корректного построения межонтологических связей (мостов). В существующих работах задача сквозного сопоставления между разнородными онтологиями часто решается либо вручную, либо эвристически по текстовому/векторному сходству, либо через LLM-сопоставление. Сопоставление рассмотренных работ по источникам знаний, поддержке национальных классификаторов, русскому языку, механизму происхождения данных, экспертной проверке и прямой оценке межонтологических связей показывает, что существующие решения преимущественно решают одну из трех задач: извлечение графа из англоязычного CTI-корпуса, вопросно-ответный

(Question Answering, QA) поиск по готовому графу либо проверку отдельных утверждений. В них, как правило, отсутствует одновременно реализованный переход от БДУ ФСТЭК России к международным базам знаний ATT & CK и D3FEND, разделение нормативного и доказательного контекста, а также отдельная оценка качества автоматически построенных межонтологических связей. Указанное сочетание признаков определяет научную задачу и границы заявляемой новизны.

Для решения данных проблем предлагается метод анализа данных киберразведки на основе модели графа знаний, алгоритмов построения межонтологических связей и извлечения контекста.

Разработка метода анализа данных киберразведки на основе модели графа знаний, алгоритмов построения межонтологических связей и извлечения контекста

Предлагаемый метод объединяет модель графа знаний, алгоритм построения межонтологических связей и алгоритм двухконтурного извлечения контекста. Далее под термином «проверяемое выравнивание» понимается свойство, при котором для каждой сформированной связи сохраняются источник, версия, компонентные оценки, примененные правила и подтверждающий путь (формальная верификация как метод анализа онтологий не применяется).

Модель предметной области BDU-KG

BDU-KG является концептуальной и логической моделью предметной области, физически реализованной как размеченный граф свойств (Labeled Property Graph). Модель объединяет нормативный слой БДУ ФСТЭК России, базы знаний MITRE ATT & CK и MITRE D3FEND, слои CVE/CWE/CAPEC и доказательные фрагменты CTI-отчетов. Модель BDU-KG не является формальной OWL-онтологией, так как аксиоматический вывод и автоматическая проверка непротиворечивости не применяются.

Модель отличается строгой типизацией сущностей: угрозы, объекты воздействия, компоненты, способы реализации угроз, меры защиты, техники атак, защитные техники, уязвимости, слабости и паттерны атак представлены как типизированные узлы. Отношения между ними разделяются на нормативные связи, заимствованные из исходных баз знаний, и межонтологические связи. Мультиязычные текстовые атрибуты используются как унифицированный носитель семантики для поиска и сопоставления. Это позволяет обеспечить семантическую совместимость русско- и англоязычных источников о TTP, прослеживаемость фактов и корректное структурное расширение подграфа в задачах многошагового анализа.

Граф свойств задается кортежем

$$G = (V, E, \lambda_V, \lambda_E, A_V, A_E, \Pi),$$

где V и E — множества узлов и ориентированных ребер; λ_V и λ_E — функции типизации узлов и отношений; A_V и A_E — их атрибуты; Π — сведения о происхождении данных.

Пусть имеются два графа знаний: $G_B = (V_B, E_B)$ — граф БДУ и $G_M = (V_M, E_M)$ — граф международного фреймворка, например ATT & CK или D3FEND. Здесь V_B и V_M обозначают множества узлов, а E_B и E_M — множества отношений внутри соответствующих графов.

Входом метода являются исходные графы БДУ (G_B) и графы международных фреймворков ATT & CK или D3FEND (G_M), корпус документов D, запрос пользователя q, набор доменных правил R и параметры Θ.

Выход включает множество межонтологических связей B, контекст ответа $C(q)$, ответ y и связанный с ним набор происхождения Π_y.

Критерии достижения цели определяются на двух уровнях: качество межонтологических связей оценивается количественными метриками Precision, Recall, F_1, AUC-ROC и Accuracy; качество QA-системы — количественными метриками Exact Match, F_1, Entity Recall@50, Context Precision, Answer Relevancy и Faithfulness.

Алгоритм построения межонтологических связей с контролем корректности

Предлагаемый алгоритм предназначен для построения межонтологических связей между сущностями БДУ и сущностями ATT & CK/D3FEND с учетом формальных доменных ограничений. Эти связи далее используются в двухконтурном алгоритме извлечения контекста для GraphRAG: нормативные факты БДУ включаются в контекст обязательно, а фрагменты CTI-отчетов используются как доказательный слой.

Алгоритм строит только два типа межонтологических связей: MAPS_TO_TECHNIQUE от способа реализации угрозы RealizationMethod к технике ATT & CK AttackTechnique и IMPLEMENTED_BY от меры защиты BduControl к защитной технике D3fendTechnique. Отношения MITIGATED_BY_CONTROL и DEFENDS_AGAINST являются предметными отношениями, импортируемыми соответственно из БДУ и MITRE D3FEND, и не оцениваются как результат сопоставления сущностей. Прямое отношение BduThreat к AttackTechnique не вводится, угроза связывается с техникой через нормативное отношение REALIZED_BY и узел RealizationMethod.

Каждый узел v из объединения V_B и V_M описывается следующими характеристиками:

— тип type(v) (например, “RealizationMethod”, “AttackTechnique”, “D3fendTechnique”, “BduControl”);

— мультиязычные текстовые поля text(v) = = {*title*, *description*, *synonyms*};

— набор атрибутов attr(v).

Межонтологическая связь задается кортежем

$$b = (u, v, r, s, \varepsilon),$$

где u и v — сущности разрешенных типов; r — тип отношения; $s \in [0, 1]$ — итоговая оценка уверенности в корректности связи; ε — набор проверяемых сведений. Структура ε включает идентификаторы и версии источников, идентификатор документа или записи, подтверждающий текстовый диапазон либо путь в графе, результаты доменных правил, компонентные оценки, итоговый статус и отметку экспертной проверки.

Построение выполняется каскадно. Сначала для каждой исходной сущности формируется не более k кандидатов по косинусному сходству многоязычных векторных представлений и лексическому перекрытию. Затем применяются критические ограничения совместимости типов, допустимого направления отношения и структурной согласованности. Кандидаты, не прошедшие ограничения, исключаются до обращения к языковой модели.

Оставшиеся кандидаты проверяются локальной LLM. Модель получает только описания двух сущностей, результаты правил и доступные доказательства и возвращает метку “match”, “partial” или “no”, числовую оценку и краткое обоснование. В последующей реализации метки отображались на интервалы: “no” — [0; 0,34], “partial” — [0,35; 0,74], “match” — [0,75; 1].

Оценка уверенности может задаваться обучаемым классификатором либо линейной агрегацией компонентных оценок

$$s(u, v) = \alpha \times s_{vec}(u, v) + \beta \times s_{rule}(u, v) + \\ + \gamma \times s_{LLM}(u, v), \quad (1)$$

где $s_{vec}(u, v)$ — косинусное сходство векторных представлений описаний сущностей; $s_{rule}(u, v)$ — оценка прохождения доменных правил; $s_{LLM}(u, v)$ — оценка LLM поддержки связи переданными фактами; α, β и γ ($\alpha + \beta + \gamma = 1$) — веса компонент, задаваемые экспертно или калибруемые на проверочной выборке.

В исходном сравнении использовались веса $\alpha = 0{,}4$, $\beta = 0{,}3$, $\gamma = 0{,}3$ и порог $\tau = 0{,}6$, выбранные на проверочной выборке. В последующей реализации применялись раздельные параметры: для отношений MAPS_TO_TECHNIQUE — 0,50/0,30/0,20 и $\tau = 0{,}65$; для IMPLEMENTED_BY — 0,40/0,40/0,20 и $\tau = 0{,}68$. Значения $0{,}55 \le s < \tau$ направлялись на экспертную проверку; значения ниже 0,55 отклонялись.

Альтернативный вариант построения использует обучаемый классификатор f_θ по 12 признакам: сходству описаний и заголовков, коэффициенту Жаккара для ключевых слов, совместимости типов, наличию и длине подтверждающего пути, общим тактикам и платформам, результату LLM-проверки, соотношению длин описаний и языковому признаку.

Завершаемость алгоритма обеспечивается конечностью множеств исходных сущностей и ограничением k. При индексированном поиске кандидатов вычислительно дорогостоящая LLM-проверка выполняется для не более чем $k|V_B|$ кандидатов, прошедших критические ограничения (вместо полного декартова произведения $|V_B| \times |V_M|$).

Алгоритм 1. BridgeBuild: построение межонтологических связей с контролем корректности

Вход: Базовый граф $G_B = (V_B, E_B)$, объединяемый граф $G_M = (V_M, E_M)$, набор правил **R**, параметр k — максимальное число кандидатов на исходную сущность, пороговое значение τ

Ensure: Набор межонтологических связей B

1: $B \leftarrow \varnothing$
2: **for all** $u \in V_B$ **such that** Eligible(u) **do**
3: C ← TopK(VectorCandidates(u, V_M), k)
4: **for all** $v \in C$ **do**
5: ($pass$, s_{rule}, e_{rule}) ← RuleVerify(u, v, R)
6: **if not** $pass$ **then**
7: **continue**
8: **end if**
9: ($label$, s_{LLM}, e_{LLM}) ← LLMVerify(u, v, e_{rule})
10: s ← $\alpha \cdot s_{vec}(u, v) + \beta \cdot s_{rule} + \gamma \cdot s_{LLM}$
11: **if** $s \ge \tau$ and $label \in \{match, partial\}$ **then**
12: r ← SelectRelation($type(u)$, $type(v)$, $label$, R)
13: $B \leftarrow B \cup \{(u, v, r, s, \varepsilon)\}$
14: **end if**
15: **end for**
16: **end for**
17: **return** B

Шаблон запроса к LLM ограничивает ответ переданным JSON, запрещает использование внешних знаний и требует машиночитаемый формат. Невалидный ответ отклоняется либо повторно запрашивается; автоматическое принятие невозможно при нарушении критического доменного правила. На шаге 13 объект ε объединяет сведения об источниках пары, результаты e_{rule} и e_{LLM} и итоговый статус проверки.

Таким образом, алгоритм построения межонтологических связей основан на алгоритмах OM/EA, отличается процедурой создания связей и их оценки. Использование независимых подтверждающих путей в графе знаний и порогового принятия связи по оценке $s(u, v)$ позволяет снизить долю ложноположительных соответствий и повысить воспроизводимость сопоставлений.

Алгоритм двухконтурного извлечения контекста

Для запроса q контекст формируется как $C(q) = P_{ack}(C_{norm}(q), C_{evid}(q), B_{tok})$, где C_{norm} — нормативное ядро, C_{evid} — доказательный слой, B_{tok} — токенный бюджет. В первом контуре извлекаются стартовые узлы БДУ, после чего выполняется ограниченное расширение по разрешенным типам ребер. Карточки узлов и типизированные триплеты нормативного подграфа включаются в итоговый контекст независимо от наличия внешних текстовых свидетельств.

Во втором контуре сущности нормативного подграфа используются для расширения запроса к векторному хранилищу. CTI-фрагменты и сводные описания сообществ ранжируются по покрытию сущностей нормативного подграфа G_{norm}, близости к запросу, разнообразию источников и избыточности. Дубликаты удаляются по идентификатору источника и нормализованному тексту. При $k = 50$ средний объем сформированного контекста в основной серии составлял около 3000 токенов.

Каждое утверждение ответа связывается с используемыми карточками, отношениями и фрагментами. Такой механизм обеспечивает проверяемость происхождения и уменьшает избыточность контекста.

Алгоритм 2. DualLoopContext: двухконтурное извлечение контекста
Вход: запрос q, токенный бюджет B_{tok}
Выход: упакованный контекст C

1: $S_0 \leftarrow \text{RetrieveBDUNodes}(q, k_1)$
2: $G_{norm} \leftarrow \text{GraphExpand}(S_0, \text{depth} = d_1, \text{edge_allowlist} = \text{NormEdges})$
3: $C_{norm} \leftarrow \text{SummarizeFacts}(G_{norm}, \text{budget} = b_1)$
4: $q' \leftarrow \text{AugmentQuery}(q, \text{Entities}(G_{norm}))$
5: $T \leftarrow \text{RetrieveCTITexts}(q', k_2)$
6: $C_{evid} \leftarrow \text{SelectAndLinkEvidence}(T, G_{norm}, \text{budget} = b_2)$
7: **return** $P_{ack}(C_{norm}, C_{evid}, B_{tok})$

Таким образом, LLM используется как генератор ответа поверх явно извлеченного и проверяемого контекста. Это важно для задач SOC-аналитики: пользователь должен видеть, какие угрозы БДУ, техники ATT & CK, защитные техники D3FEND и фрагменты CTI-отчетов использованы при формировании вывода.

Разработка GraphRAG-системы анализа данных киберразведки

Программная система реализует модель BDU-KG и конвейер генерации ответов с расширенным поиском с поддержкой русско- и англоязычных текстовых представлений. Многоязычность обеспечивается моделью векторных представлений и нормализацией терминов (отдельная экспериментальная оценка всех четырех кросс-язычных направлений в основной серии не проводилась).

В отличие от классического RAG, где контекст формируется исключительно из фрагментов документов, система приоритизирует графовые факты БДУ (объекты, последствия, способы реализации, меры) и использует текстовые доказательства как дополнительный слой обоснования.

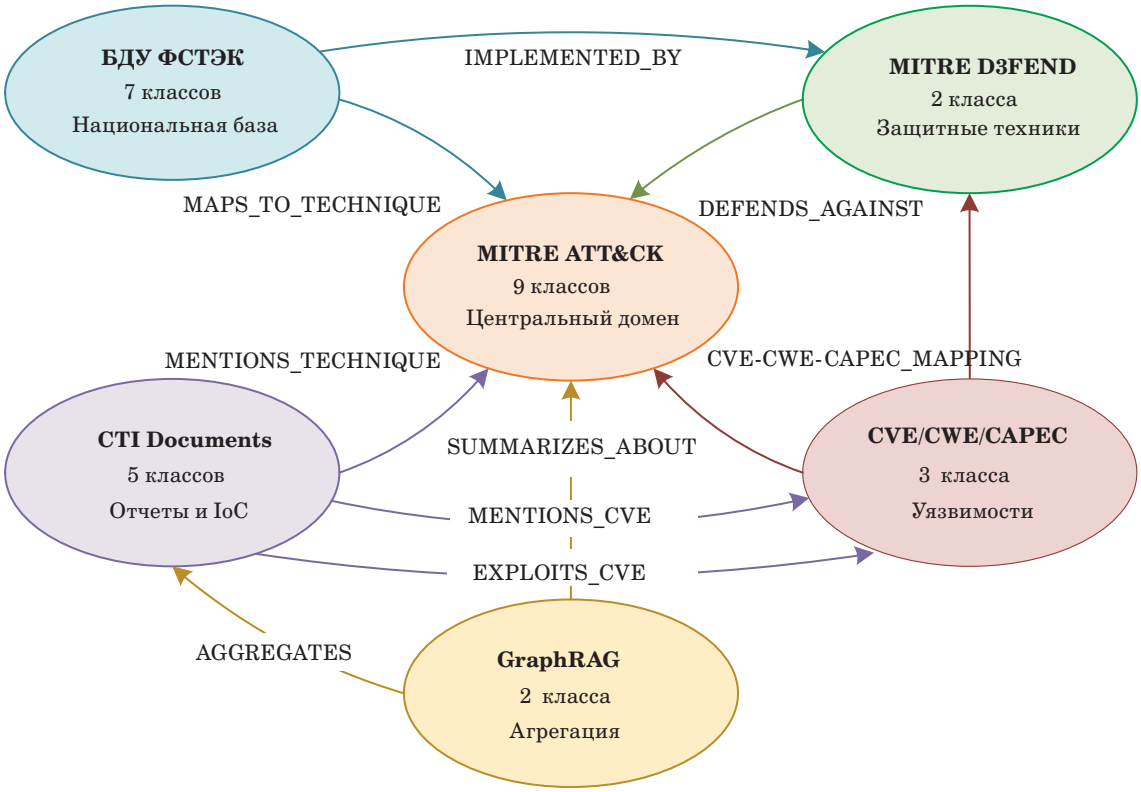
Граф знаний BDU-KG объединяет шесть взаимосвязанных доменов (рис. 1, табл. 1). На концептуальном уровне задаются типы сущностей и отношений; на логическом уровне — ограничения допустимых направлений и атрибуты происхождения; физическая реализация выполнена в Neo4j как размеченный граф свойств.

Проектная физическая схема графа (рис. 2) содержит 30 меток узлов и 23 типа отношений. В экспериментальном снимке экземпляры присутствовали для 24 меток; шесть резервных меток, относящихся к необязательным CTI-сущностям и вспомогательным слоям агрегации, не участвовали в расчете метрик. Междоменные отношения MAPS_TO_TECHNIQUE и IMPLEMENTED_BY формирует алгоритм BridgeBuild.

В экспериментальном дизайне предусмотрены две альтернативные реализации связей между графами, дающие разные компромиссы по трудоемкости и качеству.

1. Вариант M_1. Строится таблица соответствий, подготовленная экспертами в полуавтоматическом режиме.

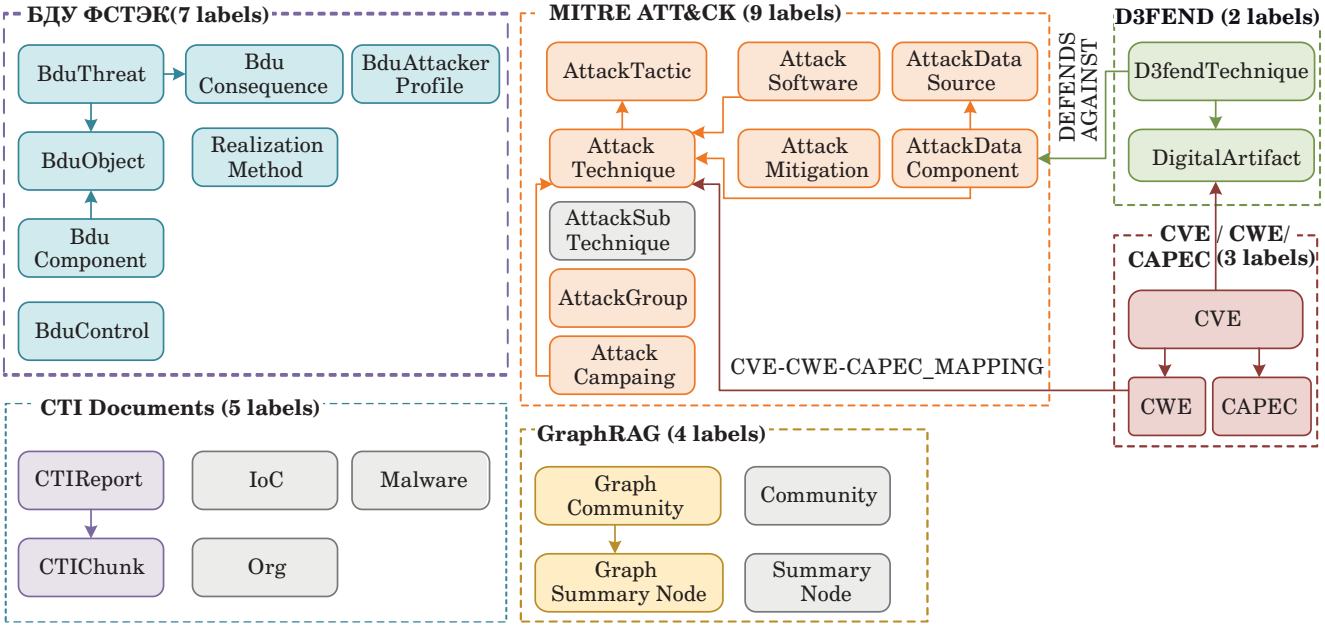
2. Вариант M_2. С помощью предложенного алгоритма построения межонтологических связей между национальным каталогом угроз и международными фреймворками вариант M_2 реализует полуавтоматическое построение межонтологических связей на основе комбинирования: семантической близости текстовых описаний, доменных ограничений/правил согласованности и ограниченной LLM-верификации, выполняемой только после прохождения критических фильтров.



■ ***Рис. 1.*** Концептуальная модель графа знаний BDU-KG
■ ***Fig. 1.*** Conceptual model of the BDU-KG knowledge graph

■ ***Таблица 1.*** Объединяемые домены
■ ***Table 1.*** Interrelated domains

Домен	Описание
БДУ ФСТЭК	Содержит классы для представления УБИ (BduThreat), объектов воздействия (BduObject), компонентов информационных систем (BduComponent), мер защиты (BduControl), негативных последствий (BduConsequence) и способов реализации угроз (RealizationMethod). Связи между классами отражают семантику отношений: угроза направлена на объект, реализуется определенным способом и приводит к последствиям
MITRE ATT & CK	Представлен классами тактик (AttackTactic), техник (AttackTechnique), групп злоумышленников (AttackGroup), кампаний (AttackCampaign), вредоносного программного обеспечения (AttackSoftware), мер противодействия (AttackMitigation) и источников данных для обнаружения (AttackDataSource, AttackDataComponent). Иерархическая структура техник и их принадлежность тактикам моделируются связями “CHILD_OF” и “PART_OF_TACTIC”
MITRE D3FEND	Включает защитные техники (D3fendTechnique) и цифровые артефакты (DigitalArtifact), на которых они разворачиваются. Связь “DEFENDS_AGAINST” обеспечивает сопоставление защитных техник с техниками атак ATT & CK
CWE-CVE-CAPEC	Объединяет записи CVE, классификацию CWE и паттерны атак CAPEC. Связи между ними позволяют проследить цепочку от конкретной уязвимости через эксплуатируемую слабость к технике атаки
CTI-отчеты о TTP	Содержит отчеты и их текстовые фрагменты, а также классы для индикаторов компрометации (IoC), вредоносных программ (Malware) и организаций (Org)
GraphRAG	Включает иерархические сообщества (GraphCommunity) и их текстовые резюме (GraphSummaryNode), формируемые конвейером Microsoft GraphRAG для поддержки глобального поиска по корпусу документов



■ ***Рис. 2.*** Физическая схема графа знаний BDU-KG
■ ***Fig. 2.*** Physical diagram of the BDU-KG knowledge graph

Экспериментальная оценка эффективности предложенного метода

Цель серии экспериментов — оценить качество автоматически построенных межонтологических связей и влияние компонентов BDU-KG на качество ответов. На первом уровне сравниваются классификаторы и методы OM/EA; на втором — конфигурации QA-системы по трем сценариям.

Для основной серии использован корпус из 2262 CTI-отчетов из 169 открытых источников (табл. 2). Он включает публикации компаний в области ИБ, публичные репозитории отчетов и бюллетени центров реагирования на компьютерные инциденты. Документы содержат сведения о TTP злоумышленников, индикаторах компрометации и мерах противодействия.

Пример межонтологической трассировки

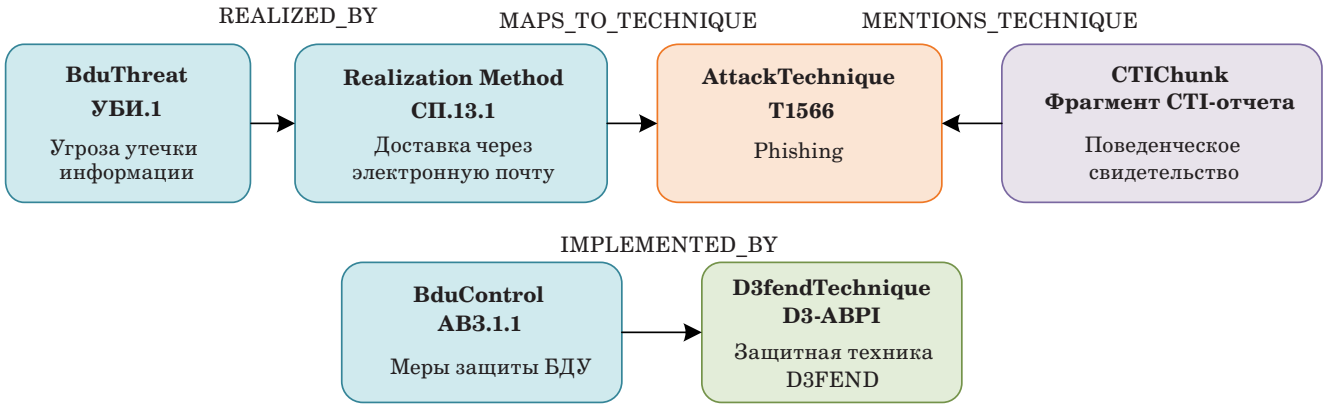
Два отдельных фрагмента межонтологической трассировки приведены на рис. 3. Нормативное отношение REALIZED_BY связывает УБИ.1 «Угроза утечки информации» со способом СП.13.1; связь MAPS_TO_TECHNIQUE соединяет способ с техникой T1566 Phishing (фишинг). Отношение MENTIONS_TECHNIQUE показывает присоединение текстового фрагмента. Отдельно мера АВЗ.1.1 связана с D3-ABPI отношением IMPLEMENTED_BY. Прямая нормативная связь УБИ.1 с АВЗ.1.1 не утверждается. Имена ребер на рисунке обозначают логические типы.

Статистика физической схемы представления графа знаний такова:

— типы узлов — 30;
— реализованные типы узлов — 24;
— типы связей — 23;
— межподсистемные связи — 5.

■ ***Таблица 2.*** Статистика собранного набора данных
■ ***Table 2.*** Statistics of the collected dataset

Характеристика	Значение
Общее количество документов	2262
Количество источников	169
Преобладающий язык	Английский (70 %)
Основные вендоры	Kaspersky, FireEye, Symantec, ESET, Trend Micro, Palo Alto Networks, CrowdStrike
Тематика	APT-группировки, вредоносное ПО, целевые атаки, IoC



■ ***Рис. 3.*** Проверяемые фрагменты межонтологической трассировки BDU-KG
■ ***Fig. 3.*** Verifiable fragments of BDU-KG cross-ontology tracing

Оценка алгоритма построения межонтологических связей

Задача сформулирована как бинарная классификация пар сущностей (u, v), где $u \in V_{BDU}$, $v \in V_{MITRE}$, $y = 1$ означает наличие корректной межонтологической связи. Подтвержденный набор содержит 2630 пар и разделен на обучающую, проверочную и тестовую части в пропорции 70/15/15: 1841, 395 и 394 пары. Разделение стратифицировано по типам сущностей и источникам.

Для каждой пары (u, v) строится вектор из 12 типов признаков (табл. 3).

Положительные примеры включают 847 экспертных пар BduThreat-AttackTechnique, 312 отношений D3FEND-ATT & CK и 156 проверенных цепочек CVE/CWE/CAPEC (табл. 4). Этот смешанный набор используется для оценки классификатора соответствий и не является отдельной оценкой двух типов связей, создаваемых алгоритмом BridgeBuild в подразделе «Алгоритм построения межонтологических связей с контролем корректности». Отрицательные примеры включают сложные пары с высоким семантическим сходством и случайные пары с балансировкой типов.

Сравниваются четыре подхода к построению классификатора (табл. 5).

Гиперпараметры подбирались с помощью кросс-валидации с пятью проходами на обучающей части, порог решения выбирался по максимуму F_1 на проверочной части. Тестовая часть использовалась для итоговой оценки согласно зафиксированному протоколу ранней редакции (табл. 6).

■ ***Таблица 3.*** Векторы признаков, используемые для обучения классификатора
■ ***Table 3.*** Feature vectors used to train the classifier

Признак	Описание	Диапазон
sim_vec	Косинусное сходство BGE-M3 вложений	[0, 1]
sim_title	Косинусное сходство только заголовков	[0, 1]
jaccard_keywords	Коэффициент Жаккара для извлеченных ключевых слов	[0, 1]
score_rule_type	Оценка совместимости типов (0/0,5/1)	{0, 0,5, 1}
score_rule_struct	Наличие подтверждающего пути в графе	{0, 1}
path_length	Минимальная длина пути через CVE/CWE/CAPEC	[0, 10]
common_tactics	Число общих тактик ATT & CK	[0, 14]
common_platforms	Число общих платформ	[0, 8]
score_llm	Оценка LLM-верификатора	[0, 1]
llm_confidence	Эвристическая оценка по длине обоснования LLM (не калиброванная вероятность)	[0, 1]
desc_length_ratio	Отношение длин описаний	[0, 1]
lang_match	Совпадение языка описаний	{0, 1}

■ ***Таблица 4.*** Структура набора данных для оценки межонтологических связей
■ ***Table 4.*** Dataset structure for evaluating cross-ontology links

Класс	Количество пар	Источник
Положительный	847	Экспертно проверенные пары BduThreat-AttackTechnique
	312	Определенные в исходных онтологиях пары D3FEND-ATT & CK
	156	Цепочки CVE/CWE/CAPEC с экспертной проверкой
Отрицательный	420	Сложные отрицательные пары: $s_{vec} > 0{,}7$, отклоненные экспертами
	895	Случайные отрицательные пары с балансировкой типов

■ ***Таблица 5.*** Проанализированные подходы к построению классификатора
■ ***Table 5.*** Analyzed approaches to classifier construction

Обозначение	Название	Характеристика
M_{base}	Линейная комбинация (контрольная модель)	Формула (1) с весами $\alpha = 0{,}4$, $\beta = 0{,}3$, $\gamma = 0{,}3$, порогом $\tau = 0{,}6$, подобранными с помощью grid search на validation set
M_{LR}	Логистическая регрессия	12 признаков с L2-регуляризацией ($C = 1{,}0$) Интерпретируемые веса признаков
M_{MLP}	Многослойный перцептрон	Количество нейронов по слоям: 12, 32, 16, 1 Функции активации: ReLU (скрытые слои), Sigmoid (выход) Dropout: 0,3 между слоями Оптимизатор: Adam, lr = 0,001 Early stopping по validation loss (patience = 10)
M_{XGB}	Gradient Boosting (XGBoost)	n_estimators = 100, max_depth = 4 Автоматический подбор важности признаков

■ ***Таблица 6.*** Качество классификации межонтологических связей на тестовой выборке
■ ***Table 6.*** Cross-ontology link classification quality on the test set

Модель	Precision	Recall	F_1	AUC-ROC	Accuracy
M_{base}	0,78	0,71	0,74	0,81	0,76
M_{LR}	0,82	0,79	0,80	0,87	0,81
M_{MLP}	0,85	0,82	0,83	0,91	0,84
M_{XGB}	0,84	0,83	0,83	0,90	0,85

Наибольшее значение F_1, равное 0,83, получено для M_{MLP} и M_{XGB}. По результатам классификации соответствий M_{XGB} рекомендован для дальнейшего применения с учетом возможности анализа важности признаков. Наиболее значимыми признаками были семантическое сходство описаний (0,23), наличие структурного подтверждающего пути (0,18), LLM-оценка (0,15) и длина пути через CVE/CWE/CAPEC (0,12) (табл. 7).

Статистическая значимость различий в качестве классификатора связей оценивалась непараметрическим методом bootstrap. Для 1000 ресэмплирований тестового набора с возвращением вычислялась метрика F_1 и разность $\Delta = F_1(B) - F_1(A)$. Далее строился 95%-й доверительный интервал для Δ процентильным методом; отсутствие нуля в интервале интерпретировалось как статистически значимое различие на уровне ($\alpha = 0{,}05$).

Анализ ошибок выявил 23 ложноположительных случая, обусловленных, главным образом, смешением уровней абстракции и поверхностным семантическим сходством, и 28 ложноотрицательных случаев, связанных с неочевидными путями CVE/CWE и мультиязычными парами с низкой векторной близостью.

Качественный анализ ошибочных классификаций связей приведен в табл. 8.

Предложенный алгоритм сопоставлялся с пороговым косинусным сходством, LogMap-Lite, прямой LLM-проверкой и LLM-проверкой кандидатов Top-K (табл. 9).

Алгоритм BridgeBuild в варианте M_{XGB} обеспечил значение для метрики $F_1 = 0{,}83$ при среднем времени обратки 0,33 с на пару. На тестовом множестве число LLM-вызовов сократилось приблизительно в семь раз. При обработке полного

■ ***Таблица 7.*** Важность признаков по модели M_{XGB} (нормализованная)
■ ***Table 7.*** Feature importance according to the M_{XGB} model (normalized)

Ранг	Признак	Важность	Интерпретация
1	sim_vec	0,23	Семантическое сходство текстовых описаний — основной признак
2	score_rule_struct	0,18	Структурные пути в графе критичны для верификации связей
3	score_llm	0,15	LLM-оценка значима, но не доминирует
4	path_length	0,12	Короткие пути через CVE/CWE подтверждают связь
5	common_tactics	0,09	Общие тактики — косвенный индикатор
6	jaccard_keywords	0,07	Лексическое пересечение полезно
7	score_rule_type	0,06	Совместимость типов — необходимое условие
8–12	Остальные	0,10	Вспомогательные признаки

■ ***Таблица 8.*** Анализ основных ошибочных классификаций связей
■ ***Table 8.*** Analysis of the main misclassifications of relationships

Типы ошибок	Описание
False Positives (ложные связи)	14 случаев: высокое текстовое сходство при разных уровнях абстракции (например, общая угроза БДУ сопоставлена с узкоспециализированной техникой ATT & CK) 9 случаев: ошибочная LLM-верификация из-за поверхностного семантического сходства
False Negatives (пропущенные связи)	16 случаев: связи через неочевидные цепочки CVE/CWE, не покрытые признаками 12 случаев: мультиязычные пары с низким sim_vec из-за ошибочного сопоставления

■ ***Таблица 9.*** Сравнение методов построения межонтологических связей
■ ***Table 9.*** Comparison of cross-ontology link construction methods

Метод	Описание	Категория	Precision	Recall	F_1	Время, с/пара	LLM-вызовы
Cosine-Threshold	Косинусное сходство BGE-M3 векторов вложений с порогом $\tau = 0{,}75$	На основе векторов вложений	0,62	0,78	0,69	0,002	0
LogMap-Lite	Версия LogMap с лексическим и структурным сопоставлением	Классический OM	0,71	0,54	0,61	0,008	0
LLM-Direct	Прямой запрос к LLM для каждой пары без предварительной фильтрации	LLM-based	0,79	0,81	0,80	2,1	645
LLM-TopK	Генерация Top-K кандидатов по векторам вложений и LLM-верификация всех кандидатов	Гибридный	0,76	0,84	0,80	1,8	6450
BridgeBuild M_{base}	Предложенный метод с линейной комбинацией оценок	Предложенный	0,78	0,71	0,74	0,31	89
BridgeBuild M_{XGB}	Предложенный метод с обучаемым классификатором	Предложенный	0,84	0,83	0,83	0,33	92

пространства (1247 сущностей БДУ × 623 техники ATT & CK) возможных пар сущностей каскадная фильтрация сократила число LLM-проверок приблизительно до 1200. Время работы алгоритма BridgeBuild распределялось следующим образом: генерация кандидатов — 12 %, доменные правила — 8 %, LLM-проверка — 78 %, классификация — 2 %.

Сценарии и конфигурации тестирования на корпусе CTI-отчетов

Проанализированы три класса QA-задач, различающиеся центральной сущностью запроса и требуемой глубиной рассуждения. Для BDU-QA сценариев центральной сущностью является угроза из БДУ ФСТЭК России, представляемая узлом BduThreat. Для Crosswalk-QA сценариев требуется переход между TTP-фрагментом, техниками ATT & CK, угрозами БДУ и защитными техниками D3FEND. Для сценариев TTP-QA основной входной объект — фрагмент CTI-отчета.

Цель эксперимента — оценить вклад каждого компонента архитектуры BDU-KG в качество ответа: векторного извлечения, структурного расширения подграфа, межонтологических связей M_1/M_2 и слоя обобщения групп сущностей.

В эксперименте используются следующие источники знаний, импортируемые в единый BDU-KG:

— БДУ ФСТЭК: угрозы (УБИ), объекты, компоненты, способы реализации, меры защиты, негативные последствия, профили нарушителей;

— ATT & CK (STIX): Enterprise/ICS/Cloud. В качестве эталонного формата используется репозиторий MITRE CTI/STIX;

— MITRE D3FEND (онтология): защитные техники и артефакты;

— CVE2CAPEC: связка CVE-CWE-CAPEC-ATT & CK-D3FEND как независимый слой для проверки качества связей;

— корпус CTI-отчетов как источник текстовых свидетельств и задач CTI-QA.

Векторный слой реализуется в СУБД Qdrant. Используются коллекции “kg_nodes”, “descriptions” и “cti_chunks”. Коллекция “kg_nodes’ содержит векторные представления карточек сущностей графа; “descriptions” — расширенные текстовые описания узлов и отношений; “cti_chunks” — фрагменты CTI-отчетов. Такая декомпозиция позволяет отдельно оценивать вклад поиска по графовым сущностям и поиска по текстовым свидетельствам.

Загрузка CTI-документов создает узлы отчетов и фрагментов, нормализует идентификаторы и сохраняет ссылку на снимок источника. Векторные представления карточек сущностей, описаний и CTI-фрагментов индексируются раздельно, что позволяет оценивать вклад структурного и текстового каналов.

Эксперименты формируются в трех взаимодополняющих сценариях.

Сценарий A (BDU-QA) проверяет ответы на вопросы по структуре БДУ: затронутые объекты и компоненты, негативные последствия, способы реализации, меры защиты и релевантность профилей нарушителя. Эталонная разметка задается в виде текстового ответа и множества идентификаторов БДУ.

Сценарий B (Crosswalk-QA) проверяет построение сквозных сопоставлений. На вход подается фрагмент CTI-отчета; требуется извлечь TTP и другие сущности, сопоставить их с УБИ и сформировать объяснение через подграф «TTP — ATT & CK — БДУ — меры БДУ — D3FEND».

Сценарий C (TTP-QA) проверяет способность системы по фрагменту CTI-отчета определить техники ATT & CK, возможные УБИ и релевантные контрмеры D3FEND/БДУ.

В качестве базовых конфигураций сравнения использованы: B_0 — Microsoft GraphRAG retrieval, использующий суммаризацию сообществ узлов и текстовые фрагменты корпуса без обращения к структурному графу BDU-KG; B_1 — KG-only QA, использующий только графовый поиск и расширение подграфа в Neo4j без векторного слоя; C_0 — Text-RAG, основанный на векторном поиске по фрагментам CTI-отчетов. Предлагаемые графовые конфигурации C_1–C_4 позволяют последовательно оценить вклад BDU-KG, межонтологических связей M_1/M_2 и слоя суммаризации сообществ (табл. 10).

Во всех конфигурациях использовались одинаковые векторные представления BGE-M3 и единый LLM-слой генерации ответов — Gemma3:27B через Ollama. Для оценки метрик с помощью RAGAS отдельно применялась модель GPT-4o в роли модели-судьи, что исключает совпадение генератора ответа и оценивателя.

Для каждого из трех сценариев сформировано по 250 тестовых вопросов, всего 750 вопросов. Эталонная разметка включает нормализованное множество идентификаторов и, где применимо, текстовое пояснение. Вопросы BDU-QA охватывают атрибуты угроз БДУ; Crosswalk-QA требуют междоменного перехода; TTP-QA направлены на извлечение техник и связанных защитных сущностей из CTI-фрагментов.

Наборы вопросов сформированы стратифицированно по типам запросов, целевым сущностям и языку источника. Для BDU-QA выровнены классы по объектам, компонентам, последствиям, способам реализации и мерам защиты; для Crosswalk-QA и TTP-QA контролировались тип цепочки и язык исходного фрагмента. Отдельный независимый набор, полностью исключенный из разработки графа и настройки порогов, в основной серии не формировался.

Метрики и протокол оценки сценариев

Метрики качества ответа на уровне идентификаторов. Точное совпадение (Exact Match, EM) равно 1 при полном совпадении нормализованного множества идентификаторов с эталоном и 0 в противном случае. Мера F_1 (F1-score) представляет собой гармоническое среднее точности и полноты: точность (Precision) отражает долю корректных идентификаторов среди выданных,

■ ***Таблица 10.*** Сравниваемые конфигурации в одинаковых условиях векторных представлений и LLM-слоя
■ ***Table 10.*** Comparable configurations under the same embedding/LLM backend conditions

ID	Конфигурация	Векторный вывод	Структурный вывод на KG	Межонтологические связи	Community/ Summary слой	Источники контекста	Роль в эксперименте
B_0	Microsoft GraphRAG-	Да	Нет	Нет	Да	TTP-корпус и обобщения сообществ, построенные по документам и сущностному графу корпуса	Базовая модель из класса GraphRAG: global retrieval по обобщениям без использования доменного графа и ограничений
B_1	KG-only QA без векторного поиска	Нет	Да	Нет	Нет	BDU-KG (узлы и ребра Neo4j)	Оценка вклада только структурного графа без векторного слоя и без обобщений
C_0	Text-RAG	Да	Нет	Нет	Нет	TTP-корпус	Базовый Text-RAG: только векторный поиск по фрагментам текста
C_1	GraphRAG-BDU	Да	Да	Нет	Нет	BDU-KG (без межонтологического выравнивания) и TTP	Базовый граф и векторный поиск: предлагаемый алгоритм извлечения контекста внутри БДУ-домена
C_2	Bridges-M1 (curated)	Да	Да	Да (M_1)	Нет	BDU-KG и межонтологические связи (M_1) и TTP	Основная конфигурация для Crosswalk-QA
C_3	Bridges-M2 (auto)	Да	Да	Да	Нет	BDU-KG и межонтологические связи (M_2) и TTP	Автоматизированное выравнивание
C_4	C3 и Communities	Да	Да	Да (M_2)	Да	BDU-KG, межонтологические связи (M_2), TTP-корпус и суммаризация сообществ	Усиление полноты контекста (для TTP-QA) за счет глобального слоя обобщения; возможное снижение Context Precision

а полнота (Recall) — долю найденных идентификаторов среди эталонных. Метрики рассчитываются раздельно для идентификаторов УБИ, ATT & CK, D3FEND и CVE/CWE/CAPEC после нормализации форматов. Для каждого вопроса мера F_1 рассчитывается по пересечению нормализованных множеств идентификаторов ответа и эталона. В таблицах приведено среднее арифметическое индивидуальных значений F_1 по вопросам соответствующего сценария, все вопросы имеют одинаковый вес.

Метрики RAGAS [24]. Faithfulness оценивает долю утверждений, поддержанных предоставленным контекстом, и не является оценкой фактической истинности. Answer Relevancy отражает соответствие ответа вопросу, Context Precision — релевантность и порядок извлеченных фрагментов. Оценивание выполнялось LLM GPT-4o отдельно от локальной модели-генератора Gemma3:27B. Экспертная калибровка моделисудьи в основной серии не проводилась, поэтому RAGAS-метрики используются как вторичные.

Метрики извлечения контекста. Entity Recall@K определяется как доля эталонных сущностей, присутствующих среди K элементов контекста. Для Text-RAG сущности восстанавливаются по каноническим идентификаторам и привязкам фрагментов к сущностям графа. При $K = 50$ в контекст включались карточки узлов, типизированные отношения и краткие CTI-фрагменты; средний объем составлял около 3000 токенов.

Экспериментальные результаты

Значения метрики Entity Recall@K рассчитывались при $K = 50$. Агрегированные результаты по трем сценариям тестирования представлены в табл. 11–13. Сценарий BDU-QA предназначен для оценки ответов на вопросы по структуре БДУ ФСТЭК России. Сценарий Crosswalk-QA оценивает качество сквозного сопоставления между отчетами кибервразведки, техниками атак, УБИ и мерами защиты. Сценарий TTP-QA направлен на проверку качества анализа фрагментов отчетов о тактиках, техниках и процедурах злоумышленников.

■ ***Таблица 11.*** Качество ответов BDU-QA
■ ***Table 11.*** BDU-QA response quality

Конфигурация	EM	F_1	Entity Recall@50	Faithfulness	Answer Relevancy	Context Precision
B_0	0,55	0,70	0,66	0,82	0,87	0,60
B_1	0,63	0,76	0,72	0,90	0,85	0,74
C_0	0,48	0,65	0,62	0,80	0,86	0,55
C_1	0,77	0,86	0,88	0,93	0,89	0,78
C_2	0,78	0,86	0,89	0,92	0,90	0,74
C_3	0,76	0,85	0,88	0,92	0,89	0,73
C_4	0,78	0,86	0,90	0,92	0,90	0,72

■ ***Таблица 12.*** Качество ответов Crosswalk-QA
■ ***Table 12.*** Crosswalk-QA response quality

Конфигурация	EM	F_1	Entity Recall@50	Faithfulness	Answer Relevancy	Context Precision
B_0	0,26	0,44	0,36	0,74	0,83	0,48
B_1	0,25	0,42	0,34	0,75	0,81	0,58
C_0	0,21	0,38	0,30	0,70	0,82	0,46
C_1	0,34	0,52	0,47	0,78	0,84	0,53
C_2	0,63	0,74	0,79	0,90	0,88	0,69
C_3	0,56	0,68	0,72	0,87	0,87	0,64
C_4	0,65	0,75	0,81	0,89	0,89	0,66

■ ***Таблица 13.*** Качество ответов TTP-QA
■ ***Table 13.*** TTP-QA response quality

Конфигурация	EM	F_1	Entity Recall@50	Faithfulness	Answer Relevancy	Context Precision
B_0	0,36	0,54	0,47	0,76	0,84	0,46
B_1	0,30	0,45	0,40	0,74	0,81	0,57
C_0	0,26	0,41	0,33	0,68	0,80	0,44
C_1	0,38	0,55	0,49	0,78	0,83	0,50
C_2	0,49	0,63	0,60	0,84	0,85	0,54
C_3	0,46	0,61	0,57	0,82	0,85	0,53
C_4	0,55	0,69	0,71	0,86	0,88	0,52

Внутреннее сопоставление конфигураций показывает различия в полноте извлечения релевантных сущностей и поддержке ответов контекстом. Наиболее простой вариант текстовой генерации с расширенным поиском, обозначенный как Text-RAG (C_0), использует только векторный поиск по текстовым фрагментам. В отличие от него конфигурация GraphRAG-BDU (C_1) дополнительно применяет структурное расширение по графу знаний BDU-KG. За счет этого в контекст включаются не только найденные текстовые фрагменты, но и связанные с ними сущности: угрозы, объекты воздействия, способы реализации угроз и меры защиты.

Переход от конфигурации C_0 к конфигурации C_1 приводит к росту точного совпадения ответа с эталоном в сценариях BDU-QA и TTP-QA. Кроме того, в сценарии BDU-QA наблюдается увеличение Entity Recall@50, что указывает на более полное извлечение нормативных сущностей банка данных угроз. Данный результат согласуется с принципом работы графового расширения: после нахождения исходных релевантных узлов система дополнительно включает в контекст связанные с ними элементы подграфа, необходимые для построения обоснованного ответа.

Таким образом, эксперимент подтверждает, что графовый контекст обеспечивает более устойчивую основу для ответа на многошаговые вопросы, чем изолированный поиск по текстовым фрагментам. При этом полученный прирост следует интерпретировать как результат более полного включения структурированных сущностей и связей в тех сценариях, где ответ требует перехода между несколькими предметными слоями. Полученные различия характеризуют исследованные конфигурации и набор вопросов. Они не отделяют эффект графовой структуры от эффекта доступа к дополнительным нормативным фактам и межонтологическим связям и не доказывают переносимость результата на независимую выборку.

В сценарии Crosswalk-QA, предназначенном для оценки сквозного сопоставления между отчетами о тактиках, техниках и процедурах злоумышленников, базой MITRE ATT & CK, БДУ ФСТЭК России и MITRE D3FEND, основной прирост качества обеспечивается межонтологическими связями. Добавление экспертно подготовленных связей M_1 в конфигурации C_2 повышает значение точного совпадения с эталоном с 0,34 для C_1 до 0,63. Автоматически построенные связи M_2 в конфигурации C_3 дают значение 0,56. Различие между C_2 и C_3 составляет 0,07 по точному совпадению и 0,06 по мере F_1, что показывает применимость автоматизированного выравнивания при ограниченных возможностях ручной проверки.

Переход к графовым конфигурациям также повышает контекстную подтвержденность ответов. В Crosswalk-QA Faithfulness возрастает с 0,70 для C_0 до 0,90 для C_2. Это означает, что большая доля утверждений поддерживается переданным контекстом (показатель не следует интерпретировать как доказательство фактической истинности ответа).

Слой сводных описаний сообществ графа, используемый в конфигурации C_4, повышает полноту извлечения сущностей, особенно в сценарии TTP-QA, где ответ требует обобщения сведений из нескольких отчетов. Однако включение таких обобщений может снижать точность контекста, поскольку часть фрагментов имеет косвенную, а не прямую связь с запросом. Поэтому C_4 следует рассматривать как конфигурацию, ориентированную на повышение полноты, но не как универсально лучшую по всем метрикам.

Сравнение с базовыми подходами B_0 и B_1 показывает различную роль компонентов системы. Для BDU-QA более эффективен структурный поиск по графу знаний, тогда как для TTP-QA больший вклад дают сводные описания корпуса. В сценарии Crosswalk-QA оба базовых подхода остаются близкими к текстовой генерации с расширенным поиском, поскольку не используют слой межонтологического выравнивания. Существенное улучшение качества достигается только в конфигурациях C_2 и C_3, где явно заданы связи между доменами знаний.

Для дополнительной проверки устойчивости после основной серии был выполнен детерминированный замер на отдельном наборе TTP-QA. Парный кластерный бутстрэп с 10 000 повторных выборок и поправкой Холма показал прирост Entity Recall@50 графовой конфигурации относительно BM25, равный 0,5225 при 95%-м доверительном интервале [0,4825; 0,5611] на 216 вопросах ($p < 0{,}0004$). После удаления кодов и названий техник из 208 вопросов прирост составил 0,5467 [0,5063; 0,5849] ($p < 0{,}0004$).

Замена линейной модели M_{base} на M_{XGB} в конфигурации C_3 повысила EM с 0,56 до 0,61, F_1 — с 0,68 до 0,72, Faithfulness — с 0,87 до 0,89 (табл. 14). Основное сравнение C_0–C_4 сохраняет исходную конфигурацию C_3 с M_{base}.

Дополнительный эксперимент с тремя генеративными моделями и тремя моделями векторного представления текста подтвердил устойчивость полученных результатов (табл. 15, 16, лучший результат выделен полужирным; формат ячейки: EM / F_1 / Faithfulness): конфигурация C_2 превосходит C_0 во всех рассмотренных комбинациях. Это свидетельствует о том, что основной вклад в повышение качества вносит не выбор конкретной языковой модели, а использование межонтологических связей и графового извлечения контекста.

Прирост точного совпадения с эталоном (EM) наблюдается для всех сочетаний генеративных и векторных моделей, что подтверждает устойчивость преимущества графовой генерации с расширенным поиском при наличии межонтологических связей. При этом качество модели векторного представления текста оказывает более заметное влияние на результат, чем выбор LLM. Наилучшие значения в проведенных экспериментах получены при совместном использовании Gemma3:27B и BGE-M3.

Результаты показывают различную роль компонентов системы. Структурный граф БДУ ФСТЭК России наиболее эффективен для нормативных запросов, межонтологические связи определяют качество сквозного сопоставления между доменами знаний, а слой сводных описаний

■ ***Таблица 14.*** Влияние классификатора связей на Crosswalk-QA

■ ***Table 14.*** Effect of the link classifier on Crosswalk-QA

Конфигурация	EM	F_1	Faithfulness
C_3 с M_{base}	0,56	0,68	0,87
C_3 с M_{XGB}	0,61	0,72	0,89

■ ***Таблица 15.*** Качество ответов Crosswalk-QA для конфигурации C_2 (Bridges-M1)
■ ***Table 15.*** Crosswalk-QA response quality for configuration C_2 (Bridges-M1)

Embedding / LLM	Gemma3:27B	Llama-3.1-70B	Qwen2.5-32B
BGE-M3	**0,63** / **0,74** / **0,90**	0,61 / 0,72 / 0,88	0,59 / 0,70 / 0,87
multilingual-e5-large	0,58 / 0,69 / 0,88	0,56 / 0,67 / 0,86	0,54 / 0,65 / 0,85
LaBSE	0,55 / 0,66 / 0,86	0,53 / 0,64 / 0,84	0,51 / 0,62 / 0,83

■ ***Таблица 16.*** Качество ответов Crosswalk-QA для конфигурации C_0 (Text-RAG)
■ ***Table 16.*** Crosswalk-QA response quality for configuration C_0 (Text-RAG)

Embedding / LLM	Gemma3:27B	Llama-3.1-70B	Qwen2.5-32B
BGE-M3	**0,21** / **0,38** / **0,70**	0,20 / 0,36 / 0,68	0,18 / 0,34 / 0,67
multilingual-e5-large	0,19 / 0,35 / 0,68	0,18 / 0,33 / 0,66	0,16 / 0,31 / 0,65
LaBSE	0,17 / 0,32 / 0,66	0,16 / 0,30 / 0,64	0,14 / 0,28 / 0,62

сообществ повышает полноту при анализе слабоструктурированных отчетов о тактиках, техниках и процедурах злоумышленников. Конфигурация C_4 обеспечивает наибольшую полноту контекста и лучшие значения метрик EM и F_1 в сценариях Crosswalk-QA и TTP-QA, однако не является оптимальной по всем метрикам. Для запросов по БДУ более строгие конфигурации C_1–C_3 сохраняют более высокую точность контекста. Следовательно, в пределах исследованного набора выбор конфигурации должен определяться типом аналитической задачи: нормативные запросы требуют более компактного и точного графового контекста, а вопросы по отчетам кибербразведки выигрывают от добавления обобщающего слоя.

Ограничения исследования

Сравниваемые конфигурации различаются способом представления и доступом к структурированным знаниям: Text-RAG использует преимущественно CTI-фрагменты, тогда как графовые варианты получают БДУ и межонтологические связи. Основной эксперимент оценивает интегрированную архитектуру и не проводит детальную оценку изолированного эффекта формата представления знаний в виде графа. Текстовая конфигурация с теми же фактами не строилась.

Полная независимость основной серии из 750 вопросов от разработки графа и настройки параметров не обеспечена; полный протокол составления и проверки эталонов не восстановлен. Для смешанного набора из 2630 пар отсутствует отдельная оценка двух типов связей действующей модели.

Отдельная оценка запросов RU-RU, EN-EN, RU-EN и EN-RU не проводилась. Значения параметров запуска seed, temperature и top_p для всех исходных запусков не были полностью зафиксированы. Оценки Faithfulness не калибровались на экспертной подвыборке.

Система анализирует угрозы, тактики, техники, уязвимости, последствия и меры защиты и не выполняет полную оценку риска ИБ для конкретной информационной системы: не учитываются ценность активов, фактически установленные версии программного обеспечения, реализованные меры, вероятность реализации угрозы и остаточный риск.

Промышленная апробация с аналитиками SOC, интеграция с CMDB, SIEM, SOAR, MISP и TAXII, обработка TLP-меток и отдельная оценка устойчивости к отравлению графа или внедрению вредоносных инструкций не проводились. Результаты имеют рекомендательный характер и требуют последующей интеграции в существующие системы мониторинга ИБ.

Заключение

В работе предложена модель графа знаний BDU-KG и два алгоритма анализа данных кибербразведки: алгоритм BridgeBuild для построения межонтологических связей и алгоритм DualLoopContext для двухконтурного извлечения нормативного и доказательного контекста. Модель реализована в виде ориентированного типизированного графа свойств с атрибутами и объединяет БДУ ФСТЭК России, базы знаний

MITRE ATT & CK, MITRE D3FEND, CVE, CWE, CAPEC и CTI-отчеты.

Оценка алгоритма BridgeBuild на тестовой выборке из 394 пар показала $F_1 = 0{,}83$ для M_{MLP} и M_{XGB}. Алгоритм BridgeBuild при использовании M_{XGB} превысил лучший из рассмотренных альтернативных методов по F_1 на 0,03 и сократил число LLM-вызовов приблизительно в семь раз в тестовом протоколе.

В основной серии на 750 вопросах графовые конфигурации обеспечили наибольший выигрыш в многошаговых сценариях. В BDU-QA рост EM с 0,48 до 0,77; в Crosswalk-QA рост с 0,21 до 0,63. Автоматические межонтологические связи M_2 позволили получить значение EM = 0,56 при EM = 0,63 для экспертных межонтологических связей M_1.

Дополнительный статистический замер подтвердил устойчивое преимущество графового извлечения над алгоритмом BM25 по Entity Recall@50, в том числе после маскирования идентификаторов. Полученные выводы относятся к исследованным источникам и сценариям экспериментов и не означают универсального превосходства графового подхода.

Полное независимое преимущество графового извлечения по дополнительной серии TTP-QA не установлено из-за зависимости эталона и доступного слоя связей. Проверка качества на новых документах требует отдельного протокола, исключающего использование эталонных связей при извлечении и контролирующего пересечение документов и их дубликатов.

Практическая значимость определяется возможностью применения разработанной системы для поддержки принятия решений аналитиками SOC при разборе CTI-отчетов, сопоставлении TTP злоумышленников с угрозами БДУ, формировании рекомендаций по мерам защиты и описания инцидентов ИБ с использованием международных таксономий. Полная оценка риска ИБ, промышленная интеграция и апробация в действующем SOC остаются направлениями дальнейшей работы.

Литература

1. **Tounsi W., Rais H.** A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 2018, vol. 72, pp. 212–233. doi:10.1016/j.cose.2017.09.001
2. **Мещеряков Р. В., Исхаков С. Ю.** Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем. *Вопросы кибербезопасности*, 2022, № 5(51), с. 82–99. doi:10.21681/2311-3456-2022-5-82-99
3. **Zhang J., Bu H., Wen H., Liu Y., Fei H., Xi R., Li L., Yang Yu., Zhu H., Meng D.** When LLMs meet cybersecurity: a systematic literature review. *Cybersecurity*, 2025, vol. 8, pp. 1–55. doi:10.1186/s42400-025-00361-w
4. **Котенко И. В., Абраменко Г. Т.** Использование больших языковых моделей для поиска угроз кибербезопасности на основе методов глубокого обучения: анализ современных исследований. *Правовая информатика*, 2024, № 3, с. 32–42. doi:10.24412/1994-1404-2024-3-32-42
5. **Würsch M., Kucharavy A., Percia David D., Mermoud A.** LLM-based entity extraction is not for cybersecurity. *Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2023) and AI+ Informetrics (AII2023)*, 2023, vol. 3451, pp. 26–32.
6. **Lewis P., Perez E., Piktus A., Petroni F., Karpukhin V., Goyal N., Küttler H., Lewis M., Yih W., Rocktäschel T., Riedel S., Kiela D.** Retrieval-augmented generation for knowledge-intensive NLP tasks. *Advances in Neural Information Processing Systems*, 2020, vol. 33, pp. 9459–9474. doi:10.48550/arXiv.2005.11401
7. **Rajapaksha S., Rani R., Karafili E.** A RAG-based question-answering solution for cyber-attack investigation and attribution. *European Symposium on Research in Computer Security*, LNCS, vol. 15264, Cham, Springer Nature Switzerland, 2024, pp. 238–256. https://doi.org/10.1007/978-3-031-82362-6_15
8. **Edge D., Trinh H., Cheng N., Bradley J., Chao A., Mody A., Truitt S., Larson J.** From local to global: A graph RAG approach to query-focused summarization. *arXiv:2404.16130*, 2024. doi:10.48550/arXiv.2404.16130
9. **Луцкович А. И., Васильев В. И., Вульфин А. М., Кириллова А. Д., Сулавко А. Е.** Автоматизированная система анализа слабоструктурированных данных киберразведки с использованием больших языковых моделей. *Информационно-управляющие системы*, 2025, № 2, с. 50–67. doi:10.31799/1684-8853-2025-2-50-67, EDN: QFQTPU
10. **Hu Y., Lei Z., Zhang Z., Pan B., Ling C., Zhao L.** GRAG: Graph Retrieval-Augmented Generation. *Findings of the Association for Computational Linguistics: NAACL 2025*, 2025, pp. 4145–4157. doi:10.18653/v1/2025.findings-naacl.232
11. **Zhu X., Xie Y., Liu Y., Li Y., Hu W.** Knowledge Graph-Guided Retrieval Augmented Generation. *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2025, pp. 8912–8924. doi:10.18653/v1/2025.naacl-long.449
12. **Манжосов А. В., Болодурина И. П.** Метод автоматизированного построения графа знаний связности формальных моделей норм и требований в области информационной безопасности. *Вестник УрФО. Безопасность в информационной сфере*, 2022, № 2(44), с. 49–56. doi:10.14529/secur220207

13. **Sikos L. F.** Cybersecurity knowledge graphs. *Knowledge and Information Systems*, 2023, vol. 65, no. 9, pp. 3511–3531. doi:10.1007/s10115-023-01860-3
14. **Chepurova A., Kuratov Y., Bulatov A., Burtsev M.** Prompt me one more time: A two-step knowledge extraction pipeline with ontology-based verification. *Graph-based Methods for Natural Language Processing: Proceedings of TextGraphs-17,* 2024, pp. 61–77. doi:10.18653/v1/2024.textgraphs-1.5
15. **Fieblinger R., Alam M. T., Rastogi N.** Actionable cyber threat intelligence using knowledge graphs and large language models. *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, IEEE, 2024, pp. 100–111. doi:10.1109/EuroSPW61312.2024.00018
16. **Wu Z., Tang F., Zhao M., Li Y.** KGV: Integrating Large Language Models with knowledge graphs for cyber threat intelligence credibility assessment. *IEEE Transactions on Mobile Computing*, 2026, pp. 1–16. doi:10.1109/TMC.2026.3692451
17. **Peng B., Zhu Y., Liu Y., Bo X., Shi H., Hong C., Zhang Y., Tang S.** Graph Retrieval-Augmented Generation: A survey. *ACM Transactions on Information Systems*, 2025, vol. 44, no. 2, pp. 1–52. doi:10.1145/3777378
18. **Kurniawan K., Kiesling E., Ekelhart A.** CyKG-RAG: Towards knowledge-graph enhanced retrieval augmented generation for cybersecurity. *International Semantic Web Conference (ISWC): CEUR Workshop Proceedings*, Baltimore, USA, November 2024, vol. 3950, pp. 1–14.
19. **Rahman M. R., Hezaveh R. M., Williams L.** What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey. *ACM Computing Surveys*, 2023, vol. 55, no. 12, pp. 1–36. doi:10.1145/3571726
20. **Nour B., Pourzandi M., Qureshi R. K., Debbabi M.** Automa: Automated generation of attack hypotheses and their variants for threat hunting using knowledge discovery. *IEEE Transactions on Network and Service Management*, 2024, vol. 21, no. 5, pp. 5178–5196. doi:10.1109/TNSM.2024.3378972
21. **Huang L., Xiao X.** CTIKG: LLM-powered knowledge graph construction from cyber threat intelligence. *First Conf on Lang Modeling*, 2024, pp. 1–24.
22. **Cheng Y., Bajaber O., Tsegai S. A., Song D., Gao P.** CTINexus: Automatic cyber threat intelligence knowledge graph construction using Large Language Models. *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P)*, Venice, Italy, 30 June–04 July 2025, IEEE, 2025, pp. 923–938. doi:10.1109/EuroSP63326.2025.00057
23. **Hu Y., Zou F., Han J., Sun X., Wang Y.** LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model. *Computers & Security*, 2024, vol. 145, pp. 103999. doi:10.1016/j.cose.2024.103999
24. **Es S., James J., Espinosa-Anke L., Schockaert S.** RAGAS: Automated evaluation of Retrieval Augmented Generation. *Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics: System Demonstrations*, 2024, pp. 150–158. doi:10.18653/v1/2024.eacl-demo.16

UDC 004.056.53
doi:10.31799/1684-8853-2026-5-37-55
EDN: IULELD

A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph

A. M. Vulfin[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-5857-2413, vulfin.alexey@yandex.ru
V. I. Vasilyev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-6105-5481
A. I. Lutskovich[a], Senior Lecturer, orcid.org/0009-0000-7257-6947
A. D. Kirillova[a], PhD, Tech., Associate Professor, orcid.org/0009-0000-4164-2526
[a]Ufa University of Science and Technology, 12, K. Marx St., 450008, Ufa, Russian Federation

Introduction: Traditional retrieval-augmented generation systems based on vector search on chunks are limited in multi-step mapping of cyber threat intelligence reports, national threat classifiers, and international knowledge bases. **Purpose:** To develop and give experimental evaluation of a knowledge graph model and algorithms for cross-ontology alignment and dual-loop context extraction in the analysis of cyber threat intelligence data. **Methods:** The model is implemented as a directed, typed graph of properties with a set of attributes that integrates a national threat database, international knowledge bases on attack tactics and techniques, protective measures, vulnerability registries, software weakness classifiers, attack pattern catalogs, and a corpus of cyber threat intelligence reports. The achievement of the goal is assessed by quantitative metrics when constructing cross-ontological connections and analyzing the capabilities of the question-answer system. **Results:** We develop an algorithm for constructing cross-ontological links with verification of semantic similarity, domain constraints, and alignment with correctness control using large language models. We implement a dual-loop context extraction algorithm that combines a knowledge graph and an evidential layer of text fragments. We propose a method for analyzing cyber threat intelligence data based on a knowledge graph model, algorithms for constructing cross-ontological links and context extraction. On the test set, the trained classifier of cross-ontological relationships has achieved the metric value F1 = 0.83. The introduced expert connections have increased the value of the EM metric of complete coincidence of the predicted and reference set of identifiers from 0.34 to 0.63, automatic connections have ensured the value of the EM = 0.56. A significant increase in the Entity Recall@50 metric has been obtained relative to text search: 0.5225, and after hiding the identifiers of tactics and techniques, the increase equals 0.5467. **Practical relevance:** The method is designed to support decision-making by analysts at the Information Security Operations Center when comparing cyber threat intelligence reports with national and international knowledge bases. **Discussion:** Cross-ontological links improve the verifiability of the answer by aligning with correctness control, and the layer of summary descriptions of the graph communities increases the consistency of the answer with the extracted context with a moderate decrease in accuracy.

Keywords – knowledge graph, graph retrieval-augmented generation, cyber threat intelligence data, tactics and techniques, ontology matching, entity alignment, large language models, MITRE ATT & CK, MITRE D3FEND, BDTV FSTEC.

For citation: Vulfin A. M., Vasilyev V. I., Lutskovich A. I., Kirillova A. D. A model and algorithms for cyber threat intelligence data analysis based on a knowledge graph. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 37–55 (In Russian). doi:10.31799/1684-8853-2026-5-37-55, EDN: IULELD

References

1. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 2018, vol. 72, pp. 212–233. doi:10.1016/j.cose.2017.09.001
2. Meshcheryakov R. V., Iskhakov S. U. Study of compromet-ation indicators for improvement of information and cyber-physical systems protection facilities. *Cybersecurity Issues*. 2022, no. 5(51), pp. 82–99 (In Russian). doi:10.21681/2311-3456-2022-5-82-99
3. Zhang J., Bu H., Wen H., Liu Y., Fei H., Xi R., Li L., Yang Yu., Zhu H., Meng D. When LLMs meet cybersecurity: A systematic literature review. *Cybersecurity*, 2025, vol. 8, pp. 1–55. doi:10.1186/s42400-025-00361-w
4. Kotenko I. V., Abramenko G. T. Using large language models for cyber threat hunting based on deep learning methods: Analysis of modern research. *Legal Informatics*, 2024, no. 3, pp. 32–42 (In Russian). doi:10.24412/1994-1404-2024-3-32-42
5. Würsch M., Kucharavy A., Percia David D., Mermoud A. LLM-based entity extraction is not for cybersecurity. *Extraction and Evaluation of Knowledge Entities from Scientific Documents (EEKE2023) and AI+ Informetrics (AII2023)*, 2023, vol. 3451, pp. 26–32.
6. Lewis P., Perez E., Piktus A., Petroni F., Karpukhin V., Goyal N., Küttler H., Lewis M., Yih W., Rocktäschel T., Riedel S., Kiela D. Retrieval-augmented generation for knowledge-intensive NLP tasks. *Advances in Neural Information Processing Systems*, 2020, vol. 33, pp. 9459–9474. doi:10.48550/arXiv.2005.11401
7. Rajapaksha S., Rani R., Karafili E. A RAG-based question-answering solution for cyber-attack investigation and attribution. *European Symposium on Research in Computer Security*, LNCS, vol. 15264, Cham, Springer Nature Switzerland, 2024, pp. 238–256. https://doi.org/10.1007/978-3-031-82362-6_15
8. Edge D., Trinh H., Cheng N., Bradley J., Chao A., Mody A., Truitt S., Larson J. From local to global: A graph RAG approach to query-focused summarization. *arXiv:2404.16130*, 2024. doi:10.48550/arXiv.2404.16130
9. Lutskovich A. I., Vasiluev V. I.., Vulfin A. M., Kirillova A. D., Sulavko A. E. Automated system for analyzing weakly structured threat intelligence data using large language models. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2025, no. 2, pp. 50–67 (In Russian). doi:10.31799/1684-8853-2025-2-50-67, EDN: QFQTPU
10. Hu Y., Lei Z., Zhang Z., Pan B., Ling C., Zhao L. GRAG: Graph Retrieval-Augmented Generation. *Findings of the Association for Computational Linguistics: NAACL 2025*, 2025, pp. 4145–4157. doi:10.18653/v1/2025.findings-naacl.232
11. Zhu X., Xie Y., Liu Y., Li Y., Hu W. Knowledge Graph-Guided Retrieval Augmented Generation. *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2025, pp. 8912–8924. doi:10.18653/v1/2025.naacl-long.449
12. Manzhosov A. V., Bolodurina I. P. Automated construction of the knowledge graph of reference to formal models of norms and treatments in the field of information security method. *Journal of the Ural Federal District. Information Security*, 2022, no. 2(44), pp. 49–56 (In Russian). doi:10.14529/secur220207
13. Sikos L. F. Cybersecurity knowledge graphs. *Knowledge and Information Systems*, 2023, vol. 65, no. 9, pp. 3511–3531. doi:10.1007/s10115-023-01860-3
14. Chepurova A., Kuratov Y., Bulatov A., Burtsev M. Prompt me one more time: A two-step knowledge extraction pipeline with ontology-based verification. *Graph-based Methods for Natural Language Processing: Proceedings of TextGraphs-17,* 2024, pp. 61–77. doi:10.18653/v1/2024.textgraphs-1.5
15. Fieblinger R., Alam M. T., Rastogi N. Actionable cyber threat intelligence using knowledge graphs and large language models. *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Vienna, Austria, IEEE, 2024, pp. 100–111. doi:10.1109/EuroSPW61312.2024.00018
16. Wu Z., Tang F., Zhao M., Li Y. KGV: Integrating Large Language Models with knowledge graphs for cyber threat intelligence credibility assessment. *IEEE Transactions on Mobile Computing*, 2026, pp. 1–16. doi:10.1109/TMC.2026.3692451
17. Peng B., Zhu Y., Liu Y., Bo X., Shi H., Hong C., Zhang Y., Tang S. Graph Retrieval-Augmented Generation: A survey. *ACM Transactions on Information Systems*, 2025, vol. 44, no. 2, pp. 1–52. doi:10.1145/3777378
18. Kurniawan K., Kiesling E., Ekelhart A. CyKG-RAG: Towards knowledge-graph enhanced retrieval augmented generation for cybersecurity. *International Semantic Web Conference (ISWC): CEUR Workshop Proceedings*, Baltimore, USA, November 2024, vol. 3950, pp. 1–14.
19. Rahman M. R., Hezaveh R. M., Williams L. What are the attackers doing now? Automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey. *ACM Computing Surveys*, 2023, vol. 55, no. 12, pp. 1–36. doi:10.1145/3571726
20. Nour B., Pourzandi M., Qureshi R. K., Debbabi M. Automa: Automated generation of attack hypotheses and their variants for threat hunting using knowledge discovery. *IEEE Transactions on Network and Service Management*, 2024, vol. 21, no. 5, pp. 5178–5196. doi:10.1109/TNSM.2024.3378972
21. Huang L., Xiao X. CTIKG: LLM-powered knowledge graph construction from cyber threat intelligence. *First Conf on Lang Modeling*, 2024, pp. 1–24.
22. Cheng Y., Bajaber O., Tsegai S. A., Song D., Gao P. CTINexus: Automatic cyber threat intelligence knowledge graph construction using Large Language Models. *2025 IEEE 10th European Symposium on Security and Privacy (EuroS&P)*, Venice, Italy, 2025, IEEE, 2025, pp. 923–938. doi:10.1109/EuroSP63326.2025.00057
23. Hu Y., Zou F., Han J., Sun X., Wang Y. LLM-TIKG: Threat intelligence knowledge graph construction utilizing large language model. *Computers & Security*, 2024, vol. 145, pp. 103999. doi:10.1016/j.cose.2024.103999
24. Es S., James J., Espinosa-Anke L., Schockaert S. RAGAS: Automated evaluation of Retrieval Augmented Generation. *Proceedings of the 18th Conference of the European Chapter of the Association for Computational Linguistics: System Demonstrations*, 2024, pp. 150–158. doi:10.18653/v1/2024.eacl-demo.16

УДК 621.376.9
doi:10.31799/1684-8853-2026-5-56-72
EDN: CMAJJN

Научные статьи
Articles

Способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности

С. В. Штанько[а], *доктор техн. наук, доцент, orcid.org/0000-0002-8391-8911, vka@mil.ru*
В. А. Крягин[а], *преподаватель, orcid.org/0009-0002-7529-283X*
П. Н. Топчий[а], *преподаватель, orcid.org/0009-0008-4678-7685*
Д. А. Аникин[б], *начальник отдела, orcid.org/0009-0003-8295-312X*
[а]*Военно-космическая академия им. А. Ф. Можайского, Ждановская наб., 13, Санкт-Петербург, 197198, РФ*
[б]*Министерство обороны Российской Федерации, Знаменка ул., 19, Москва, 119160, РФ*

Введение: *радиостеганографические методы, основанные на встраивании стегосигнала в открытый сигнал-контейнер на физическом уровне, позволяют решить задачу обеспечения конфиденциальности информации и, в отличие от криптографических методов, скрыть сам факт передачи информации по радиоканалу, однако требуют обеспечения энергетической скрытности стегосигнала и стойкости к попыткам его обнаружения злоумышленником.* ***Цель:*** *разработать способ энергетического маскирования радиосигнала внутри сигнала-контейнера на основе дополнительной фазовой манипуляции и нелинейной расширяющей псевдослучайной последовательности, обеспечивающего скрытую передачу информации по стегоканалу с заданной помехоустойчивостью для легального абонента и невозможность обнаружения стегосигнала злоумышленником.* ***Результаты:*** *предложен способ формирования стегосигнала путем дополнительной фазовой манипуляции малым углом вектора фазоманипулированного сигнала-контейнера. Угол отклонения выбирался из условия маскировки энергии одного чипа в пределах дисперсии фазового шума. Расширение спектра стегосигнала выполнялось нелинейной псевдослучайной последовательностью, формируемой генератором нелинейной псевдослучайной последовательности, стойкой к анализу. Получены аналитические соотношения для вероятности правильного обнаружения и вероятности битовой ошибки. Показано, что при длине расширяющей последовательности 16 383 элемента легальный абонент достигал вероятности правильного обнаружения 0,9972 при отношении энергии чипа к спектральной плотности шума $q = -33$ дБ, тогда как злоумышленник при поэлементном приеме не может обнаружить стегосигнал при $q < 0$ дБ. Вероятность битовой ошибки менее 10^{-8} достигалась при $q = -30$ дБ, а злоумышленнику требовалось более 12 дБ — разница составила 42 дБ. Разработан стенд полунатурного моделирования на базе программно-определяемых радиоустройств; отклонение экспериментальных данных от расчетных не превысило пяти процентов.* ***Практическая значимость:*** *способ применим к широкому классу цифровых радиосистем с фазовой манипуляцией и может использоваться для передачи данных по встроенному каналу в системах критической информационной инфраструктуры.*

Ключевые слова *— фазовая манипуляция, псевдослучайная последовательность, фазовая диаграмма, сигнал-контейнер, расширяющая последовательность, корреляционный прием, стегосигнал, стегосообщение, нелинейная расширяющая последовательность.*

Для цитирования: Штанько С. В., Крягин В. А., Топчий П. Н., Аникин Д. А. Способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности. *Информационно-управляющие системы*, 2026, № 5, с. 56–72. doi:10.31799/1684-8853-2026-5-56-72, EDN: CMAJJN
For citation: Shtanko S. V., Kryagin V. A., Topchiy P. N., Anikin D. A. A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 56–72 (In Russian). doi:10.31799/1684-8853-2026-5-56-72, EDN: CMAJJN

Введение

В современных условиях развитие глобальных систем связи и передачи данных приводит к непрерывному возрастанию требований к безопасности информации, циркулирующей в таких системах, в частности, ее составляющей — конфиденциальности. Особенно актуально это для объектов критической информационной инфраструктуры [1], под которыми понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы специального назначения, предназначенные для управления субъектами критической информационной инфраструктуры (МВД, МЧС, здравоохранения, транспортной инфраструктуры и т. д.). В более значительной степени подвержены угрозам нарушения конфиденциальности системы, элементы которых объединены радиоканалами, ввиду их пространственной доступности [2].

Основу системы обеспечения конфиденциальности информации в указанных системах, как правило, составляют криптографические методы. Их применение реализует ограничение (предотвращение) доступа к семантике передаваемых

данных для всех, кроме пользователей, обладающих некоторыми закрытыми параметрами — ключами. Результаты анализа потоков данных (трафика), включая интенсивность, объем и динамику передачи сообщений, сами по себе могут быть источником информации для злоумышленника, даже без получения доступа к смыслу передаваемых данных. Поэтому для некоторых задач желательным является не только сокрытие смысла передаваемой информации, но и самого факта ее передачи. Для решения задач скрытой передачи данных по встроенному каналу используются стеганографические методы, позволяющие встраивать некоторую дополнительную информацию (стегосообщение) в открытую информацию (контейнер). Такие методы реализуются на уровне обработки информации и не зависят от носителя (канала передачи) информации. Например, широко известен подход, связанный с внедрением скрытой информации в двоичные файлы (изображения, видео). При этом без знания ключевой информации злоумышленник не может не только получить доступ к смыслу встроенной информации, но и установить сам факт ее наличия [3].

Аналогичный подход может быть применен и на физическом уровне. В этом случае уже элементы сигнала, являющегося носителем дополнительной информации, встраиваются в сигнал — носитель основной информации. Радиостеганографические методы основаны на встраивании стегосигнала в сигнал-контейнер (открытый носитель). В этом случае под сокрытием передачи информации следует понимать не только невозможность ее обнаружения при перехвате и получения доступа к ее смыслу, но и сокрытие самого факта передачи по каналу радиосвязи какой-либо информации помимо той, которая содержится в сигнале-контейнере. Поскольку такие методы реализуются фактически на физическом уровне, это значительно затрудняет потенциальному злоумышленнику не только задачу анализа добытых данных, в том числе на предмет содержания в контейнере встроенной информации, но и регистрацию и прием сигнала-носителя такой информации (стегосигнала).

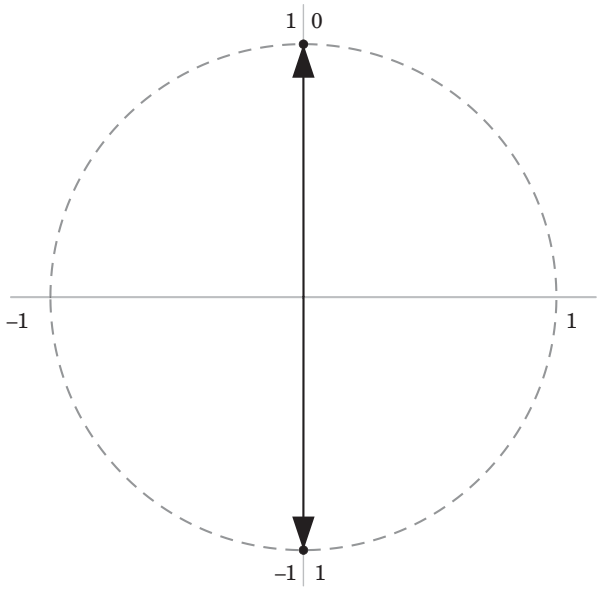
В статье предлагается способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности, позволяющий осуществлять прием стегосигнала с требуемой помехоустойчивостью легальному абоненту с одной стороны и значительно ограничивающий возможности злоумышленника по обнаружению и приему стегосигнала с другой. Ряд частных результатов, положенных в основу настоящей работы, докладывался авторами ранее применительно к смежным задачам — передаче информации по космическим радиолиниям [4] и защите навигационных сигналов от имитационных воздействий [5]. В настоящей статье они впервые объединены в рамках единого способа формирования радиостеганографического сигнала, что и составляет ее основной научный результат.

Описание способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности

В основе предлагаемого способа лежит использование дополнительной фазовой манипуляции малым углом в структуре существующего радиосигнала-контейнера. На первом этапе для упрощения понимания в качестве сигнала-контейнера рассмотрим бинарный (двухпозиционный) фазоманипулированный сигнал ФМ-2 с 0 – π манипуляцией (рис. 1), описываемый аналитическим выражением

$$S_{\text{ФМ2}}(t) = AG(t)\cos(\omega_0 t), \qquad (1)$$

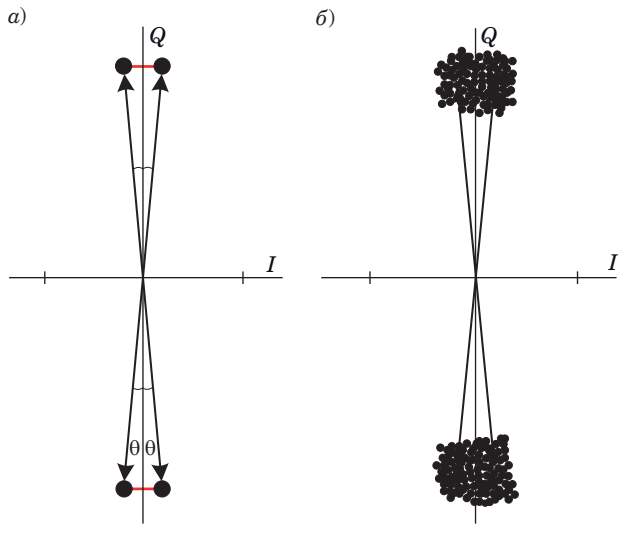
где A — амплитуда сигнала; $G(t)$ — бинарная расширяющая псевдослучайная последовательность (ПСП), модулированная информационной последовательностью, принимающая значения ±1 и обеспечивающая инверсию фазы несущей (0 – π манипуляция); ω_0 — несущая частота.



■ ***Рис. 1.*** Фазовая диаграмма сигнала ФМ-2
■ ***Fig. 1.*** Phase diagram of the FM-2 signal

Опишем способ внедрения (маскирования) двоичного стегосигнала в сигнал-контейнер (1). Чтобы внедрить данные, необходимо дополнительно изменять (модулировать) параметры сигнала-контейнера, но делать это необходимо так, чтобы посторонний наблюдатель не мог зарегистрировать эти изменения (принять стегосигнал). Внедрение происходит путем формирования дополнительной фазовой составляющей на основе сигнала-контейнера (1). С этой целью будем отклонять вектор, описывающий сигнал-контейнер в каждом из возможных положений, на дополнительный угол $\pm\theta$ (рис. 2, *а*) так, чтобы значение модуля вектора разности не превышало величину, соответствующую дисперсии шумов. Угол θ определим следующим образом: $\theta = \theta_0 \cdot L_{ст}(t) \cdot B(t)$, где $L_{ст}(t)$ — бит встраиваемого сообщения; $B(t)$ — бинарная ПСП, принимающая значения ± 1. Вектор сигнала-контейнера при его отклонении на дополнительный угол модуляции θ должен находиться в пределах зоны неопределенности, ограниченной дисперсией фазового шума (рис. 2, *б*).

Очевидно, что в этом случае посимвольное обнаружение и прием будут невозможны ввиду малой энергии стегосигнала. Однако, если модулировать стегосигнал расширяющей последовательностью и осуществлять корреляционный прием с накоплением символов расширяющей ПСП, используя достаточно большой период накопления, можно добиться требуемого отношения сигнал/шум для стегосигнала. Платой за это будет относительно низкая скорость передачи данных.

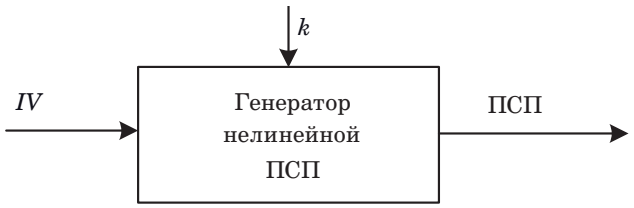


■ ***Рис. 2.*** Фазовая диаграмма сигнала-контейнера с дополнительной модуляцией, формирующей стегосигнал при отсутствии (*а*) и наличии (*б*) шума

■ ***Fig. 2.*** Constellation diagram of the cover signal with additional modulation forming the stego signal in the absence (*а*) and in the presence (*б*) of noise

В этом случае вектор разности, полученный в результате отклонения на угол $+\theta$, соответствует чипу расширяющей ПСП стегосигнала «1», $-\theta$ — «0». Другими словами, знак отклонения на дополнительный угол определяется произведением информационного бита $L_{ст}(t)$ и символа расширяющей ПСП $B(t)$. При корреляционном приеме с известной последовательностью $B(t)$ легальный абонент восстанавливает биты $L_{ст}(t)$ путем накопления энергии за период ПСП. Расчеты, подтвержденные экспериментом, показывают, что существует возможность выбора такого диапазона значений параметров сигнала-контейнера и стегосигнала (длительность символа сигнала-контейнера; угол θ, определяющий энергию стегосигнала; период накопления; количество чипов расширяющей ПСП в информационном символе стегосигнала и т. д.), при котором энергии информационного символа, накопленного легальным абонентом сигнала при условии знания им расширяющей ПСП стегосигнала, достаточно для его качественного (с заданной помехоустойчивостью) обнаружения и корреляционного приема. В то же время в условиях отсутствия сведений о структуре расширяющей ПСП у потенциального злоумышленника накопление и выделение им энергии информационного символа невозможно, а энергии одного чипа расширяющей ПСП недостаточно для его выделения и почипового обнаружения и приема.

Для того чтобы вероятный злоумышленник не имел возможности подобрать структуру расширяющей ПСП стегосигнала, в качестве таковой следует использовать нелинейную последовательность, отличающуюся высокой структурной скрытностью (формируемую с использованием специальных нелинейных функций) [6]. При этом необходимо учитывать, что такая последовательность должна иметь хорошие корреляционные свойства, позволяющие реализовывать корреляционный прием и обработку такого сигнала с требуемой помехоустойчивостью [7, 8]. Известно, что качественные криптографические алгоритмы обладают корреляционными свойствами, близкими к корреляционным свойствам истинно случайной последовательности при условии достаточно большого периода накопления [9, 10]. В этом смысле их использование позволит осуществлять корреляционный прием с требуемым качеством при условии выполнения достаточно жестких требований к вопросам синхронизации в процессе выделения стегоканала из канала-контейнера, однако эта задача может быть успешно решена с помощью самого сигнала-контейнера. Выполненные оценки показывают, что для последовательностей указанного типа при достаточно большом периоде накопления (16 000 элементов) максимальный уровень боковых лепестков автокорреляционной функции не превышает –28 дБ



IV – параметр начального состояния генератора

■ ***Рис. 3.*** Способ формирования нелинейной ПСП

■ ***Fig. 3.*** Nonlinear pseudorandom sequence generation method

относительно главного максимума, а уровень взаимно-корреляционной функции не превышает –27 дБ, что не хуже соответствующих показателей линейных ПСП той же длины и не приводит к снижению помехоустойчивости корреляционного приема.

В качестве расширяющей можно использовать, например, нелинейную ПСП, получаемую с помощью генератора ПСП, работающего на основе криптографического алгоритма «Кузнечик» [6]. Для этого источник и получатель должны обладать общим закрытым параметром, являющимся аналогом ключа k (рис. 3), на основе которого они смогут формировать идентичную нелинейную ПСП, используемую для расширения спектра сигнала и корреляционного приема соответственно.

Последовательность вырабатывается в режиме гаммирования с обратной связью по выходу: вектор начального состояния IV зашифровывается на ключе k, результат каждой итерации подается на вход следующей, а искомая последовательность образуется конкатенацией полученных блоков:

$$Y_1 = E(IV, k),\ Y_i = E(Y_{i-1}, k),\ B = Y_1 \| Y_2 \| \ldots \| Y_n,$$

где IV — вектор начального состояния (128 бит); k — ключ (256 бит); $E(\cdot)$ — функция зашифрования 128-битного блока.

Стороны, обладающие общими k и IV, при наличии синхронизации формируют идентичную апериодическую последовательность требуемой длины. Предложенный способ сохраняет работоспособность при использовании любого алгоритма с требуемой стойкостью и скоростью выработки.

Вычислительная сложность формирования такой ПСП невелика. Требуемая скорость ее выработки определяется чиповой скоростью сигнала-носителя и для широкополосных радиосистем составляет единицы-десятки мегабит в секунду, что на два-три порядка ниже производительности известных программных и аппаратных реализаций алгоритма «Кузнечик» и обеспечивает формирование ПСП в реальном времени со значительным запасом.

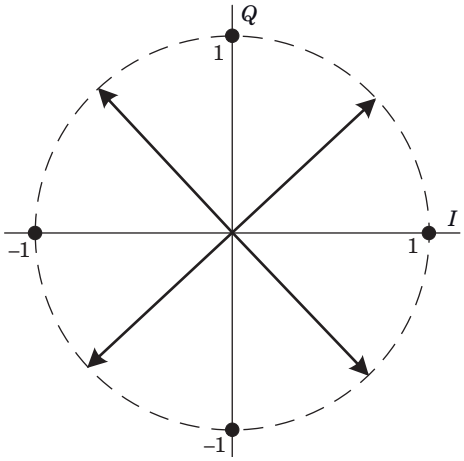
Следует отметить, что реализация описанного подхода в значительной степени затруднена сложностью поиска и обнаружения стегосигнала, поскольку элементарный чип последовательности обладает очень низкой энергией. Однако при предъявлении достаточно высоких требований к синхронизации сигнала-контейнера и стегосигнала и их когерентной обработке данная проблема успешно может быть решена, поскольку синхронизация будет осуществляться при помощи сигнала-носителя, а поиск стегосигнала будет выполняться по элементам структуры сигнала-носителя (например, по специальным синхропосылкам). В этом смысле удобным представляется использование в качестве сигнала-носителя сигнала цифровой широкополосной радиосистемы, реализующей высокую степень синхронизации и использующей радиосигнал с квадратурным уплотнением. Такой сигнал можно рассматривать как четырехуровневый фазоманипулированный радиосигнал ФМ-4 [11–13]. В этом случае доплеровский сдвиг и многолучевое распространение отрабатываются штатными средствами системы-носителя. Доплеровская расстройка устраняется слежением за несущей сигнала-контейнера, а многолучевость разрешается корреляционной обработкой широкополосного сигнала-контейнера, поскольку при разности хода лучей, превышающей длительность чипа, побочные лучи разделяются и не искажают основной корреляционный пик. Синхронизация стегоканала выполняется не по слабому стегосигналу, а по сигналу-контейнеру, поэтому малый угол дополнительной фазовой модуляции ее не усложняет. В реализованном макете тактовая синхронизация стегоканала осуществлялась по периодической метке, представляющей собой заранее заданную короткую двоичную последовательность, передаваемую в канале-контейнере.

Рассмотрим для примера в качестве сигнала-контейнера (носителя) радиосигнал цифровой широкополосной радиосистемы с квадратурным уплотнением. Пусть сигнал представляет собой фазоманипулированный радиосигнал ФМ-4. Аналитическая запись такого радиосигнала с квадратурным уплотнением имеет вид

$$S_{\text{кон}}(t) = AG_I(t)\cos(\omega_0 t) - AG_Q(t)\sin(\omega_0 t), \quad (2)$$

где A — амплитуда квадратурных компонент радиосигнала; $G_{I,Q}$ — модулирующие последовательности соответствующих квадратурных составляющих, принимающие значения ±1; ω_0 — круговая несущая частота.

Сигнальное созвездие для всех возможных комбинаций значений G_I и G_Q представлено на рис. 4.



■ ***Рис. 4.*** Фазовая диаграмма сигнала-контейнера ФМ-4
■ ***Fig. 4.*** Phase diagram of the FM-4 signal container

Маскированный сигнал (стегосигнал) формируется следующим образом. Каждый символ встраиваемого сообщения $L_{ст}(t)$ модулирует по фазе расширяющую последовательность стегосообщения – нелинейную ПСП с высокой структурной скрытностью $B(t)$, формируемую с помощью ключа k генератором нелинейной ПСП, $S_{ст}(t) = L_{ст}(t) \otimes B(t)$. В данном случае при формировании стегосигнала так же, как и при формировании сигнала-контейнера, используется метод прямого расширения спектра сигнала с помощью нелинейной ПСП, при этом принято ограничение: длительность символа расширяющей последовательности стегосигнала должна быть кратной длительности передаваемого символа расширяющей последовательности сигнала-контейнера.

Для того чтобы изменения фазы, соответствующие символам расширяющей последовательности стегосигнала $S_{ст}(t)$, были неразличимы на уровне шумов [14], угол θ выбирается из условия маскировки энергии одного чипа стегосигнала в фазовом шуме: $\theta_0^2 \le \sigma_\varphi^2$. При этом каждый информационный бит соответствует N чипам расширяющей ПСП, и только накопленная за период расширения энергия, пропорциональная $N\theta_0^2$, обеспечивает требуемое отношение сигнал/шум при корреляционном приеме. Другими словами, выбор больших значений базы стегосигнала позволяет обеспечить заданную помехоустойчивость, однако платой за это является снижение скорости передачи информации в стегоканале.

Рассмотрим полную аналитическую модель совмещенного сигнала $S_{сов}(t)$, содержащего стегосигнал $S_{ст}(t)$ в сигнале-контейнере $S_{кон}(t)$. Совмещенный сигнал образуется дополнительной фазовой модуляцией сигнала-контейнера стегосигналом:

$$S_{сов}(t) = \\ = AG_I(t)\cos[\omega_0 t + \theta(t)] - AG_Q(t)\sin[\omega_0 t + \theta(t)]. \quad (3)$$

Эквивалентная запись совмещенного сигнала в комплексной форме имеет вид

$$\tilde{S}_{сов}(t) = \tilde{S}_{кон}(t)e^{j\theta(t)}; \quad (4)$$

$$S_{сов}(t) = \Re\left\{\tilde{S}_{кон}(t)e^{j\theta(t)}\right\}; \quad (5)$$

$$\tilde{S}_{кон}(t) = A[G_I(t) + jG_Q(t)]e^{j\omega_0 t}. \quad (6)$$

Выражение (3) для малых углов $\theta(t) << 1$ можно представить в виде приближенного выражения, полученного разложением в ряд Тейлора:

$$S_{сов}(t) \approx S_{кон}(t)\cos[\theta(t)] + S^{\perp}_{кон}(t)\sin[\theta(t)]. \quad (7)$$

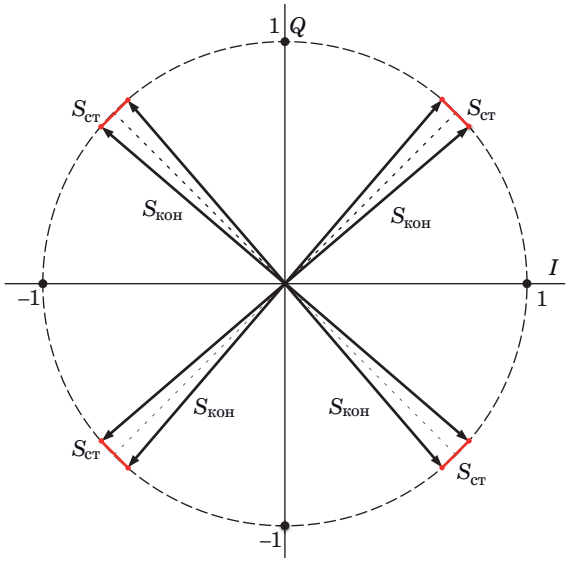
При $\cos\theta \approx 1$, $\sin\theta \approx \theta$

$$S_{кон}(t) = AG_I(t)\cos\omega_0 t - AG_Q(t)\sin\omega_0 t; \quad (8)$$

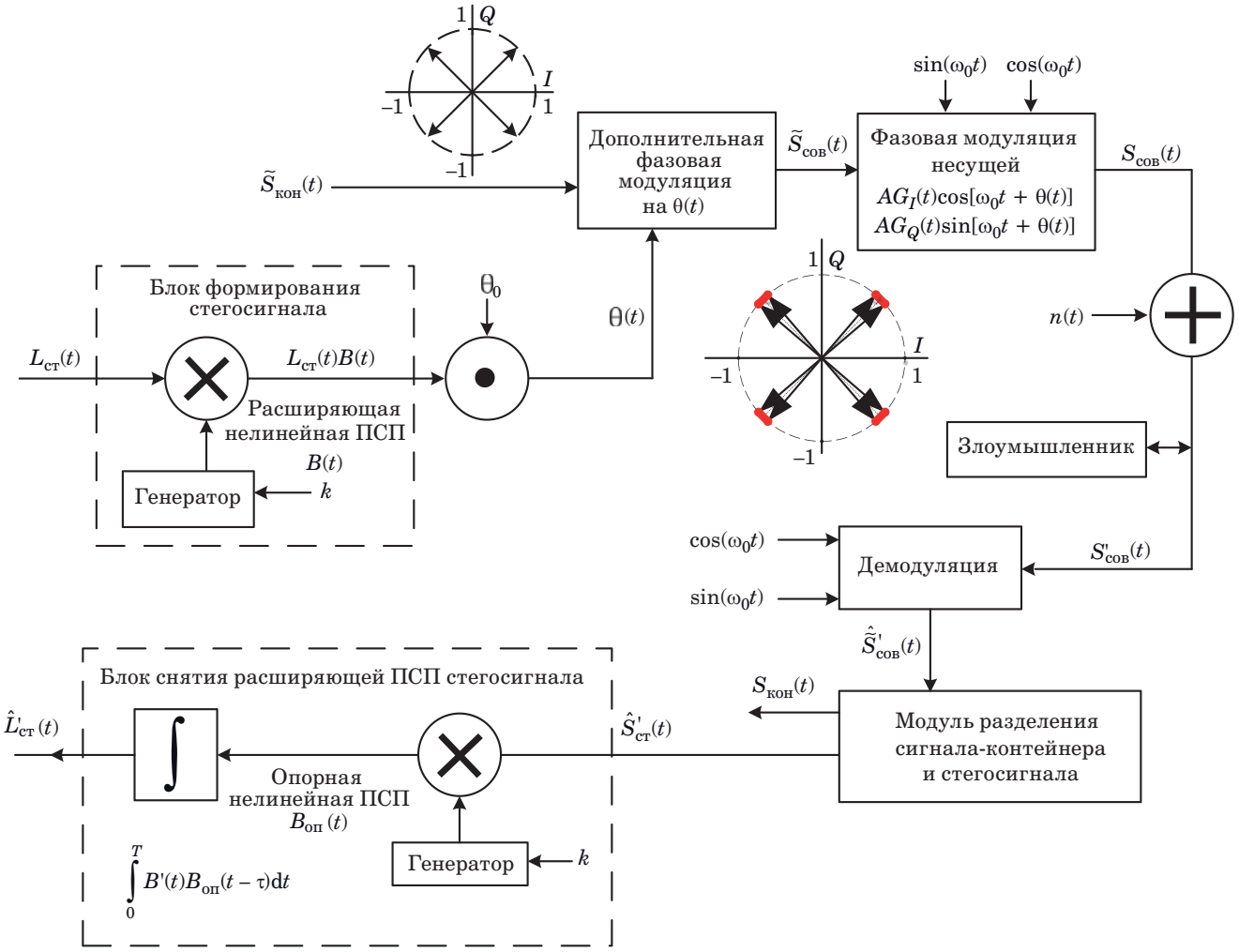
$$S_{сов}(t) \approx S_{кон}(t) + \theta(t) \cdot S^{\perp}_{кон}(t), \quad (9)$$

где $S^{\perp}_{кон}(t) = AG_Q(t)\cos\omega_0 t + AG_I(t)\sin\omega_0 t$ – сигнал, ортогональный сигналу-контейнеру в комплексной плоскости (I, Q), определяющий направление поворота созвездия.

Поясним физический смысл приведенных соотношений. Дополнительная фазовая манипуляция $\theta(t)$ поворачивает комплексный вектор сигнала-контейнера в каждой позиции созвездия (определяемой комбинацией $G_I(t)$, $G_Q(t)$) на угол $\pm\theta(t)$ по закону чипов расширяющей последовательности стегосигнала. Величина θ_0 выбирается из условия энергетической маскировки. Фазовая диаграмма совмещенного сигнала представлена на рис. 5.



■ ***Рис. 5.*** Фазовая диаграмма совмещенного сигнала
■ ***Fig. 5.*** Phase diagram of the combined signal



■ ***Рис. 6.*** Модель процесса формирования, передачи и приема совмещенного сигнала
■ ***Fig. 6.*** Model of combined signal generation, transmission, and reception process

Затем полученный совмещенный сигнал моделирует высокочастотный сигнал и передается абоненту-получателю. Модель процесса формирования, передачи и приема совмещенного сигнала (стегосигнала и сигнала-контейнера) представлена на рис. 6.

При приеме совмещенного комплексного радиосигнала $S'_{сов}(t)$ в смеси с шумом $n(t)$ абонент-получатель производит его демодуляцию и выделение стегосигнала из совмещенного. Для этого после демодуляции абонент-получатель осуществляет разделение сигнала-контейнера и стегосигнала. С этой целью на основе принятой комплексной огибающей $\hat{\tilde{S}}'_{сов}(t)$ формируется оценка сигнала-контейнера $\tilde{S}'_{кон}(t)$ путем принятия решений по символам расширяющей последовательности контейнера. Стегосигнал выделяется как разность принятого совмещенного сигнала и оценки контейнера:

$$\hat{S}'_{ст} = \hat{\tilde{S}}'_{сов} - \hat{S}'_{кон},$$

что соответствует выделению ортогональной составляющей $\theta(t)\cdot S^{\perp}_{кон}(t)$ в соответствии с приближенным выражением (9). Полученный таким образом сигнал $\hat{S}'_{ст}(t)$ поступает на блок снятия расширяющей ПСП стегосигнала.

Для осуществления корреляционной обработки полученной реализации стегосигнала абонент-получатель, зная ключ алгоритма формирования k, формирует опорный сигнал, соответствующий нелинейной расширяющей последовательности $B_{оп}(t)$:

$$R(\tau) = \int_0^T B'(t)\,B_{оп}(t-\tau)\,dt, \qquad (10)$$

где $B_{оп}(t)$ — опорная нелинейная ПСП; T — интервал корреляции (накопления).

Сформировать опорную нелинейную ПСП и осуществить корреляционный прием, а также сформировать стегосигнал с использованием расширяющей ПСП $B_{оп}(t)$ может только абонент, обладающий ключом k.

Оценка сложности реализации воздействий злоумышленником при применении способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП

Особенностью предлагаемого подхода является тот факт, что при его реализации для возможного злоумышленника сложной задачей является не только получение доступа к смыслу передаваемой в стегосигнале информации, но и установление самого факта наличия дополнительного канала передачи данных.

Рассмотрим действия злоумышленника при попытке получить доступ к дополнительному каналу при условии, что он знает (или обоснованно предполагает), что такой канал существует. В этом случае для него возможны две стратегии:

— злоумышленник пытается установить закон формирования расширяющей ПСП дополнительного канала, чтобы осуществить накопление необходимого количества чипов ПСП и реализовать корреляционный прием;

— злоумышленник пытается выделить отдельные чипы расширяющей ПСП и осуществить посимвольный прием (в том числе в режиме постобработки).

Стойкость описанного способа к первой стратегии злоумышленника полностью определяется стойкостью специального алгоритма, используемого для формирования нелинейной расширяющей ПСП, и не является предметом данной статьи, однако отметим, что в этих целях может использоваться любой криптографический алгоритм, обладающий необходимой устойчивостью к анализу и скоростью формирования.

Стойкость способа ко второй стратегии определяется энергетическими характеристиками стегосигнала и сигнала-контейнера. Покажем, что существует возможность выбора таких энергетических параметров, которые, с одной стороны, позволяют осуществлять корреляционный прием легальному абоненту при условии наличия у него знаний о законе формирования расширяющей ПСП, а с другой стороны, лишают злоумышленника возможности посимвольной обработки даже при наличии у него гипотетических элементов антенны и приемного тракта с наилучшими для него характеристиками.

Рассмотрим пример, иллюстрирующий выбор параметров стегосигнала, при которых возможности злоумышленника обнаружить и принять его, в том числе с использованием узконаправленных антенн с большим коэффициентом усиления, ограничены. Пусть длительность символа передаваемой информации в стегосигнале $\tau_с = 0{,}016$ с. Выберем мощность стегосигнала так, чтобы пик корреляционной функции на приемной стороне был достаточен для его обнаружения, а спектральная плотность мощности сигнала при этом оставалась существенно ниже уровня шума [5]. В этом случае злоумышленник, не располагающий структурой расширяющей последовательности, прием осуществить не сможет. Тогда накопление на интервале корреляционной обработки, равном длительности символа стегосигнала, эквивалентно сужению полосы до $\Delta f = 62{,}5$ Гц [5].

Оценим фоновый шум на входе приемника для наихудшего случая, включая тепловой шум антенны, потери в тракте, шум усилителя. Эквивалентную шумовую температуру антенны зададим $T_а^{ш} = 290$ К. Мощность шума составляет

$$P_а^{ш} = k\Delta f T_а^{ш}, \qquad (11)$$

где $k = 1{,}38 \cdot 10^{-23}$ Дж/К — постоянная Больцмана.

Подстановка указанных значений дает $P_а^{ш} \approx$ $\approx$ –186 дБВт. Пусть до приемника доходит около –161 дБВт мощности стегосигнала, тогда отношение сигнал/шум 25 дБ обеспечивает корреляционный прием [4]. Злоумышленнику, которому известна лишь длительность символа, но не структура последовательности, приходится регистрировать смесь сигнала с шумом в полосе, обратной длительности чипа $\tau_ч$. Если на один информационный символ (период накопления) отводится 8191 чип расширяющей ПСП, эта полоса возрастает до $\Delta F_{нар} = 1/\tau_ч = L/\tau_с \approx 0{,}5$ МГц. Даже для гипотетической антенны с $T_а^{ш} = 150$ К мощность шума в ней составит –149 дБВт — на 12 дБ выше мощности сигнала, что практически исключает почиповый прием стегосигнала [4].

Оценим вероятность правильного приема при осуществлении обнаружения стегосигнала легальным абонентом, знающим структуру расширяющей ПСП, и злоумышленником, не обладающим этим знанием. Будем полагать вероятность ложной тревоги $P_{л.т} = 0{,}1$ [5]. Вероятность правильного обнаружения при когерентном приеме в простейшем случае определяется соотношением [15, 16]

$$P_{п.о} = \Phi\left(\sqrt{2q} - \Phi^{-1}\left(1 - P_{л.т}\right)\right), \qquad (12)$$

где $\Phi(x) = \dfrac{2}{\sqrt{2\pi}}\int_0^x e^{-\frac{t^2}{2}}\,dt$ — функция Крампа;

q — эффективное отношение сигнал/шум: для злоумышленника $q = q_ч$, для легального абонента $q = q_ч L = q_с$, $q_ч = E_ч/N_0$ — отношение энергии $E_ч$ одного чипа к N_0, а $q_с = E_с / N_0$ — отношение энергии $E_с$ символа к N_0.

Как было показано в [5], «поскольку злоумышленник не знает структуры расширяющей нелинейной ПСП и специального ключа, будем полагать, что он пытается осуществлять поэлементный прием. Энергия сигнала, определяющая вероятность его правильного обнаружения злоумышленником $P_{п.о}$, в этом случае определяется амплитудой сигнала и длительностью одного чипа расширяющей ПСП $\tau_ч$. Для легального абонента, напротив, энергия сигнала будет определяться длительностью информационного символа $\tau_с = \tau_ч B = \tau_ч L$, где B — база сигнала, численно равная длине расширяющей ПСП L. Таким образом, эквивалентное отношение сигнал/шум для легального абонента будет в B раз больше: $q_с = q_ч B$». Для иллюстрации различия в показателях помехоустойчивости и представления их наглядного сравнения на одном графике будем нормировать отношение сигнал/шум на энергию одного чипа расширяющей ПСП и рассматривать величину $E_ч/N_0$, при этом для легального абонента эффективное отношение сигнал/шум в решающем устройстве $q = q_с = q_ч L$, а для злоумышленника $q = q_ч$. При этом реальная эквивалентная шумовая полоса для легального абонента определяется интервалом накопления $\tau_с$ и примерно равна $1/\tau_с$, тогда как для злоумышленника, работающего по чипам, — $1/\tau_ч$.

Зависимости вероятности правильного обнаружения стегосигнала от отношения сигнал/шум q (отношения энергии чипа расширяющей ПСП $E_ч$ к спектральной плотности мощности шума N_0) приведены на рис. 7, *а* [5] для вероятности ложной тревоги $P_{л.т} = 0{,}1$. Кривая *1* описывает поэлементный прием злоумышленником, а кривые *2*, *3* и *4* — прием легальным абонентом при длинах расширяющей нелинейной ПСП $L = 511$, 8191 и 16 383 элемента.

При $q < 0$ дБ поэлементный прием для злоумышленника практически нереализуем [17, 18], тогда как легальный абонент, располагающий структурой расширяющей ПСП длиной $L = 16\,383$ элемента, уже при $q = -33$ дБ достигает вероятности правильного обнаружения $P_{п.о} = 0{,}9972$ [5].

Следует подчеркнуть, что для злоумышленника, не обладающего знанием опорной ПСП, принята упрощенная (и оптимистичная для него) модель приемника. Предполагается, что решение принимается по символу при эффективном отношении сигнал/шум $q_ч$, без выигрыша от корреляции с ПСП. В реальных условиях отсутствие ПСП приводит к еще более низкой вероятности правильного обнаружения символа, поэтому полученные оценки для злоумышленника фактически являются верхней границей его возможностей.

Теперь оценим возможность искажения информационного символа стегосигнала для легального абонента, осуществляющего корреляционный прием, и для злоумышленника, пытающегося осуществить поэлементный прием.

Количественной мерой искажения символа (элемента стегосообщения) будем полагать вероятность битовой ошибки в переданном стегосообщении, определяемую в соответствии с выражением

$$P_0 = Q\left(\sqrt{\frac{E(1-\rho)}{N_0}}\right), \qquad (13)$$

где $Q(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,\mathrm{d}t$ — гауссов интеграл ошибок; ρ — временной коэффициент взаимной корреляции, который принимает значения от –1 до 1 включительно.

Для сигналов, использующих фазовую манипуляцию несущей частоты на 0 – π, значение $\rho = -1$. Таким образом, в данном случае вероятность битовой ошибки определяется следующим выражением:

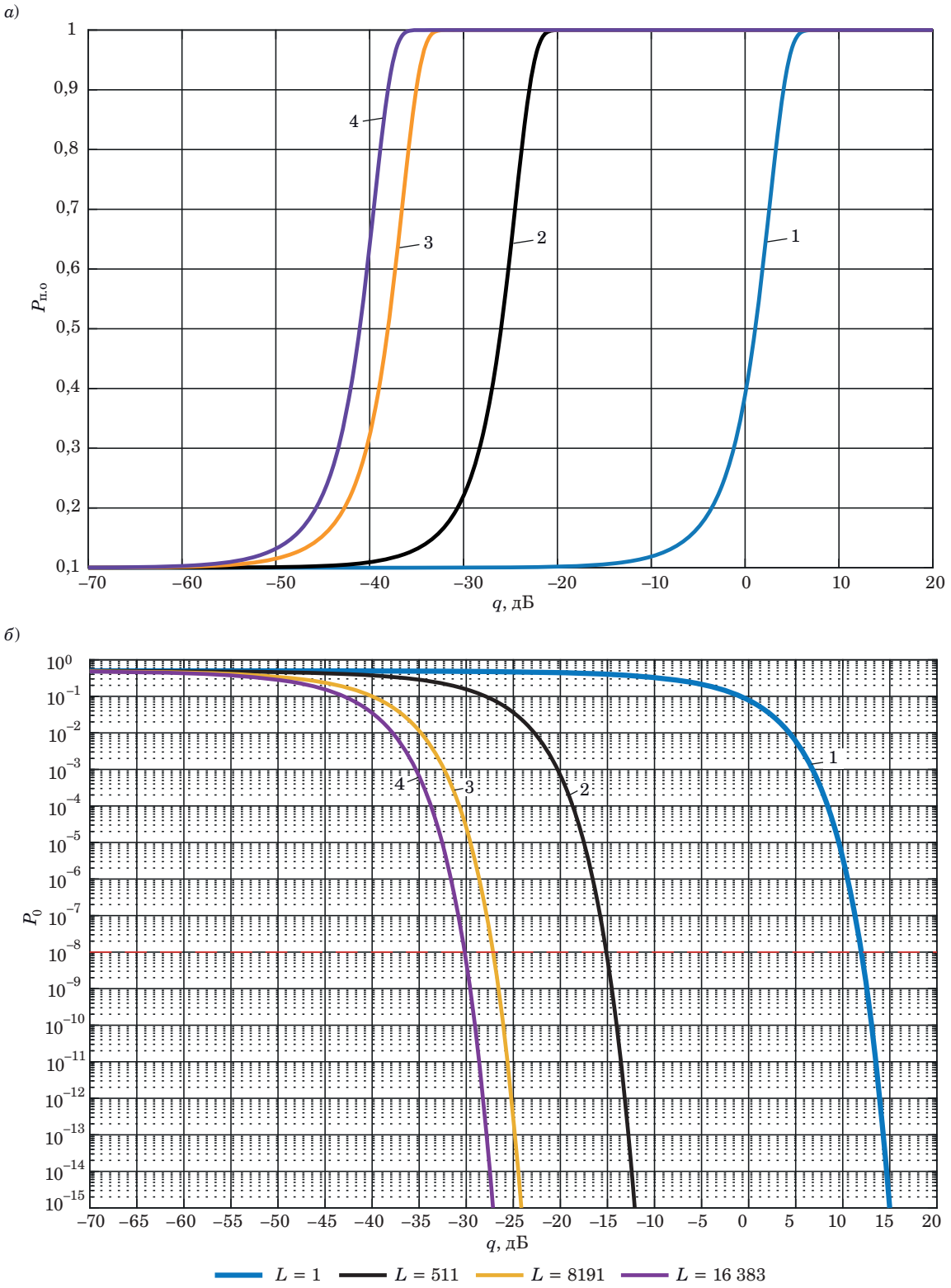
$$P_0 = Q\left(\sqrt{\frac{2E}{N_0}}\right). \qquad (14)$$

В выражениях (13), (14) величина P_0 рассматривается как вероятность ошибки информационного символа при бинарном приеме. Для легального абонента, реализующего корреляционный прием по полной расширяющей ПСП длиной L, энергия символа пропорциональна $E_с = E_ч L$, а соответствующее отношение сигнал/шум $q = q_с = q_ч L$. Для злоумышленника, осуществляющего поэлементный (почиповый) прием и не использующего знание ПСП, решение по тому же информационному символу принимается при существенно меньшей эффективной энергии, близкой к $E_ч$, т. е. при гораздо меньшем E/N_0 в (13), (14), а эффективное отношение сигнал/шум $q = q_ч$.

Отметим, что для злоумышленника величина P_0 в (13), (14) отражает вероятность ошибки при решении по одному чипу расширяющей ПСП. При восстановлении всего информационного символа в целом эта вероятность будет еще выше [4, 5].

Как уже отмечалось, у легального абонента энергия определяется длительностью информационного символа $\tau_с = \tau_ч B$ (против длительности чипа $\tau_ч$ у злоумышленника), что дает ему выигрыш в отношении сигнал/шум в B раз: $q_с = q_ч B$ [4].

Зависимости вероятности битовой ошибки принятого стегосообщения от эквивалентного отношения сигнал/шум приведены на рис. 7, *б:* кривая *1* описывает прием злоумышленником,



■ ***Рис. 7.*** Зависимость вероятности правильного обнаружения стегосигнала (*а*) [5] и битовой ошибки (*б*) от отношения сигнал/шум: *1* — прием злоумышленником; *2–4* — прием легальным абонентом при расширяющей нелинейной ПСП

■ ***Fig. 7.*** Dependence of the stego signal detection probability (*a*) [5] and bit error probability (*б*) on the signal-to-noise ratio: *1* — reception by an adversary; *2–4* — reception by a legitimate subscriber using an expanding nonlinear pseudorandom sequence

кривые *2*, *3* и *4* — прием легальным абонентом при длинах расширяющей нелинейной ПСП L = 511, 8191 и 16 383 элемента [4].

Из графиков видно, что требуемая достоверность информационного обмена (вероятность битовой ошибки) при передаче информационного сообщения меньше 10^{-8} [12] у легального абонента при применении расширяющей нелинейной ПСП длиной L = 16 383 элемента достигается при q = –30 дБ, в то время как для злоумышленника — при q = 12 дБ, что в реальных условиях эксплуатации достичь сложно.

Таким образом, расчеты, подтвержденные экспериментом, показывают, что существует возможность выбора такого диапазона значений параметров сигнала-контейнера и стегосигнала (длительности символов сигнала-контейнера, угла, определяющего энергию стегосигнала, периода накопления, количества символов расширяющей нелинейной ПСП в информационном символе стегосигнала и т. д.), при которых энергии информационного символа, накопленного легальным абонентом сигнала при условии знания им расширяющей нелинейной ПСП стегосигнала, достаточно для его качественного (с заданной помехоустойчивостью) обнаружения и корреляционного приема.

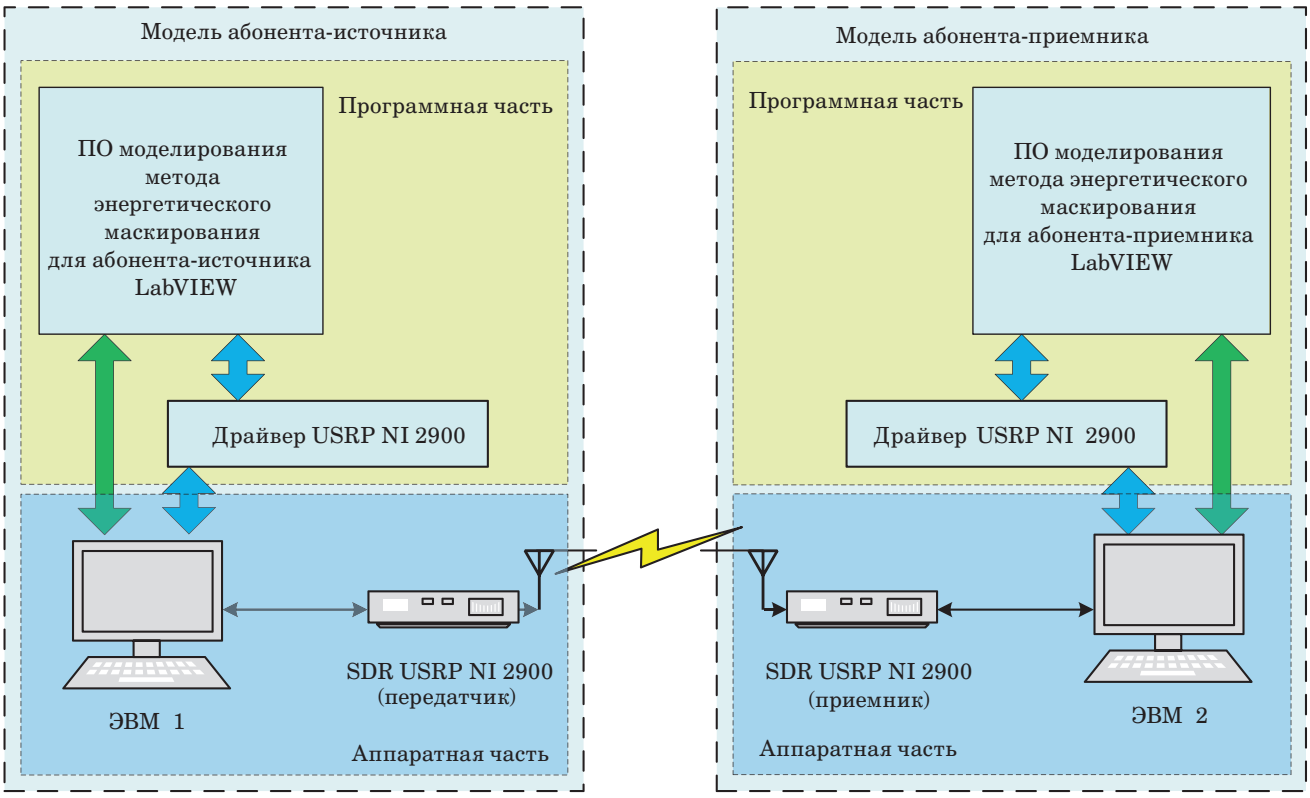
В то же время в условиях отсутствия сведений о расширяющей нелинейной ПСП у потенциального злоумышленника накопление энергии и выделение им информационного символа невозможно, а энергии одного чипа недостаточно для почипового обнаружения и приема.

Программная реализация способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП

Для оценки возможности физической реализации предложенного способа разработаны программное обеспечение (ПО) компьютерного моделирования и стенд полунатурного моделирования способа формирования радиостеганографического сигнала.

Основная часть ПО моделирования выполнена на языке G в среде графического программирования LabVIEW [19].

Стенд полунатурного моделирования (рис. 8) представляет собой аппаратно-программный комплекс, включающий модели абонента-источника и абонента-приемника.



■ ***Рис. 8.*** Структурная схема стенда полунатурного моделирования способа формирования радиостеганографического сигнала

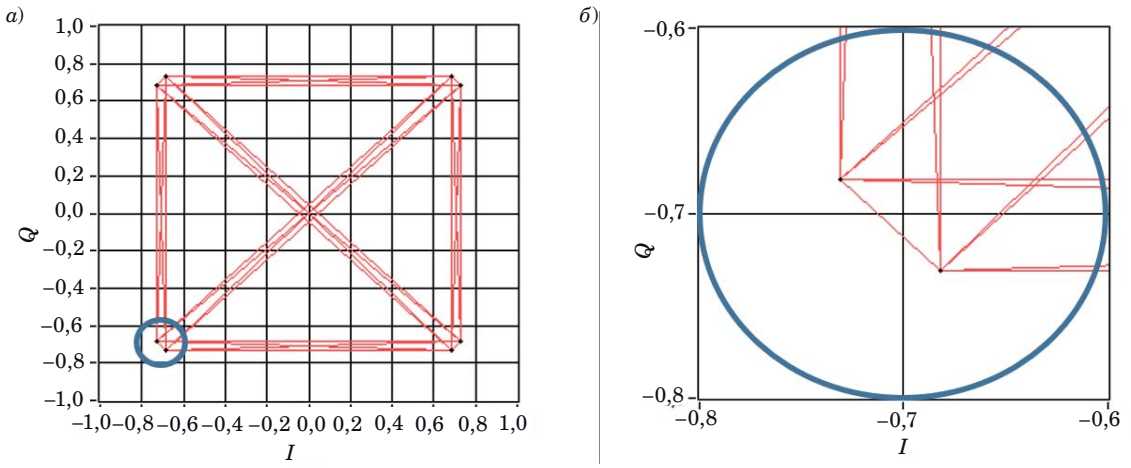
■ ***Fig. 8.*** Structural diagram of the stand for semi-natural modeling of the formation method radio steganographic signal

Для формирования радиоканала в качестве приемо-передающих устройств использовались программно-определяемые радиоустройства USRP NI 2900 (Software-defined radio, SDR). Устройство NI USRP 2900 — это настраиваемый дуплексный приемопередатчик с несущей частотой от 70 МГц до 6 ГГц и полосой пропускания 56 МГц. Одно из устройств выполняет передачу совмещенного сигнала, а второе — прием этого сигнала, реализуя таким образом физическую модель радиоканала передачи информации. Непосредственно логику формирования и обработки совмещенного сигнала в ходе выполнения алгоритма определяет разработанное ПО моделирования соответствующего способа формирования радиостеганографического сигнала, загруженное в устройства USRP NI 2900.

Выполнено моделирование процесса передачи информации с использованием способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП. Предложенный способ позволяет выполнять совместную передачу информации по каналу-контейнеру и передачу по стегоканалу.

Квадратурная диаграмма передаваемой информации по каналу-контейнеру и стегоканалу на панели приборов программы LabVIEW показана на рис. 9. На рис. 9, *а* представлена квадратурная диаграмма при одинаковых масштабах осей *I* и *Q*. На ней различимы четыре позиции сигнала-контейнера с напряжением 1 В (чипы со значением «0» и «1» расширяющей ПСП по двум квадратурным составляющим), тогда как две позиции стегосигнала (±0,01 В) при таком масштабе практически неразличимы. Увеличение масштаба осей (рис. 9, *б*) позволяет различить разные позиции стегосигнала в пределах одной позиции сигнала-контейнера.

Квадратурная диаграмма сигнала-контейнера, принятого в смеси с шумом, показана на рис. 10 [4].



■ ***Рис. 9.*** Фазовая диаграмма совмещенного сигнала: *а* — в масштабе всего сигнала; *б* — в увеличенном масштабе [4]
■ ***Fig. 9.*** Constellation diagram of the combined signal: *а* — full view; *б* — enlarged view [4]

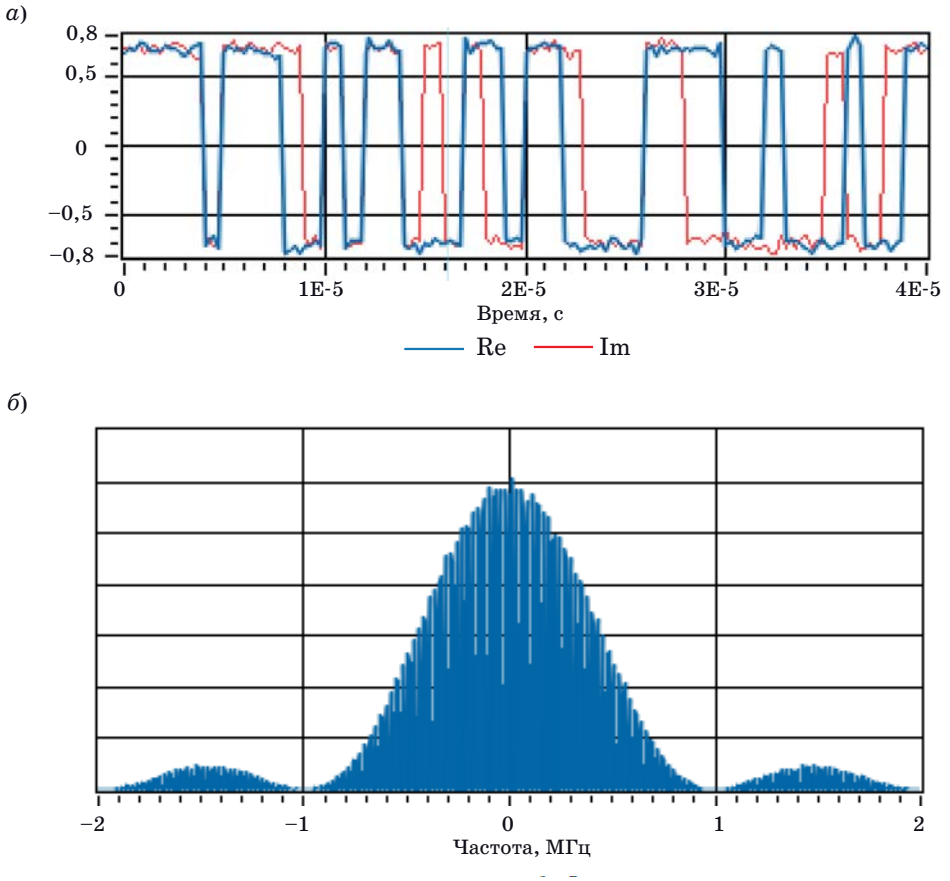


■ ***Рис. 10.*** Фазовая диаграмма принимаемого сигнала-контейнера в смеси с шумом [4]
■ ***Fig. 10.*** Phase diagram of the received container signal in a mixture with noise [4]

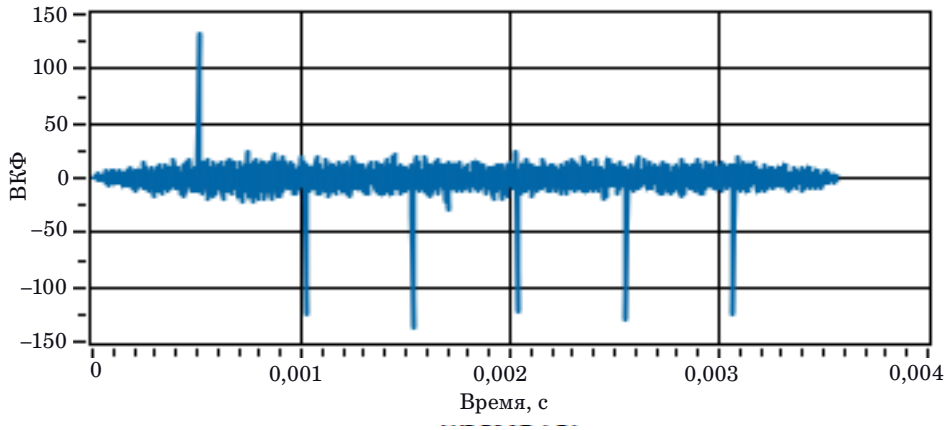
Осциллограмма и спектр принятого совмещенного сигнала показаны на рис. 11, *а* и *б*. Сигнал-контейнер легко различим и во временной, и в частотной областях, и на квадратурной диаграмме, тогда как стегосигнал теряется в шуме и на фоне контейнера. Его выделение без знания структуры нелинейной ПСП невозможно [4].

Полученная в результате свертки демодулированного сигнала с опорной ПСП корреляционная функция (рис. 12) содержит положительные и отрицательные пики (свертка с опорными сигналами символов «0» и «1») [4].

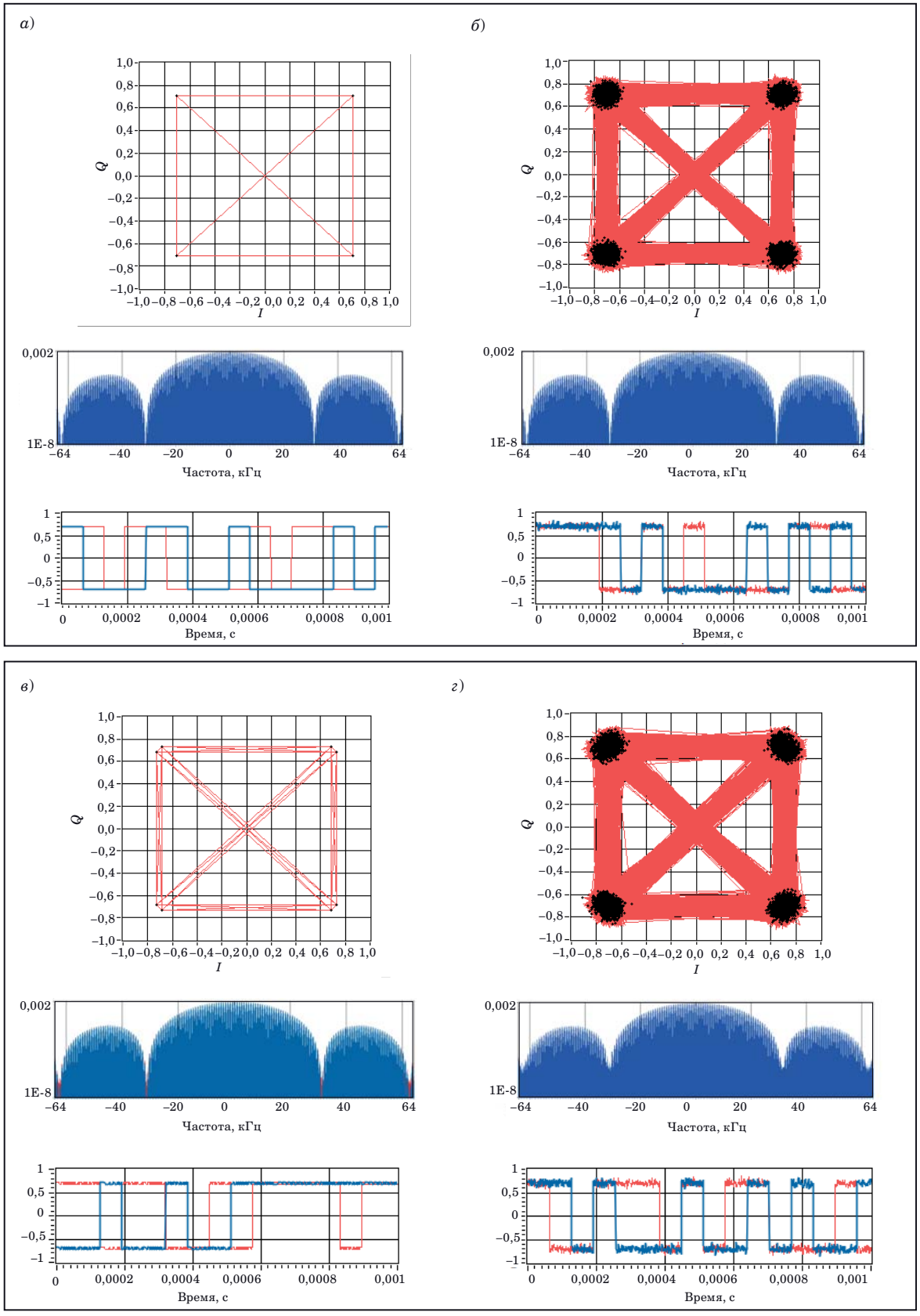
На рис. 13 сопоставлены квадратурные диаграммы, спектры и временные диаграммы «пустого» сигнала-контейнера и совмещенного сигнала



■ ***Рис. 11.*** Осциллограмма (*а*) и спектр (*б*) принимаемого совмещенного сигнала в смеси с шумом
■ ***Fig. 11.*** Oscillogram (*а*) and spectrum (*б*) of the received combined signal mixed with noise



■ ***Рис. 12.*** Взаимная корреляционная функция принимаемого стегосигнала
■ ***Fig. 12.*** Cross-correlation function of the received stego signal



■ ***Рис. 13.*** Фазовые диаграммы, спектры и временные диаграммы: *а* — «пустой» сигнал-контейнер без шума; *б* — «пустой» сигнал-контейнер в смеси с шумом; *в* – совмещенный сигнал без шума; *г* — совмещенный сигнал в смеси с шумом

■ ***Fig. 13.*** Constellation diagrams, spectra, and time-domain waveforms: *а* — cover signal without noise; *б* — cover signal with noise; *в* – combined signal without noise; *г* — combined signal with noise

без шума и в смеси с шумом. Как следует из сравнения рис. 13, *а* и *в*, встраивание стегосигнала смещает точки квадратурного созвездия лишь незначительно и заметно только в отсутствие шума. В реальном канале (рис. 13, *б*, *г*) совмещенный сигнал и «пустой» контейнер визуально и статистически неотличимы. Ни по квадратурной диаграмме, ни по спектру, ни по временной диаграмме факт наличия стегосигнала без знания ключа формирования расширяющей ПСП не обнаруживается.

Результаты эксперимента с использованием разработанного ПО подтверждают реализуемость предложенного способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП, а также возможность выбора таких параметров, которые позволят осуществлять обнаружение, прием и обработку стегосигнала легальными абонентами при невозможности его обнаружения злоумышленником.

Заключение

В работе предложен новый способ формирования скрытого (маскированного) сигнала, основанный на использовании дополнительной фазовой манипуляции и нелинейной расширяющей ПСП, реализующий метод радиостеганографии, который, с одной стороны, позволяет легальным абонентам принимать скрытый сигнал с необходимым качеством, а с другой — существенно ограничивает возможности злоумышленника по его обнаружению и приему.

Показано, что при применении способа для передачи информации по стегоканалу можно выбрать параметры стегосигнала (индекс модуляции, период накопления, количество чипов расширяющей ПСП в информационном символе стегосигнала и т. д.), при которых энергии информационного символа, накопленной легальным абонентом при условии знания им расширяющей ПСП, достаточно для его обнаружения и корреляционного приема, а также целесообразно использовать расширение спектра сигнала нелинейной ПСП, обладающей высокой структурной скрытностью.

Основные результаты:

1. Получены аналитические соотношения для выбора параметров стегосигнала, обеспечивающих $P_{\text{п.о}} > 0{,}9972$ для легального получателя при $P_{\text{п.о}} \approx 0{,}1$ для злоумышленника.

2. Показано, что при использовании ПСП длиной $L = 16\,383$ легальный приемник обеспечивает $P_{\text{п.о}} < 10^{-8}$ при $q = -30$ дБ, в то время как злоумышленнику требуется $q > 12$ дБ, что на 42 дБ выше.

3. Экспериментально подтверждена работоспособность метода на стенде с USRP NI 2900. Отклонение экспериментальных данных от расчетных не превышает 5 %.

4. Способ применим к широкому классу цифровых радиосистем: WiFi, LTE, DVB-T и др. [20–22].

Таким образом, предложенный радиостеганографический способ, определенный на физическом уровне, может использоваться практически в любой цифровой радиосистеме, например в сетях Wi-Fi 802.11, цифровых мобильных сетях, цифровом телевидении, навигационных системах и т. д. [23, 24].

Направления дальнейших исследований:

1) анализ влияния многолучевого распространения и доплеровского сдвига;

2) адаптивный выбор параметров стегосигнала в зависимости от условий канала;

3) разработка протоколов обмена ключами для синхронизации ПСП;

4) исследование возможности одновременной передачи нескольких стегосигналов.

Литература

1. **Долженков С. С., Максимова Е. А.** Исследование антропоморфических видов организации межобъектного взаимодействия на уровне субъекта критической информационной инфраструктуры. *Вестник Санкт-Петербургского университета государственной противопожарной службы МЧС России*, 2025, № 1, с. 94–108. doi:10.61260/2218-130X-2025-1-94-108, EDN: MEPVXZ
2. **Cuevas D., Gutiérrez M., Ibáñez J., Santamaría I.** Low probability of detection communication using noncoherent grassmannian signaling. *Proceedings of the 2025 59th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 2025, pp. 514–518. doi:10.1109/IEEECONF67917.2025.11443893
3. **D'Oro S., Restuccia F., Melodia T.** Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying. *Proceedings of the IEEE INFOCOM 2019*, Paris, 2019, pp. 1585–1593. doi:10.1109/INFOCOM.2019.8737581
4. **Штанько С. В., Крягин В. А.** Применение сигнально-кодовой конструкции с дополнительной квадратурной модуляцией при передаче информации по космическим радиолиниям. *СПбНТОРЭС: труды ежегодной научно-технической конференции*, СПб., 2023, № 1(78), с. 167–170. EDN: RWLXQM
5. **Штанько С. В., Крягин В. А.** Вопросы практической реализации способа передачи навигационных сигналов с использованием дополнительного канала для передачи навигационных меток. *Навигация и гидрография*, 2025, № 3(80), с. 37–48. EDN: JFWGFB

6. **Беляев С. С., Будько М. Б., Будько М. Ю., Гирик А. В., Грозов В. А.** Построение функции генерации криптографически стойких псевдослучайных последовательностей на базе алгоритма «Кузнечик». *Вопросы кибербезопасности*, 2021, № 4(44), с. 25–34. doi:10.21681/2311-3456-2021-4-25-34, EDN: GBNJBU
7. **Дегтярев А. Н., Афонин И. Л., Поляков А. Л.** Корреляционный прием одномерных полосовых сигналов в условиях действия межсимвольной интерференции и межканальных помех с периодическим опорным сигналом. *Радиоэлектроника. Наносистемы. Информационные технологии*, 2025, т. 17, № 3, с. 279–284. doi:10.17725/j.rensit.2025.17.279, EDN: IFGMJF
8. **Кондрашов Ю. В., Бирюков М. А., Сазонов В. В., Ротенбергер А. А.** Влияние корреляционных функций широкополосных сигналов на помехоустойчивость их приема в многолучевых каналах связи. *Электросвязь*, 2022, № 3, с. 10–15. doi:10.34832/ELSV.2022.28.3.001, EDN: NGNWBJ
9. **Бобровский В. В.** Особенности корреляционной обработки шумоподобных сигналов в электроразведочной аппаратуре. *Геофизические исследования*, 2022, т. 23, № 2, с. 39–54. doi:10.21455/gr2022.2-3, EDN: DCPGAB
10. **Чесноков М. Н., Литвинов А. А., Соловьев А. А., Волгушев Д. Б.** Помехозащищенность приема ортогональных стохастических широкополосных сигналов в условиях воздействия запаздывающих помех. *Успехи современной радиоэлектроники*, 2021, т. 75, № 4, с. 48–56. doi:10.18127/j20700784-202104-07, EDN: ZGBQUX
11. **Кисельников А. Е.** *Алгоритмы идентификации типов искажения сигналов с цифровой модуляцией на основе анализа вектора ошибок*: дис. … канд. техн. наук, Ярославль, ЯрГУ, 2021, 132 с. EDN: AVDIRR
12. **Михайлик Д. А., Малыгин И. В.** Расчет устойчивости системы спутниковой связи на основе широкополосных сигналов по отношению к импульсным и флуктуационным помехам. *Ural Radio Engineering Journal*, 2023, т. 7, № 2, с. 153–165. doi:10.15826/urej.2023.7.2.004, EDN: KOQCWC
13. **Chen C., Zeng X., Ao M., Li C., Zhou F., Ye F.** Security protection of GNSS reference station data based on bespoke steganography embedding algorithm. *Proceedings of the IEEE International Conference on Communications (ICC 2025)*, Chengdu, 2025, pp. 197–202. doi:10.1109/ICC51173.2025.11069711
14. **Aggarwal R., Dagefu F., Kong J., Choi J., Kim B., Spasojevic P.** On covertness of DSSS against Energy and cycle detectors under link QoS requirements. *Proceedings of the IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*, Oslo, 2025, pp. 1–6. doi:10.1109/VTC2025-Spring.2025.00001
15. **Дегтярев А. Н., Афонин И. Л., Поляков А. Л., Зеленкевич Д. Ю.** Повышение помехоустойчивости обнаружителя сигнала. *Радиоэлектроника. Наносистемы. Информационные технологии*, 2025, т. 17, № 4, с. 409–418. doi:10.17725/j.rensit.2025.17.409, EDN: CVTQSU
16. **Потапов А. А.** Определение порогов обнаружения радиосигналов для метода энергетического детектора. *Журнал радиоэлектроники*, 2021, № 9. doi:10.30898/1684-1719.2021.9.3, EDN: BGELRC
17. **Иванов Н. М.** Обнаружение и пеленгование новых слабых сигналов в присутствии мощных помех. *Радиотехника*, 2025, т. 89, № 11, с. 131–137. doi:10.18127/j00338486-202511-15, EDN: FVTQYR
18. **Потапов А. А.** Радиомониторинг низкоуровневых радиосигналов посредством анализа периодических спектральных выборок. *Нелинейный мир*, 2021, т. 19, № 3, с. 5–17. doi:10.18127/j20700970-202103-01, EDN: BZXRPI
19. **Абрамов А. А., Якуш Н. А.** Разработка методики поверки USRP для высокоточного исследования радиосистем. *Труды МАИ*, 2022, № 127. doi:10.34759/trd-2022-127-12, EDN: MZLARX
20. **Гавришев А. А., Осипов Д. Л.** Оценка скрытности OFDM сигналов, основанных на BPSK модуляции, с помощью методов нелинейной динамики. *TComm: Телекоммуникации и транспорт*, 2022, т. 16, № 9, с. 13–19. doi:10.36724/2072-8735-2022-16-9-13-19, EDN: GICCDT
21. **Bonati L., D'Oro S., Restuccia F., Basagni S., Melodia T.** SteaLTE: Private 5G cellular connectivity as a service with full-stack wireless steganography. *IEEE INFOCOM 2021 — IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2021, pp. 1–10. doi:10.1109/INFOCOM42981.2021.9488889
22. **Grzesiak K., Piotrowski Z., Kelner J. M.** A wireless covert channel based on dirty constellation with phase drift. *Electronics*, 2021, vol. 10, no. 6, art. 647. doi:10.3390/electronics10060647
23. **Карцан И. Н.** Математическая модель защищенного канала связи для морских исследований методом стеганографии. *Informatics. Economics. Management*, 2024, т. 3, № 2, с. 415–424. doi:10.47813/2782-5280-2024-3-2-0415-0424, EDN: MPYZSM
24. **Grzesiak K., Piotrowski Z., Kelner J. M.** Covert channel based on quasi-orthogonal coding. *Electronics*, 2023, vol. 12, no. 10, art. 2249. doi:10.3390/electronics12102249

UDC 621.376.9
doi:10.31799/1684-8853-2026-5-56-72
EDN: CMAJJN

A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence

S. V. Shtanko[a], Dr. Sc., Tech., Associate Professor, orcid.org/0000-0002-8391-8911, vka@mil.ru
V. A. Kryagin[a], Lecturer, orcid.org/0009-0002-7529-283X
P. N. Topchiy[a], Lecturer, orcid.org/0009-0008-4678-7685
D. A. Anikin[b], Head of Department, orcid.org/0009-0003-8295-312X
[a]A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia Emb., 197198, Saint-Petersburg, Russian Federation
[b]Ministry of Defense of the Russian Federation, 19, Znamenka St., 119160, Moscow, Russian Federation

Introduction: The development of global communication systems has increased the standards for information confidentiality, especially in critical information infrastructure systems whose elements are interconnected via radio channels. Cryptographic methods conceal the meaning of transmitted data but do not hide the very fact of information exchange. Radio steganographic methods based on embedding a stego signal into an open carrier signal at the physical layer address this issue; however, they require energy concealment of the stego signal and robustness against an attacker's detection attempts. **Purpose:** To develop a method of energy masking for a radio signal inside a carrier signal based on additional phase manipulation and a nonlinear spreading pseudorandom sequence, which provides covert information transmission over a stego channel with a specified noise immunity for the legitimate user and prevents an attacker from detecting the stego signal. **Results:** The proposed method forms the stego signal by applying an additional small-angle phase manipulation to the vector of the phase-modulated carrier signal. The deviation angle has been chosen so that the energy of a single chip could remain masked within the phase-noise variance. The spectrum of the stego signal has been spread by a nonlinear pseudorandom sequence generated by a nonlinear pseudorandom sequence generator resistant to analytical attacks. Analytical expressions for the probability of correct detection and the bit error probability have been obtained. The findings show that, for a spreading sequence length of 16383 chips, the legitimate user has achieved a detection probability of 0.9972 at a chip-energy-to-noise spectral density ratio of $q = -33$ dB, whereas an attacker employing chip-by-chip reception has failed to detect the stego signal for $q < 0$ dB. A bit error probability below 10^{-8} has been achieved at $q = -30$ dB, while an attacker has required more than 12 dB, which has given a 42 dB advantage. A semi-hardware testbed based on software-defined radios has been developed; the deviation of experimental results from analytical estimates has not exceeded five percent. **Practical relevance:** The method is applicable to a wide class of digital phase-modulated radio systems and can be used for data transmission over an embedded channel in critical information infrastructure systems.

Keywords — phase manipulation, pseudorandom sequence, phase diagram, container signal, expanding sequence, correlation technique, stego signal, stego message, nonlinear expanding sequence.

For citation: Shtanko S. V. , Kryagin V. A., Topchiy P. N. , Anikin D. A. A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 56–72 (In Russian). doi:10.31799/1684-8853-2026-5-56-72, EDN: CMAJJN

References

1. Dolzhenkov S. S., Maksimova E. A. Study of anthropomorphic types of organization of interobject interaction at the level of a subject of critical information infrastructure. *Vestnik Saint-Petersburg University of State Fire Service of EMERCOM of Russia*, 2025, no. 1, pp. 94–108 (In Russian). doi:10.61260/2218-130X-2025-1-94-108, EDN: MEPVXZ
2. Cuevas D., Gutiérrez M., Ibáñez J., Santamaría I. Low probability of detection communication using noncoherent grassmannian signaling. *Proceedings of the 2025 59th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 2025, pp. 514–518. doi:10.1109/IEEECONF67917.2025.11443893
3. D'Oro S., Restuccia F., Melodia T. Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying. *Proceedings of the IEEE INFOCOM 2019*, Paris, 2019, pp. 1585–1593. doi:10.1109/INFOCOM.2019.8737581
4. Shtanko S. V., Kryagin V. A. The use of a signal-code structure with additional quadrature modulation when transmitting information over space radio lines. *SPbNTORES: trudy ezhegodnoi nauchno-tekhnicheskoi konferentsii* [SPbNTORES: Proceedings of the Annual Scientific and Technical Conference]. Saint-Petersburg, 2023, no. 1(78), pp. 167–170 (In Russian). EDN: RWLXQM
5. Shtanko S. V., Kryagin V. A. Issues of practical implementation of the method of transmitting navigation signals using an additional channel for transmitting navigation tags. *Navigation and Hydrography*, 2025, no. 3(80), pp. 37–48 (In Russian). EDN: JFWGFB
6. Beliaev S., Budko M., Budko M., Guirik A., Grozov V. Development of a pseudo-random sequence generation function based on the "Kuznechik" cryptographic algorithm. *Voprosy kiberbezopasnosti*, 2021, no. 4(44), pp. 25–34 (In Russian). doi:10.21681/2311-3456-2021-4-25-34, EDN: GBNJBU
7. Degtiarev A. N., Afonin I. L., Poliakov A. L. Correlation reception of one-dimensional bandpass signals under conditions of inter-symbol interference and inter-channel interference with a periodic reference signal. *Radioelectronics. Nanosystems. Information Technologies*, 2025, vol. 17, no. 3, pp. 279–284 (In Russian). doi:10.17725/j.rensit.2025.17.279, EDN: IFGMJF
8. Kondrashov Yu. V., Biriukov M. A., Sazonov V. V., Rotenberger A. A. Influence of correlation functions of broadband signals on the noise immunity of their reception in multipath communication channels. *Elektrosviaz'*, 2022, no. 3, pp. 10–15 (In Russian). doi:10.34832/ELSV.2022.28.3.001, EDN: NGNWBJ
9. Bobrovskii V. V. Peculiarities of correlation processing of pseudonoise signals in electrical prospecting equipment. *Geophysical Research*, 2022, vol. 23, no. 2, pp. 39–54 (In Russian). doi:10.21455/gr2022.2-3, EDN: DCPGAB
10. Chesnokov M. N., Litvinov A. A., Soloviev A. A., Volgushev D. B. Performance of orthogonal stochastic code signals in the presence of delayed interference. *Achievements of Modern Radioelectronics*, 2021, vol. 75, no. 4, pp. 48–56 (In Russian). doi:10.18127/j20700784-202104-07, EDN: ZGBQUX
11. Kisel'nikov A. E. *Algoritmy identifikatsii tipov iskazheniia signalov s tsifrovoi moduliatsiei na osnove analiza vektora oshibok*. Dis. kand. tekhn. nauk [Algorithms for identifying types of distortion of digitally modulated signals based on error vector analysis. PhD tech. sci. diss.]. Yaroslavl, IarGU Publ., 2021. 132 p. (In Russian). EDN: AVDIRR
12. Mikhailik D. A., Malygin I. V. Estimation of the immunity of a satellite communication system based on wideband signals in relation to impulse and fluctuating interferences. *Ural Radio Engineering Journal*, 2023, vol. 7, no. 2, pp. 153–165 (In Russian). doi:10.15826/urej.2023.7.2.004. EDN: KOQCWC
13. Chen C., Zeng X., Ao M., Li C., Zhou F., Ye F. Security protection of GNSS reference station data based on bespoke steganography embedding algorithm. *Proceedings of the IEEE International Conference on Communications (ICC 2025)*, Chengdu, 2025, pp. 197–202. doi:10.1109/ICC51173.2025.11069711
14. Aggarwal R., Dagefu F., Kong J., Choi J., Kim B., Spasojevic P. On covertness of DSSS against Energy and cycle detectors under link QoS requirements. *Proceedings of the IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*, Oslo, 2025, pp. 1–6. doi:10.1109/VTC2025-Spring.2025.00001

15. Degtiarev A. N., Afonin I. L., Poliakov A. L., Zelenkevich D. Yu. Improving the noise immunity of the signal detector. *Radioelectronics. Nanosystems. Information Technologies*, 2025, vol. 17, no. 4, pp. 409–418 (In Russian). doi:10.17725/j.rensit.2025.17.409, EDN: CVTQSU
16. Potapov A. A. Radio signals detection thresholds estimation for energy detection technique. *Journal of Radio Electronics*, 2021, no. 9 (In Russian). doi:10.30898/1684-1719.2021.9.3, EDN: BGELRC
17. Ivanov N. M. Detecting and direction finding of new weak signals in presence of high-power noise. *Radioengineering*, 2025, vol. 89, no. 11, pp. 131–137 (In Russian). doi:10.18127/j00338486-202511-15, EDN: FVTQYR
18. Potapov A. A. Low-level signals radiomonitoring using periodic spectrum samples analysis. *Nonlinear World*, 2021, vol. 19, no. 3, pp. 5–17 (In Russian). doi:10.18127/j20700970-202103-01, EDN: BZXRPI
19. Abramov A. A., Yakush N. A. Development of USRP verification methodology for high-precision radio system research. *Trudy MAI*, 2022, no. 127 (In Russian). doi:10.34759/trd-2022-127-12, EDN: MZLARX
20. Gavrishev A. A., Osipov D. L. Evaluation of the stealth of OFDM-signals based on BPSK modulation, using nonlinear dynamics methods. *T-Comm*, 2022, vol. 16, no. 9, pp. 13–19 (In Russian). doi:10.36724/2072-8735-2022-16-9-13-19, EDN: GICCDT
21. Bonati L., D'Oro S., Restuccia F., Basagni S., Melodia T. SteaLTE: Private 5G cellular connectivity as a service with full-stack wireless steganography. *IEEE INFOCOM 2021 – IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2021, pp. 1–10. doi:10.1109/INFOCOM42981.2021.9488889
22. Grzesiak K., Piotrowski Z., Kelner J. M. A wireless covert channel based on dirty constellation with phase drift. *Electronics*, 2021, vol. 10, no. 6, art. 647. doi:10.3390/electronics10060647
23. Kartsan I. N. Mathematical model of secure communication channel for marine research by steganography method. *Informatics. Economics. Management*, 2024, vol. 3, no. 2, pp. 415–424 (In Russian). doi:10.47813/2782-5280-2024-3-2-0415-0424, EDN: MPYZSM
24. Grzesiak K., Piotrowski Z., Kelner J. M. Covert channel based on quasi-orthogonal coding. *Electronics*, 2023, vol. 12, no. 10, art. 2249. doi:10.3390/electronics12102249

УВАЖАЕМЫЕ АВТОРЫ!

Научная электронная библиотека (НЭБ) продолжает работу по реализации проекта SCIENCE INDEX. После того как Вы зарегистрируетесь на сайте НЭБ (http://elibrary.ru/defaultx.asp), будет создана Ваша личная страничка, содержание которой составят не только Ваши персональные данные, но и перечень всех Ваших печатных трудов, имеющихся в базе данных НЭБ, включая диссертации, патенты и тезисы к конференциям, а также сравнительные индексы цитирования: РИНЦ (Российский индекс научного цитирования), h (индекс Хирша) от Web of Science и h от Scopus. После создания базового варианта Вашей персональной страницы Вы получите код доступа, который позволит Вам редактировать информацию, помогая создавать максимально объективную картину Вашей научной активности и цитирования Ваших трудов.

УДК 004.62, 004.7
doi:10.31799/1684-8853-2026-5-73-84
EDN: CWRBDL

Научные статьи
Articles

Средний возраст информации в распределенных системах хранения данных с равноправными узлами

Д. Р. Крылов[a], *аспирант, orcid.org/ 0009-0008-5901-5342*
У. А. Болотских[a], *магистрант, orcid.org/0009-0009-0733-594X*
А. М. Тюрликов[a], *доктор техн. наук, профессор, orcid.org/0000-0001-7132-094X, turlikov@vu.spb.ru*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *распределенные системы хранения данных могут быть реализованы с помощью ведущих и ведомых узлов или на основе равноправных узлов. Для систем на основе равноправных узлов влияние параметров системы на такой показатель качества функционирования, как средний возраст информации, малоизучен.* ***Цель:*** *разработать модель реплицируемой системы хранения данных с равноправными узлами, позволяющую сформулировать и решить задачу минимизации среднего возраста информации за счет выбора размера кворума записи.* ***Результаты:*** *предложена модель, отражающая основные особенности функционирования реплицируемых систем хранения данных с равноправными узлами, на которые в многоадресном режиме по ненадежному каналу передается обновление. События, что обновление успешно доставлено, происходят независимо для разных узлов. Вероятность успешной доставки обновления является одним из параметров модели. Указан способ вычисления верхней оценки для среднего возраста информации. Приведено сравнение с имитационным моделированием и установлено, что эта оценка отличается от точного значения не более чем на 1 %. Сформулирована и решена оптимизационная задача выбора размера кворума записи, минимизирующего средний возраст информации. Численные результаты показали, что оптимальный размер кворума записи растет с увеличением общего числа узлов. Получена зависимость среднего возраста информации от общего числа узлов при оптимальном размере кворума записи и фиксированных других параметров модели. Отмечено наличие минимума в этой зависимости.* ***Практическая значимость:*** *предложенная модель отражает общие особенности реплицируемых систем хранения данных с равноправными узлами и может быть использована при проектировании реальных систем для соблюдения баланса согласованности и доступности.* ***Обсуждение:*** *ключевым допущением модели является независимость успешной доставки обновления на разные узлы. В реальных системах при многоадресной передаче это допущение может не выполняться, что требует дальнейшего исследования и учета зависимости между событиями доставки.*

Ключевые слова *— средний возраст информации, системы хранения данных, репликация, кворум чтения, кворум записи.*

Для цитирования: Крылов Д. Р., Болотских У. А., Тюрликов А. М. Средний возраст информации в распределенных системах хранения данных с равноправными узлами. *Информационно-управляющие системы*, 2026, № 5, с. 73–84. doi:10.31799/1684-8853-2026-5-73-84, EDN: CWRBDL
For citation: Krylov D. R., Bolotskikh U. A., Turlikov A. M. Average age of information in distributed data storage systems with peer nodes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 73–84 (In Russian). doi:10.31799/1684-8853-2026-5-73-84, EDN: CWRBDL

Введение

Распределенные системы хранения данных (РСХД) широко используются в современных дата-центрах для работы с большими объемами информации. Для предотвращения потери данных из-за выхода из строя узлов [1] в подобных системах применяется дублирование (репликация) фрагментов информации (реплик) на нескольких узлах [2–4]. Но так как во многих сервисах данные регулярно изменяются, то необходимо поддерживать актуальность информации, хранящуюся на узлах, а значит, обновлять уже хранящуюся информацию до более новой. В связи с этим возникает задача обеспечения определенного уровня согласованности в работе системы, чтобы избежать конфликтов при выполнении параллельных операций с данными [5, 6]. Операции, работающие с одной версией данных, называются согласованными. Согласно теореме CAP (Consistency, Availability, Partition tolerance) [7–9], в РСХД нет возможности достичь одновременно высоких показателей согласованности и доступности, что связано с взаимным влиянием этих принципов друг на друга [10]. Следовательно, возникает необходимость в поиске баланса между доступностью и согласованностью.

Основными операциями в современных дата-центрах являются запись и чтение, а самая частая — перезапись уже хранящихся данных [11, 12]. В процессе обновления данных сохраняется временная метка обновления — момент, когда данные были перезаписаны.

Существуют подходы организации работы с данными в таких системах для достижения определенного уровня согласованности и доступности.

Среди них можно выделить системы, которые в англоязычной литературе называются “Leader-based systems” [13, 14]. Они содержат в себе узлы двух типов: “leader” и “follower”, — которые в силу отсутствия устоявшейся терминологии в русском языке будем называть соответственно «ведущие» и «ведомые». Суть подхода заключается в том, что из общего множества узлов выбираются ведущие узлы, на которых обновление информации происходит всегда гарантированно, а на остальных, ведомых, лишь с некоторой вероятностью, обусловленной возможными ошибками в канале и прочими ситуациями, которые могут возникать в результате работы реальных систем [14]. Такой подход позволяет достичь относительно высокого уровня согласованности при приемлемой доступности. Представителями подобных систем на практике можно назвать Amazon DynamoDB, Google Spanner и Apple Foundation, использующие алгоритмы Paxos; для альтернативного алгоритма Raft есть такие хранилища, как MongoDBm и InfluxDB [15–19].

“Leader-based systems” — это частный случай подхода на основе кворумов [20], где нет фиксированных ведущих и ведомых узлов, а обновление должно достичь некоторого минимально необходимого числа узлов (размер кворума записи), после которого процесс обновления считается успешно выполненным и инициируется переход к следующей итерации записи. В этом случае узлами, подлежащими перезаписи, могут оказаться любые из их общего множества, а сама запись происходит только с помощью многоадресной рассылки, которая не гарантирует успешной записи. Такой подход позволяет достичь высокого уровня доступности при удерживании оптимального уровня согласованности. Данный подход рассматривается в настоящей работе и в англоязычной литературе носит название “Dynamo-style data storage” [21]. Такое название не отражает особенностей подобных систем, и прямой перевод на русский язык не имеет смысла, поэтому мы данный способ построения РСХД будем называть как системы хранения данных «с равноправными узлами». Поскольку для Dynamo-style data storage существуют понятия кворума чтения и кворума записи, а для систем Leader-based существуют понятия только кворума чтения, то системы Dynamo-style также можно называть системами «на основе кворумов».

В связи с наличием временных меток обновления на узлах для отслеживания актуальности данных удобно применить метрику, заимствованную из области систем массового обслуживания, — возраст информации (Age of Information, AoI), [22, 23]. Данная метрика позволит проанализировать работу рассматриваемой далее РСХД.

Работ с исследованиями среднего возраста информации в РСХД на основе кворумов проводилось немного. Например, в работе [21] изучалось влияние размера кворума записи на средний возраст информации в системе, получаемой операцией чтения. По результатам данной работы можно судить о наличии оптимального состояния системы, при котором средний возраст информации минимизируется. В работе [24] исследования были продолжены в сторону динамической периодической синхронизации для установления оптимального периода синхронизации при переменной нагрузке.

При увеличении размера кворума записи увеличивается и время, необходимое на запись обновления, что негативно сказывается на среднем возрасте информации. Но при малом размере кворума шанс чтения актуальной версии данных операцией чтения уменьшается, что также ведет к увеличению среднего возраста информации. Таким образом, в работе системы могут существовать оптимальные наборы параметров, при которых средний возраст информации будет минимальным.

В работе [21] время считается непрерывным, а задержки записи моделируются непрерывными случайными величинами (сдвинутое экспоненциальное распределение), от чего процесс записи начинается и заканчивается в произвольные моменты времени. В настоящей статье вся работа системы организована в кадрах, каждый из которых состоит из целого числа слотов (единиц времени), что соответствует реальным системам, где операции планируются по тактам или тикам таймера. Другим важным недостатком работы [21] является то, что не учитывается вероятность отказа при передаче, потому что предполагается, что запись на узел в конечном счете всегда происходит, просто с разной задержкой, которая представляет из себя одну непрерывную случайную величину. В нашем исследовании в каждом слоте делается попытка записи на все узлы, и она успешна с вероятностью p независимо для каждого узла, что позволяет учитывать потери пакетов, тайм-ауты, сетевые ошибки и другие сбои, характерные для реальных РСХД. Еще один недостаток в работе [21] заключается в том, что задержка между завершением одной записи и началом следующей учитывается через сдвиг c в экспоненциальном распределении, но этот сдвиг не интуитивен и не отделен от процесса записи. Нами введена явная фиксированная задержка c слотов между кадрами, что соответствует реальным системам, где после завершения записи требуется время на обработку, формирование следующего обновления, синхронизацию.

В представленной работе исследуется влияние размера кворума записи на средний возраст информации, полученной запросом на чтение.

Время разделено на слоты, в каждом из которых происходит попытка записи обновления на все узлы системы. Успешная запись происходит с некоторой вероятностью, после чего данные сразу становятся доступными для чтения. Запрос на чтение отправляется на некоторое число случайно выбранных узлов, что дает результат, по которому можно судить о среднем возрасте информации.

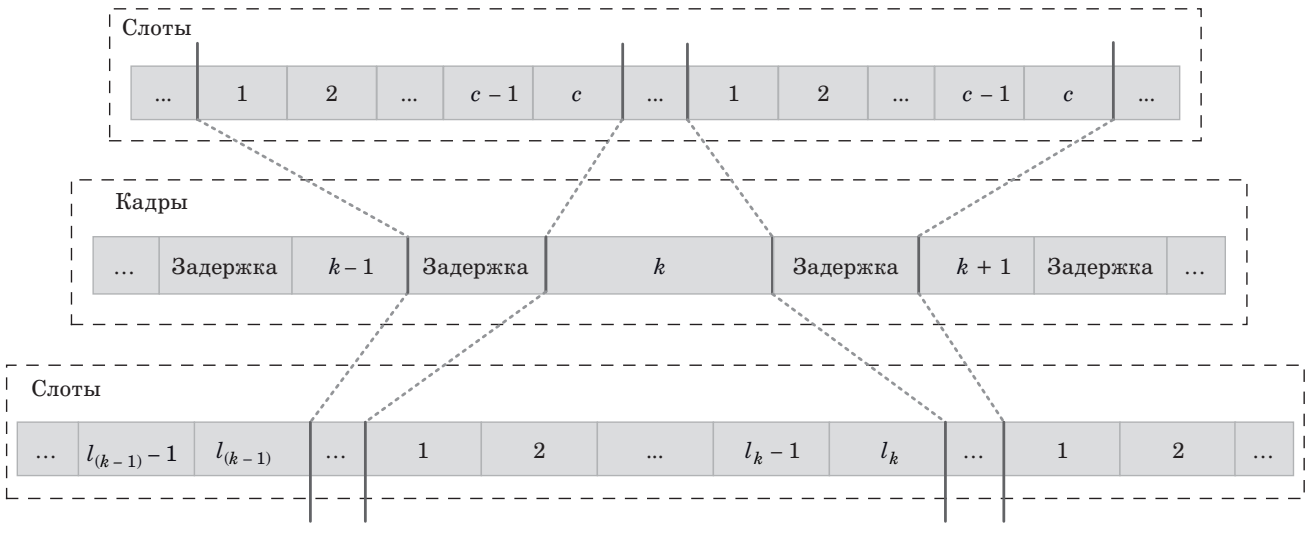
Описание модели системы

Рассмотрим систему хранения данных на основе кворумов для чтения и записи. Всего в системе содержится n узлов, все они имеют один и тот же фрагмент данных, называемый репликой. В системе существуют понятия кворума чтения R и кворума записи W. Кворум записи представляет из себя подмножество размером w узлов, а кворум чтения составляют r узлов. Таким образом, $0 < w \le n$, как и $0 < r \le n$. Узлы, находящиеся в кворуме записи, являются минимально необходимым множеством, которое будет хранить самую последнюю версию реплик. В кворуме чтения содержатся узлы, с которых происходит чтение данных.

Работа системы по времени последовательно разделяется на кадры (рис. 1), каждый из которых имеет свой порядковый номер, обозначенный k. Кадры делятся на временные интервалы, называемые слотами. За единицу времени взят один слот. Отдельно взятые кадры могут отличаться по длительности (числу слотов l_k в кадре), поскольку начало следующего кадра связано с событием инициализации нового обновления. Между кадрами имеется задержка записи, которая составляет фиксированное время, равное c слотам.

Любой кадр начинается с инициализации нового обновления, после чего в каждом слоте кадра происходит попытка записи на узлы системы. Инициализированное обновление считается самым актуальным до конца текущего кадра. Запись происходит посредством многоадресной рассылки, поэтому обновление может не дойти сразу до всех узлов-получателей, в связи с чем может потребоваться большее число слотов внутри кадра. Это обусловлено возможными ошибками в канале, потерями пакетов данных и другими причинами, следующими из реальных условий работы систем. Когда нужное количество узлов заполняет кворум записи, кадр заканчивается, и происходит задержка до следующего кадра. Фиксация успешно записанного обновления на узле происходит в конце слота, после чего оно может быть получено операцией чтения, которая может быть осуществлена в любом слоте во время задержки.

Источник осуществляет запись обновления с помощью многоадресной рассылки на все n узлов системы, но ожидает не менее w откликов с подтверждением успешной записи. Положительно ответившие узлы входят в подмножество W. Будем считать, что весь процесс записи на узел занимает один слот. Многоадресная передача не гарантирует своевременное и корректное получение информации узлом, следовательно, успешная доставка описывается вероятностью p. События успешной записи обновления реплики для разных узлов независимы. Попытка записи происходит в начале каждого слота. Процесс обновления считается завершенным после получения не менее w подтверждений от n узлов системы, при этом положительный ответ от узла засчитывается только один раз за все слоты кадра.

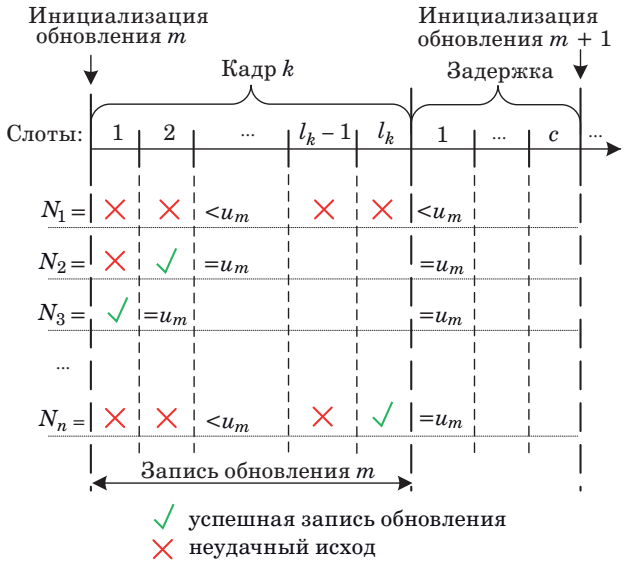


■ ***Рис. 1.*** Разделение времени работы системы на кадры и слоты
■ ***Fig. 1.*** Running time segmentation into frames and slots in the system

Таким образом, запись одного обновления может растягиваться на множество слотов, а после завершения кадра уникальных успешных записей на узлы может быть больше, чем w. После окончания текущего кадра инициализация нового обновления (появление следующего кадра) происходит только через c слотов, что обусловлено задержкой записи.

Рассмотрим процесс записи обновления более детально (рис. 2). При удачной перезаписи реплики на узле сохраняется временная метка обновления u_m (m — порядковый номер обновления), которая представляет момент, когда новая запись была инициирована. Отсчет времени начинается с запуска системы. Полная запись обновления занимает один кадр, после чего следует задержка длительностью c слотов перед началом нового кадра со следующим обновлением.

Рассмотрим процесс записи обновления с номером m в кадре k. Инициализация происходит в момент времени u_m. В каждом слоте осуществляется попытка записи обновления на все узлы системы с вероятностью p, что является показателем надежности доставки данных. При успешном получении данных временные метки узлов N_i, где $i \in \{1, 2, \ldots, n\}$ — номер узла системы, перезаписываются новой, соответствующей обновлению m, и хранятся до следующей перезаписи другим обновлением. Фиксация обновления на узле происходит сразу же в конце слота, в котором оно было получено, что дает возможность быть полученным запросом на чтение. Оно может быть произведено в любом слоте любого кадра, в том числе и в период задержки. Попытки записи предпринимаются до тех пор, пока не наберется в совокупности как минимум w узлов с последней версией данных.



■ ***Рис. 2.*** Процесс записи m-го обновления
■ ***Fig. 2.*** The process of writing the m-th update

Так как $w < n$, то к концу процесса обновления могут остаться узлы с более старой версией данных, например, как у N_1, куда обновление так и не смогло записаться (см. рис. 2). Внутри кадра находится l_k слотов, где k — номер кадра.

Получение информации с узлов осуществляется с помощью запросов на чтение, которые отправляются случайному набору узлов в количестве r, не превышающем общего количества узлов в системе. Эти r узлов образуют множество R, называемое кворумом чтения. Случайный выбор узлов отражает равномерное распределение нагрузки, что имеет место в реальных системах. По причине того, что на разных случайно выбранных узлах может содержаться информация разной свежести, среди них берется реплика с самой новой временной меткой. Чтение информации возможно только в конце слота. Операции чтения и записи производятся независимо друг от друга.

Узел, хранящий последнюю версию данных, называется согласованным. Если согласованный узел попал в кворум чтения, то и операция чтения станет согласованной, передав актуальную информацию. В кворумных системах существуют строгая и нестрогая согласованности. Нестрогая согласованность (или нестрогий кворум) описывает случай, когда кворумы записи и чтения могут не пересекаться, т. е. $w + r \le n$, и тогда гарантий получения последнего обновления операцией записи нет. Для строгой согласованности (или строгого кворума) кворумы записи и чтения должны пересекаться хотя бы в одном узле, т. е. $w + r > n$. Получение актуальных данных при этом будет гарантировано, поскольку кворумы записи и чтения будут содержать общие узлы.

Данное исследование посвящено анализу среднего возраста информации, который может быть получен с помощью запроса на чтение. Возраст информации $\Delta_i(t)$ для i-го узла в момент времени t определяется как разница между текущим временем t и меткой во времени $N_i(t)$ последнего обновления данного узла:

$$\Delta_i(t) = t - N_i(t). \tag{1}$$

Что касается запроса на чтения: возраст информации $\Delta(t)$ в момент времени t представляет собой наименьшее значение среди показателей устаревания r узлов, которые были задействованы в запросе:

$$\Delta(t) = \min(\Delta_1(t), \ldots, \Delta_r(t)). \tag{2}$$

Для вычисления среднего возраста информации $\overline{\Delta}$ применяется формула

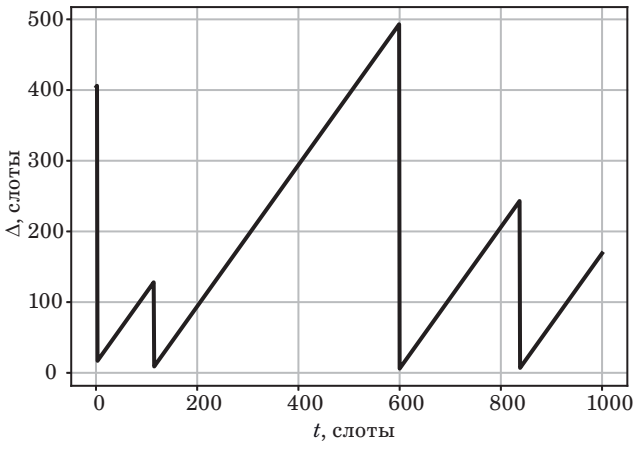
$$\overline{\Delta} = \lim_{T\to\infty} \frac{\int_0^T \Delta(t)\mathrm{d}t}{T}. \tag{3}$$

Представленная выше модель РСХД с равноправными узлами задается при помощи следующего набора переменных: n — общее число узлов в системе; w — число узлов, входящих в кворум записи; r — число узлов кворума чтения; p — вероятность успешного выполнения записи на узлы; c — число слотов задержки перед записью. Для демонстрации функционирования системы разработана имитационная модель в виде программного обеспечения.

Запросы на чтение с узла проводились в период после стабилизации системы, когда система проработала некоторое длительное время. Возраст информации $\Delta_i(t)$ рассчитывался согласно выражению (1). Возрастной процесс информации на узле (рис. 3) имеет сложный характер, следовательно, определение среднего возраста информации является отдельной задачей.

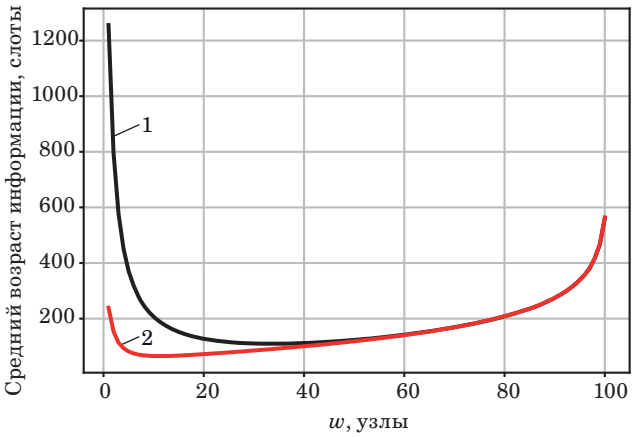
Зависимость среднего возраста информации от размера кворума записи w показана на рис. 4. На графиках определяются минимумы среднего возраста информации: для графика *1* — примерно в районе 35 узлов в кворуме записи, а для графика *2* минимум смещен и находится вблизи 11 узлов.

Средний возраст информации, получаемый из системы при большем числе узлов кворума чтения, оказался свежее. Такое поведение графиков с выраженным минимумом можно объяснить тем, что при малом числе w слишком мало узлов в конечном итоге получают обновление, из-за чего вероятность попадания таких узлов в кворум чтения R слишком низкая. При больших значениях w средний возраст информации увеличивается из-за излишне длительного процесса записи обновления, что переходит в ощутимую задержку до инициализации следующего обновления.



■ ***Рис. 3.*** Возраст информации по запросу на чтения с четвертого узла

■ ***Fig. 3.*** Age of information upon a read request from fourth node



■ ***Рис. 4.*** Зависимость среднего возраста информации от количества узлов w в кворуме записи при $r = 5$ (линия *1*) и $r = 25$ (линия *2*); $n = 100$, $p = 0{,}01$, $c = 100$

■ ***Fig. 4.*** Graph of the dependence of the average information age on the number of nodes in the write quorum w for $r = 5$ (line *1*) and $r = 25$ (line *2*); $n = 100$, $p = 0.01$, $c = 100$

Определение зависимости среднего возраста информации от параметров модели без имитационного моделирования

Утверждение 1. Длина кадра $X_{(w)}$ — это случайная величина, распределенная как w-я порядковая статистика из n случайных величин, распределенных по геометрическому закону с параметром p.

Доказательство:

Пусть появилось обновление, и нужно выполнить процесс записи. В каждую единицу времени источник рассылает обновление всем узлам, на которых еще не была выполнена успешная операция записи. Для каждого узла попытка операции записи является независимой и завершается успешно с вероятностью p. После успешной записи обновления узел больше не участвует в процессе записи. Весь цикл записи обновления продолжается до тех пор, пока не будет получено как минимум w подтверждений.

Для каждого узла $i = 1, \ldots, n$ введем случайную величину X_i — время (в единицах), которое потребовалось узлу для успешной записи. Величины X_i являются независимыми и имеют геометрическое распределение с параметром p.

Пусть $X_{(1)} \le X_{(2)} \le \ldots \le X_{(n)}$ — упорядоченные значения выборки $\{X_1, \ldots, X_n\}$. Тогда момент завершения процесса записи определяется величиной $X_{(w)}$ — w-й порядковой статистикой выборки объемом n. □

В данной работе математическое ожидание w-й порядковой статистики из n независимых геометрически распределенных случайных величин будет обозначаться как $\mu_{w:n}$, что является средней длиной кадра.

Утверждение 2. Математическое ожидание длины кадра может быть вычислено следующим образом:

$$\mu_{w:n} = \frac{(1-p)^n + \sum_{i=1}^{w-1} C_n^i p^i (1-p)^{n-i} (1+\mu_{w-i:n-i}) + \sum_{i=w}^{n} C_n^i p^i (1-p)^{n-i}}{1-(1-p)^n}, \quad (4)$$

а для первой итерации

$$\mu_{1:n} = \frac{1}{1-(1-p)^n}. \quad (5)$$

Доказательство:

Для нахождения среднего времени процесса записи нужно вычислить математическое ожидание w-й порядковой статистики из n независимых геометрически распределенных случайных величин $E[X_{(w)}]$.

В каждую единицу времени может быть три состояния:

1) не выполнена ни одна успешная операция записи. С вероятностью $C_n^0 p^0 (1-p)^n$ ни один узел не выполняет операцию записи. В этом случае затрачивается одна единица времени, и система остается в исходном состоянии;

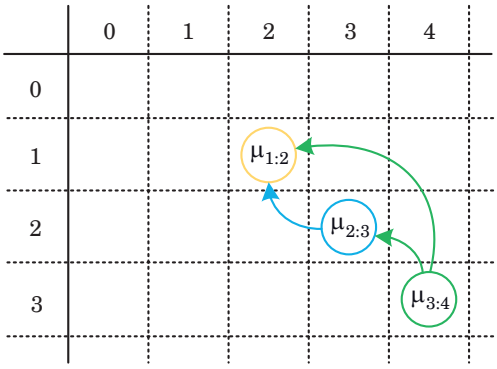
2) успешно выполнено i операций записи, где $0 < i < w$. В этом случае обновления были успешно записаны на i различных узлах с вероятностью $C_n^i p^i (1-p)^{n-i}$. Для завершения процесса записи требуется еще $w - i$ успешных операций записи по оставшимся $n - i$ узлам. Процесс продолжается с измененными параметрами;

3) успешно выполнено $i \geq w$ операций записи. Условие окончания процесса записи выполнено, цикл записи завершается, и текущее время фиксируется как случайная величина $X_{(w)}$. Событие происходит с вероятностью $C_n^i p^i (1-p)^{n-i}$.

Соответственно, для первой итерации формулы выражение примет вид

$$\mu_{1:n} = \frac{(1-p)^n + \sum_{i=1}^{n} C_n^i p^i (1-p)^{n-i}}{1-(1-p)^n} = \frac{1}{1-(1-p)^n}.$$

Таким образом, величина $X_{(w)}$ является временем достижения состояния, в котором успешно выполнено w и больше операций записи. □



■ ***Рис. 5.*** Процесс вычисления $\mu_{3:4}$

■ ***Fig. 5.*** $\mu_{3:4}$ calculating process

Полученная формула (4) является рекуррентной, и ее вычисление осуществляется с использованием метода динамического программирования. Каждой паре параметров w и n соответствует отдельная ячейка двумерного массива, в которую записывается значение $\mu_{w:n}$. Промежуточные значения $\mu_{1:n-w+1}$, $\mu_{2:n-w+2}$, …, $\mu_{w-1:n-1}$, $\mu_{w:n}$ последовательно вычисляются и сохраняются в массиве. Каждое новое значение $\mu_{w:n}$ определяется на основе ранее полученных результатов, и при его вычислении осуществляется обращение к уже заполненным ячейкам массива, что позволяет избежать повторных вычислений. В качестве иллюстрации на рис. 5 представлен процесс вычисления значения $\mu_{3:4}$:

$$\mu_{3:4} \sim \mu_{2:3} + \mu_{1:2},$$
$$\mu_{2:3} \sim \mu_{1:2}.$$

Пусть k — номер актуальной версии данных на текущий момент. Обозначим вероятность считывания последней на момент чтения версии данных запросом на чтение как $P_1 = \Pr\{\min(U_1, U_2, \ldots, U_r) = k\}$, где U_i — номер версии данных, полученных в результате i-го запроса на чтение после завершения текущего кадра. Соответственно, вероятность считывания предпоследней версии данных будет $P_2 = \Pr\{\min(U_1, U_2, \ldots, U_r) = k - 1\}$. Следовательно, в общем случае вероятность $P_i = \Pr\{\min(U_1, U_2, \ldots, U_r) = k - (i - 1)\}$, где i меняется в диапазоне от 1 до k.

Утверждение 3. Математическое ожидание среднего возраста информации $\bar{\Delta}$ для средней длины кадра $\mu_{w:n}$ при любых w и n

$$\bar{\Delta} = \left(\mu_{w:n} + \frac{c-1}{2}\right) + \sum_{i=2}^{\infty} P_i (i-1)(\mu_{w:n} + c). \quad (6)$$

Доказательство:

Пусть k — номер актуальной версии данных на текущий момент. По причине того, что система работает бесконечно долгое время, актуальная

версия может принимать любое неограниченное значение. Тогда, используя выражение (4), можно привести следующую цепочку рассуждений.

Исходя из описания работы системы, средний возраст информации в случае, когда операцией чтения считывается k-я версия данных, может быть вычислена как

$$\mu_{w:n} + \frac{c-1}{2},$$

для случая считывания $k-1$ версии данных

$$\mu_{w:n} + \frac{c-1}{2} + \mu_{w:n} + c,$$

для $k-2$ версии данных

$$\mu_{w:n} + \frac{c-1}{2} + 2\left(\mu_{w:n} + c\right).$$

Для версий $k-3$ и старее вычисление происходит аналогично.

Учитывая, что чтение каждой версии данных происходит с вероятностями P_1, P_2 и т. д., можно получить выражение для расчета среднего возраста информации

$$\overline{\Delta} = P_1\left(\mu_{w:n} + \frac{c-1}{2}\right) + P_2\left(\mu_{w:n} + \frac{c-1}{2} + \mu_{w:n} + c\right) + P_3\left(\mu_{w:n} + \frac{c-1}{2} + 2\left(\mu_{w:n} + c\right)\right) + \ldots$$

Упростим выражение:

$$\overline{\Delta} = \left(\mu_{w:n} + \frac{c-1}{2}\right) + \sum_{i=2}^{\infty} P_i\left(i-1\right)\left(\mu_{w:n} + c\right). \quad \square$$

Следует отметить, что значения вероятностей P_i вычисляются достаточно сложно. Далее будет показано, как можно построить верхнюю оценку для среднего возраста информации. С этой целью видоизменим правило работы системы: будем предполагать, что для видоизмененной системы обновление к концу кадра получает ровно w узлов. Учитывая, что в исходной системе обновление может получить больше, чем w узлов, средний возраст информации для видоизмененной системы будет больше, чем для исходной.

Обозначим через $\hat{P}_1$ вероятность считывания последней на момент чтения версии данных. В общем случае, используя рассуждения, которые вводились для исходной системы, через $\hat{P}_i$ обозначим то, что в результате r запросов на чтение номер самой актуальной версии равен $k-(i-1)$, где k — номер актуальной версии.

Утверждение 4. Для видоизмененной системы вероятности $\hat{P}_i$ рассчитываются следующим образом:

$$\hat{P}_i = q^{i-1}\left(1-q\right), \tag{7}$$

где q — вероятность того, что при чтении обращение будет относиться к узлам, на которых нет новой версии:

$$q = \prod_{i=0}^{r-1} \frac{n-w-i}{n-i}. \tag{8}$$

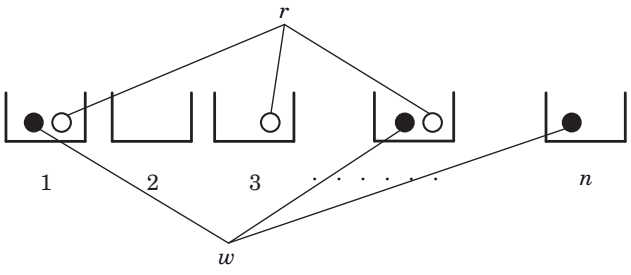
Доказательство:

Из описания работы видоизмененной модели следует, что после завершения обновления из n узлов в системе ровно w узлов будут иметь последнюю версию информации. Таким образом, если W — это множество узлов, получивших обновление, а R — это множество узлов, с которых производится чтение, то вероятность $\hat{P}_i$ можно записать как $\hat{P}_i = \Pr\{R \subset W\}$.

Рассмотрим рис. 6. Пусть имеется n ящиков. В ящики случайно помещаются w черных шаров и r белых шаров. В данной интерпретации ящики обозначают узлы, черные шары — запись нового обновления, а белые шары — операцию чтения.

Вероятность того, что первый белый шар не попадет в ящик с черным шаром, равна $\frac{n-w}{n}$; для второго белого шара $\frac{n-1-w}{n-1}$; для третьего белого шара $\frac{n-2-w}{n-2}$, и далее аналогично. Таким образом, получим полное выражение для q:

$$q = \frac{n-w}{n} \cdot \frac{n-1-w}{n-1} \cdot \frac{n-2-w}{n-2} \cdot \ldots \cdot \frac{n-(r-1)-w}{n-(r-1)} = \prod_{i=0}^{r-1} \frac{n-w-i}{n-i}. \quad \square$$



■ ***Рис. 6.*** Иллюстрация к задаче вычисления оценки снизу вероятности того, что W и R не пересекутся

■ ***Fig. 6.*** Illustration for the problem of computing a lower bound on the probability that W and R do not intersect

Используя полученную вероятность чтения последней на момент чтения версии данных (7) и выражение (6) из утверждения 3, можно получить выражение для точного вычисления среднего возраста информации для видоизмененной модели, которое также является оценкой сверху для исходной модели.

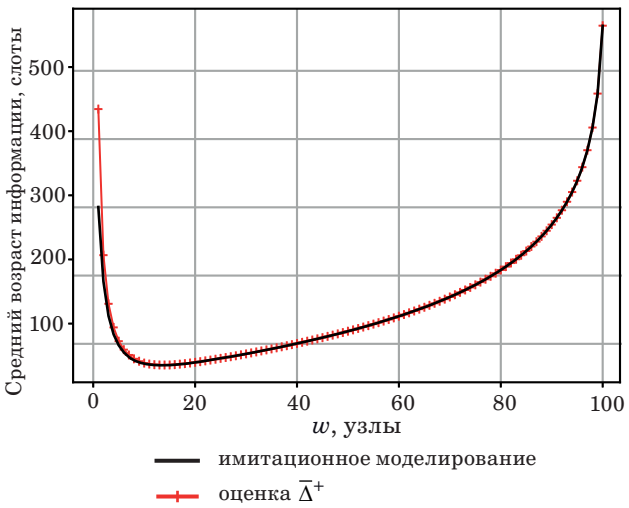
Утверждение 5. Выражение для вычисления точного значения математического ожидания среднего возраста информации $\overline{\Delta}^{+}$ для средней длины кадра $\mu_{w:n}$ при любых w и n в видоизмененной модели

$$\overline{\Delta}^{+} = \left(\mu_{w:n} + \frac{c-1}{2}\right) + \sum_{i=2}^{\infty} \hat{P}_i\left(i-1\right)\left(\mu_{w:n} + c\right). \quad (9)$$

Средний возраст информации согласно формуле (9), что является оценкой сверху для исходной модели, и средний возраст информации, полученный имитационным моделированием, показаны на рис. 7.

Из графиков видно, что значения очень близки при всех w, следующих после некоторого оптимального значения размера кворума записи, соответствующего минимуму среднего возраста информации. До оптимума же наблюдается небольшое расхождение.

Далее будет сформулирована оптимизационная задача для получения оптимального размера кворума, при котором средний возраст информации будет минимальным.



■ ***Рис. 7.*** Зависимость среднего возраста информации, полученного имитационным моделированием и его оценкой сверху, от размера кворума записи

■ ***Fig. 7.*** Graphs of the average age of information obtained by simulation modeling and its upper bound as a function of the write quorum size

Выбор размера кворума записи

При определенных значениях размера кворума записи w средний возраст информации может принимать некоторое минимальное значение. Наличие минимума объясняется тем, что при слишком малом размере кворума записи в конце кадров числа узлов, получивших последнюю версию данных, недостаточны, чтобы регулярно получать самую последнюю информацию операцией чтения, следовательно, средний возраст информации увеличивается. При слишком большом размере кворума записи увеличивается размер кадра вследствие того, что успешная запись происходит лишь с некоторой вероятностью. Этот эффект обусловлен тем, что кадр увеличивается, а значит, проходит больше времени с момента инициализации этого обновления, поэтому средний возраст также растет. Таким образом, есть некоторые оптимальные значения размера кворума записи, при которых средний возраст информации будет минимальным.

Выбор размера кворума записи можно сформулировать в виде оптимизационной задачи по минимизации среднего возраста информации, где w может принимать значения от 1 до n при заданных значениях параметров n и c:

$$w_{\text{opt}} = \arg\min_{w} \overline{\Delta}\left(w, n, c\right). \quad (10)$$

Значения среднего возраста информации $\overline{\Delta}(w, n, c)$ могут быть получены с помощью имитационного моделирования с любой заданной точностью, однако это требует больших вычислительных затрат.

Выше был описан способ вычисления верхней оценки для среднего возраста информации (9). Для верхней оценки можно сформулировать следующую оптимизационную задачу:

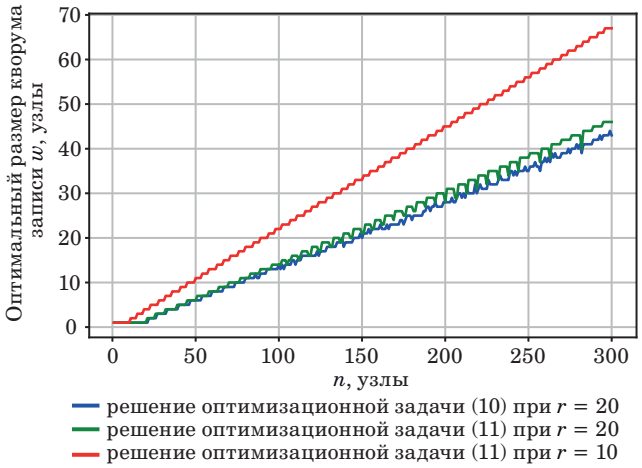
$$\hat{w}_{\text{opt}} = \arg\min_{w} \overline{\Delta}^{+}\left(w, n, c\right). \quad (11)$$

Для решения оптимизационных задач (10) и (11) можно использовать полный перебор w или одну из процедур одномерного поиска минимума, такую, как деление отрезка пополам, золотое сечение или числа Фибоначчи.

Далее будут рассмотрены результаты решения оптимизационной задачи (10) с использованием имитационного моделирования и результаты численного решения оптимизационной задачи (11).

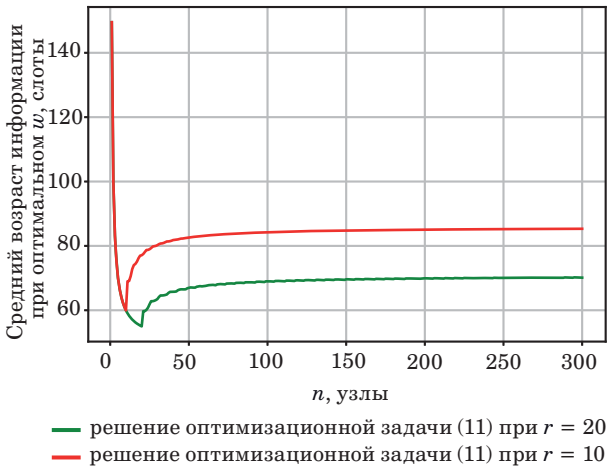
Численные результаты

Оптимальное число узлов кворума записи в зависимости от общего числа узлов в системе получено с помощью решений оптимизационных



■ ***Рис. 8.*** Зависимость оптимального числа узлов кворума записи w от общего числа узлов n в системе

■ ***Fig. 8.*** Graphs of the optimal number of write quorum nodes w, as a function of the total number of nodes in the system n



■ ***Рис. 9.*** Зависимость среднего возраста информации в условиях оптимального кворума от n

■ ***Fig. 9.*** Graphs of the average age of information under optimal quorum as a function of n

задач (10) и (11) (рис. 8). Для вычислений использовались параметры: $r = 20$, $p = 0{,}01$, $c = 100$. Отдельно были посчитаны значения для $r = 10$. Параметр n принимал значения от 1 до 300. Для получения решения оптимизационной задачи (10) использовалось моделирование с одним миллионом экспериментов.

По мере роста числа n заметен рост числа узлов кворума записи, однако зависимости не являются монотонно возрастающими. В начале графиков наблюдается оптимальное число узлов кворума записи w, равное 1, что обусловливается явлением строгого кворума. В этом случае операцией чтения всегда будет получена самая актуальная версия данных, поскольку хотя бы один узел, с которого производится чтение, имеет последнее обновление. Также наблюдается отклонение значений, полученных с помощью (10) и (11) при $r = 20$. Наибольшее расхождение между значениями не превышает трех узлов. Такое расхождение может быть вызвано близкими значениями среднего возраста информации в области его минимума. Данные расхождения практически не влияют на средний возраст информации, рассчитанный с использованием оптимальных значений размера кворума записи, полученного решениями оптимизационных задач (10) и (11). При меньшем размере кворума чтения оптимальное число узлов кворума записи растет быстрее по мере увеличения n, что можно видеть на графике при $r = 10$.

На рис. 9 рассматривается средний возраст информации в условиях оптимального кворума в зависимости от n, согласно полученным данным, показанным на рис. 8 для выражения (11).

Средний возраст информации при оптимальных значениях w, полученных имитационным моделированием для выражения (10), не показан на рис. 9, так как он практически полностью совпадает в данном масштабе графиков с выражением (11). Максимальное расхождение между данными значениями среднего возраста информации не превышает 0,7, что можно считать несущественным. У графиков наблюдается выраженный минимум при $n = 20$ для графика с $r = 20$. До данного значения $r = n = 20$ при малом n дольше набираются необходимые w успешных подтверждений записи, из-за чего растягивается средняя длина кадра, а это влечет больший средний возраст информации. Когда r становится меньше n, то появляется вероятность, что среди случайно выбранных r узлов не окажется ни одного узла с последней версией данных, из-за чего также может повышаться средний возраст информации. Следовательно, образуется минимум, который видно на графике. Для графика при $r = 10$ аналогично.

Таким образом, наглядно продемонстрированы основные особенности работы системы в условиях оптимального кворума записи в зависимости от других параметров системы.

Заключение

Рассмотрена реплицируемая система хранения данных на основе равноправных узлов. Отмечено, что отличительной особенностью такой системы является наличие так называемых кворумов чтения и записи, которые представляют множества узлов, с которых происходит считывание данных

и запись обновления соответственно. Предложена модель, отражающая основные особенности реплицируемой системы хранения данных с кворумами чтения и записи. В предложенной модели время работы разделено на кадры и слоты, а запись обновления на узлы происходит с вероятностью p и завершается при получении не менее w подтверждений. В качестве показателя актуальности данных рассмотрен средний возраст информации, получаемый запросом на чтение. Показано, что длина кадра является случайной величиной, распределение которой соответствует w-й порядковой статистике из n независимых геометрически распределенных случайных величин с параметром p. Для ее математического ожидания выведена рекуррентная формула и предложен метод динамического программирования. Сформулирована оптимизационная задача выбора размера кворума записи, минимизирующего средний возраст информации. На основе исходной модели предложена видоизмененная модель, в которой к концу кадра обновление записывается ровно на w узлов, что позволило упростить вычисления и получить оценку сверху для среднего возраста информации. Численные результаты показали, что оптимальный размер кворума записи растет с увеличением общего числа узлов, а оценка сверху хорошо согласуется с имитационным моделированием; выявлено наличие минимума среднего возраста информации при оптимальном кворуме записи в зависимости от общего числа узлов в системе. Модель может быть использована при проектировании реплицируемых систем хранения данных для соблюдения баланса согласованности и доступности. Важным допущением является независимость успешной доставки обновления на разные узлы; в реальных системах при многоадресной передаче это может не выполняться, что требует дальнейшего исследования и учета зависимости между событиями доставки.

Финансовая поддержка

Исследование выполнено при финансовой поддержке Российского научного фонда, грант № 22-19-00305 «Пространственно-временные стохастические модели беспроводных сетей с большим числом абонентов».

Литература

1. **Богатырев В. А., Богатырев С. В., Богатырев А. В.** Граничная оценка надежности кластерных систем на основе декомпозиции марковской модели при ограниченном восстановлении узлов с накоплением отказов. *Научно-технический вестник информационных технологий, механики и оптики*, 2025, т. 25, № 3, с. 574–583. doi:10.17586/2226-1494-2025-25-3-574-583, EDN: QQJPSJ
2. **Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V.** Recovery of real-time clusters with the division of computing resources into the execution of functional queries and the restoration of data generated since the last backup. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2024, vol. 14123, pp. 236–250. doi:10.1007/978-3-031-50482-2_19
3. **Najjar A., Mokadem R., Pierson J. M.** A review of data placement and replication strategies based on machine learning. *2024 IEEE 30th International Conference on Parallel and Distributed Systems (ICPADS)*, IEEE, 2024, pp. 278–285. doi:10.1109/ICPADS63004.2024.00042
4. **Mastromauro L., Andrade D. S., Ozmen M. O., Kinsy M. A.** Survey of attacks and defenses on consensus algorithms for secure data replication in distributed systems. *IEEE Access*, 2025, vol. 13, pp. 143631–143667. doi:10.1109/ACCESS.2025.3597260
5. **Sevin A.** Implementation of a data-parallel approach on a lightweight hash function for IoT devices. *Mathematics*, 2025, vol. 13, no. 5, pp. 734. doi:10.3390/math13050734
6. **Noor S., Awan H. H., Hashmi A. S., Saeed A., Khan S., AlQahtani S. A.** Optimizing performance of parallel computing platforms for large-scale genome data analysis. *Computing*, 2025, vol. 107, no. 3, pp. 86. doi:10.1007/s00607-025-01441-y
7. **Patel P.** Dynamic CAP optimization in distributed databases via adaptive graph neural networks with causal inference. *Engineering Archive*, 2025, pp. 1–14. doi:10.31224/4825
8. **Borrill P.** What distributed computing got wrong: The category mistake that turned design choices into laws of nature. *arXiv preprint*, 2026, arXiv:2602.18723, pp. 1–28. doi:10.48550/arXiv.2602.18723
9. **Wright C. S.** Resolving CAP through automata-theoretic economic design: A unified mathematical framework for real-time partition-tolerant systems. *arXiv preprint*, 2025, arXiv:2507.02464, pp. 1–51. doi:10.48550/arXiv.2507.02464
10. **Song Y., Liu C., Shou M. Z.** Omniconsistency: Learning style-agnostic consistency from paired stylization data. *Advances in Neural Information Processing Systems*, 2026, vol. 38, pp. 173300–173322. doi:10.52202/085713-5216
11. **Olivieri L., Negrini L., Arceri V., Ferrara P., Cortesi A.** Detection of read-write issues in hyperledger fabric smart contracts. *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, 2025, pp. 329–337. doi:10.1145/3672608.3707721

12. **Desai M., Quinn R., Asadinia M.** SMART-WRITE: adaptive learning-based write energy optimization for phase change memory. *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2025, pp. 00640–00648. doi:10.1109/CCWC62904.2025.10903957
13. **Behrouzi-Far A., Soljanin E., Yates R. D.** Data freshness in leader-based replicated storage. *2020 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2020, pp. 1806–1811. doi:10.1109/ISIT44484.2020.9174411
14. **Крылов Д. Р., Пойманова Е. Д., Тюрликов А. М.** Модель реплицируемой системы хранения данных с использованием среднего возраста информации в качестве показателя актуальности данных. *Информационно-управляющие системы*, 2024, № 3, с. 11–23. doi:10.31799/1684-8853-2024-3-11-23, EDN: XSSHJI
15. **Elhemali M., Gallagher N., Gordon N., Idziorek J., Krog R., Lazier C., Mo E., Mritunjai A., Perianayagam S., Rath T., Sivasubramanian S., Sorenson J. C. III, Sosothikul S., Terry D., Vig A.** Amazon DynamoDB: A scalable, predictably performant, and fully managed NoSQL database service. *2022 USENIX Annual Technical Conference (USENIX ATC 22)*, 2022, pp. 1037–1048.
16. **Sagan M., Plechawska-Wójcik M.** Comparative analysis of non-relational databases on the example of Amazon DynamoDB and MongoDB. *Journal of Computer Sciences Institute*, 2026, vol. 39, pp. 108–114. doi:10.35784/jcsi.8549
17. **Golec M., Zhang Z., Wang H., Golec M., Singh R., Gill S. S.** Google cloud spanner-based data management application for smart gaming industry. *Computational Intelligence Techniques for 5G Enabled IoT Networks*, Cham, Springer Nature Switzerland, 2025, pp. 49–59. doi:10.1007/978-3-031-82733-4_4
18. **Zhu X., Nie X., Liu J.** Time series database optimization based on InfluxDB. *2023 International Conference on Power, Electrical Engineering, Electronics and Control (PEEEC)*, IEEE, 2023, pp. 879–885. doi:10.1109/PEEEC60561.2023.00172
19. **Ruan C., Zhang Y., Zhang J., Li C., Ma X., Chen H., Zhou J., Li F., Yang X.** PolyBase: Adapting to data affinity changes in geo-replicated database via row-level consensus-group affiliation re-assignment. *Proceedings of the VLDB Endowment*, 2024, vol. 18, no. 3, pp. 702–714. doi:10.14778/3712221.3712236
20. **Naseri Seyedi Noudoust N., Adabi S., Rezaee A.** A quorum-based data consistency approach for non-relational database. *Cluster Computing*, 2022, vol. 25, no. 2, pp. 1515–1540. doi:10.1007/s10586-021-03531-w
21. **Zhong J., Yates R. D., Soljanin E.** Minimizing content staleness in dynamo-style replicated storage systems. *IEEE INFOCOM 2018 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2018, pp. 361–366. doi:10.1109/INFCOMW.2018.8406971
22. **Yates R. D., Sun Y., Brown D. R., Kaul S. K., Modiano E., Ulukus S.** Age of information: An introduction and survey. *IEEE Journal on Selected Areas in Communications*, 2021, vol. 39, no. 5, pp. 1183–1210. doi:10.1109/JSAC.2021.3065072
23. **Qu Y., Chen Z., Pappas N., Tang C., Wang M., Quek T. Q. S.** Analysis of age of information for a discrete-time dual-queue system. *IEEE Transactions on Communications*, 2025, vol. 73, no. 11, pp. 10855–10870. doi:10.1109/TCOM.2025.11015332
24. **Zhang C., Wang L., Xiao L., Jiang S., Han M., Wang J., Wei B., Qin G.** Minimizing the cost of periodically replicated systems via model and quantitative analysis. *Frontiers of Computer Science*, 2024, vol. 18, no. 5, art. 185206. doi:10.1007/s11704-023-2625-8

UDC 004.62, 004.7
doi:10.31799/1684-8853-2026-5-73-84
EDN: CWRBDL

Average age of information in distributed data storage systems with peer nodes

D. R. Krylov[a], Post-Graduate Student, orcid.org/ 0009-0008-5901-5342
U. A. Bolotskikh[a], Master Student, orcid.org/0009-0009-0733-594X
A. M. Turlikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7132-094X, turlikov@vu.spb.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Distributed data storage systems can employ leader and follower nodes or peer nodes. For systems with peer nodes, researchers have given little attention to how system parameters affect a performance metric such as average age of information; therefore, investigating this effect is a pressing task. **Purpose:** To develop a model of a replicated data storage system with peer nodes that allows formulating and solving the problem of minimizing average age of information by choosing write quorum size. **Results:** We propose a model that reflects the main operational features of replicated data storage systems with peer nodes, to which the system multicasts an update over an unreliable channel. Successful update delivery events occur independently for different nodes. One of the model parameters is the probability of successful update delivery. We specify a method for calculating an upper bound for the average age of information. We compare this bound with simulation modeling and show that it differs from the exact value by no more than 1%. We formulate and solve an optimization problem that selects the write quorum size to minimize the average age of information. Numerical results show that the optimal write quorum size grows as the total number of nodes increases. We obtain the dependence of the average age of information on the total number of nodes for the optimal write quorum size and fixed other model parameters. We note that this dependence has a minimum. **Practical relevance:** The proposed model reflects the general features of replicated data storage systems with peer nodes, and engineers can apply it when designing real systems to maintain a balance between consistency and availability. **Discussion:** The model relies on a key assumption: successful update delivery to different nodes is independent. In real systems with multicast transmission this assumption may fail, so further research should account for dependence between delivery events.

Keywords — average age of information, data storage, replication, read quorum, write quorum.

For citation: Krylov D. R., Bolotskikh U. A., Turlikov A. M. Average age of information in distributed data storage systems with peer nodes. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 73–84 (In Russian). doi:10.31799/1684-8853-2026-5-73-84, EDN: CWRBDL

Financial support

The research was carried out with financial support from the Russian Science Foundation, grant No. 22-19-00305 “Spatiotemporal stochastic models of wireless networks with a large number of subscribers”.

References

1. Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V. Boundary estimation of the reliability of cluster systems based on the decomposition of the Markov model with limited recovery of nodes with accumulated failures. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 3, pp. 574–583. doi:10.17586/2226-1494-2025-25-3-574-583, EDN: QQJPSJ
2. Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V. Recovery of real-time clusters with the division of computing resources into the execution of functional queries and the restoration of data generated since the last backup. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2024, vol. 14123, pp. 236–250. doi:10.1007/978-3-031-50482-2_19
3. Najjar A., Mokadem R., Pierson J. M. A review of data placement and replication strategies based on machine learning. *2024 IEEE 30th International Conference on Parallel and Distributed Systems (ICPADS)*, IEEE, 2024, pp. 278–285. doi:10.1109/ICPADS63004.2024.00042
4. Mastromauro L., Andrade D. S., Ozmen M. O., Kinsy M. A. Survey of attacks and defenses on consensus algorithms for secure data replication in distributed systems. *IEEE Access*, 2025, vol. 13, pp. 143631–143667. doi:10.1109/ACCESS.2025.3597260
5. Sevin A. Implementation of a data-parallel approach on a lightweight hash function for IoT devices. *Mathematics*, 2025, vol. 13, no. 5, pp. 734. doi:10.3390/math13050734
6. Noor S., Awan H. H., Hashmi A. S., Saeed A., Khan S., AlQahtani S. A. Optimizing performance of parallel computing platforms for large-scale genome data analysis. *Computing*, 2025, vol. 107, no. 3, pp. 86. doi:10.1007/s00607-025-01441-y
7. Patel P. Dynamic CAP optimization in distributed databases via adaptive graph neural networks with causal inference. *Engineering Archive*, 2025, pp. 1–14. doi:10.31224/4825
8. Borrill P. What distributed computing got wrong: The category mistake that turned design choices into laws of nature. *arXiv preprint*, 2026, arXiv:2602.18723, pp. 1–28. doi:10.48550/arXiv.2602.18723
9. Wright C. S. Resolving CAP through automata-theoretic economic design: A unified mathematical framework for real-time partition-tolerant systems. *arXiv preprint*, 2025, arXiv:2507.02464, pp. 1–51. doi:10.48550/arXiv.2507.02464
10. Song Y., Liu C., Shou M. Z. Omniconsistency: Learning style-agnostic consistency from paired stylization data. *Advances in Neural Information Processing Systems*, 2026, vol. 38, pp. 173300–173322. doi:10.52202/085713-5216
11. Olivieri L., Negrini L., Arceri V., Ferrara P., Cortesi A. Detection of read-write issues in hyperledger fabric smart contracts. *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, 2025, pp. 329–337. doi:10.1145/3672608.3707721
12. Desai M., Quinn R., Asadinia M. SMART-WRITE: adaptive learning-based write energy optimization for phase change memory. *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2025, pp. 00640–00648. doi:10.1109/CCWC62904.2025.10903957
13. Behrouzi-Far A., Soljanin E., Yates R. D. Data freshness in leader-based replicated storage. *2020 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2020, pp. 1806–1811. doi:10.1109/ISIT44484.2020.9174411
14. Krylov D. R., Poymanova E. D., Turlikov A. M. Modeling a replicated storage system with the use of the average age of information as an indicator of data relevance. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 3, pp. 11–23 (In Russian). doi:10.31799/1684-8853-2024-3-11-23, EDN: XSSHJI
15. Elhemali M., Gallagher N., Gordon N., Idziorek J., Krog R., Lazier C., Mo E., Mritunjai A., Perianayagam S., Rath T., Sivasubramanian S., Sorenson J. C. III, Sosothikul S., Terry D., Vig A. Amazon DynamoDB: A scalable, predictably performant, and fully managed NoSQL database service. *2022 USENIX Annual Technical Conference (USENIX ATC 22)*, 2022, pp. 1037–1048.
16. Sagan M., Plechawska-Wójcik M. Comparative analysis of non-relational databases on the example of Amazon DynamoDB and MongoDB. *Journal of Computer Sciences Institute*, 2026, vol. 39, pp. 108–114. doi:10.35784/jcsi.8549
17. Golec M., Zhang Z., Wang H., Golec M., Singh R., Gill S. S. Google cloud spanner-based data management application for smart gaming industry. *Computational Intelligence Techniques for 5G Enabled IoT Networks*, Cham, Springer Nature Switzerland, 2025, pp. 49–59. doi:10.1007/978-3-031-82733-4_4
18. Zhu X., Nie X., Liu J. Time series database optimization based on InfluxDB. *2023 International Conference on Power, Electrical Engineering, Electronics and Control (PEEEC)*, IEEE, 2023, pp. 879–885. doi:10.1109/PEEEC60561.2023.00172
19. Ruan C., Zhang Y., Zhang J., Li C., Ma X., Chen H., Zhou J., Li F., Yang X. PolyBase: Adapting to data affinity changes in geo-replicated database via row-level consensus-group affiliation re-assignment. *Proceedings of the VLDB Endowment*, 2024, vol. 18, no. 3, pp. 702–714. doi:10.14778/3712221.3712236
20. Naseri Seyedi Noudoust N., Adabi S., Rezaee A. A quorum-based data consistency approach for non-relational database. *Cluster Computing*, 2022, vol. 25, no. 2, pp. 1515–1540. doi:10.1007/s10586-021-03531-w
21. Zhong J., Yates R. D., Soljanin E. Minimizing content staleness in dynamo-style replicated storage systems. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2018, pp. 361–366. doi:10.1109/INFCOMW.2018.8406971
22. Yates R. D., Sun Y., Brown D. R., Kaul S. K., Modiano E., Ulukus S. Age of information: An introduction and survey. *IEEE Journal on Selected Areas in Communications*, 2021, vol. 39, no. 5, pp. 1183–1210. doi:10.1109/JSAC.2021.3065072
23. Qu Y., Chen Z., Pappas N., Tang C., Wang M., Quek T. Q. S. Analysis of age of information for a discrete-time dual-queue system. *IEEE Transactions on Communications*, 2025, vol. 73, no. 11, pp. 10855–10870. doi:10.1109/TCOM.2025. 11015332
24. Zhang C., Wang L., Xiao L., Jiang S., Han M., Wang J., Wei B., Qin G. Minimizing the cost of periodically replicated systems via model and quantitative analysis. *Frontiers of Computer Science*, 2024, vol. 18, no. 5, art. 185206. doi:10.1007/s11704-023-2625-8

УДК 004.032.26; 616.12-073.7
doi:10.31799/1684-8853-2026-5-85-95
EDN: CSPEWE

Научные статьи
Articles

Применение сверточной нейронной сети InceptionTime для классификации электрокардиограмм с множественными метками

В. М. Чубич[a], *доктор техн. наук, профессор, orcid.org/0000-0003-2006-0046, chubich@ami.nstu.ru*
Е. С. Коцелап[a], *студентка, orcid.org/0009-0008-6142-3580*
[a]*Новосибирский государственный технический университет, К. Маркса пр., 20, Новосибирск, 630073, РФ*

Введение: *проблема классификации электрокардиограмм с множественными метками возникает по причине того, что одной записи могут соответствовать несколько диагнозов. Поскольку редкие диагнозы представлены в меньшем количестве, а их признаки проявляются на участках различной длины, использование единого масштаба анализа и общего порога решения повышает риск смещения модели к частым состояниям и пропуска редких патологий.* ***Цель:*** *адаптировать и экспериментально исследовать одномерную сверточную нейронную сеть InceptionTime для классификации электрокардиограмм с множественными метками.* ***Результаты:*** *разработанная схема классификации электрокардиограмм сочетает многомасштабное извлечение признаков, взвешенную бинарную кросс-энтропию с логитами и индивидуальные пороги для пяти диагностических суперклассов. Экспериментальная проверка, проведенная на наборе десятисекундных двенадцатиканальных электрокардиограмм, включавшем записи без патологий, с инфарктом миокарда, изменениями реполяризации, нарушениями проводимости и гипертрофией, выявила, что на тестовой выборке полнота составила 0,74, а макроусредненная гармоническая мера точности и полноты — 0,72. Сравнение с рекуррентными и сверточными архитектурами показало, что модель на основе архитектуры InceptionTime обеспечила наибольшую полноту и продемонстрировала один из лучших результатов по макроусредненной гармонической мере точности и полноты.* ***Практическая значимость:*** *адаптированная модель может служить алгоритмической основой программного модуля предварительного анализа электрокардиограмм и систем поддержки врачебных решений. Независимая оценка диагностических состояний позволяет выявлять несколько патологий в одной записи, а применение отдельных порогов для каждого класса — снижать риск пропуска редких патологий и предварительно выделять записи для последующей проверки специалистом.* ***Обсуждение:*** *дальнейшие исследования целесообразно направить на повышение качества распознавания редких диагностических классов и проверку модели на других биомедицинских сигналах (анализ электроэнцефалограмм, оценка уровня стресса и эмоций человека и др.).*

Ключевые слова *— сверточная нейронная сеть, InceptionTime, глубокое обучение, бинарная кросс-энтропия, электрокардиография, дисбаланс классов, классификация с множественными метками, диагностика сердечно-сосудистых заболеваний.*

Для цитирования: Чубич В. М., Коцелап Е. С. Применение сверточной нейронной сети InceptionTime для классификации электрокардиограмм с множественными метками. *Информационно-управляющие системы*, 2026, № 5, с. 85–95. doi:10.31799/1684-8853-2026-5-85-95, EDN: CSPEWE

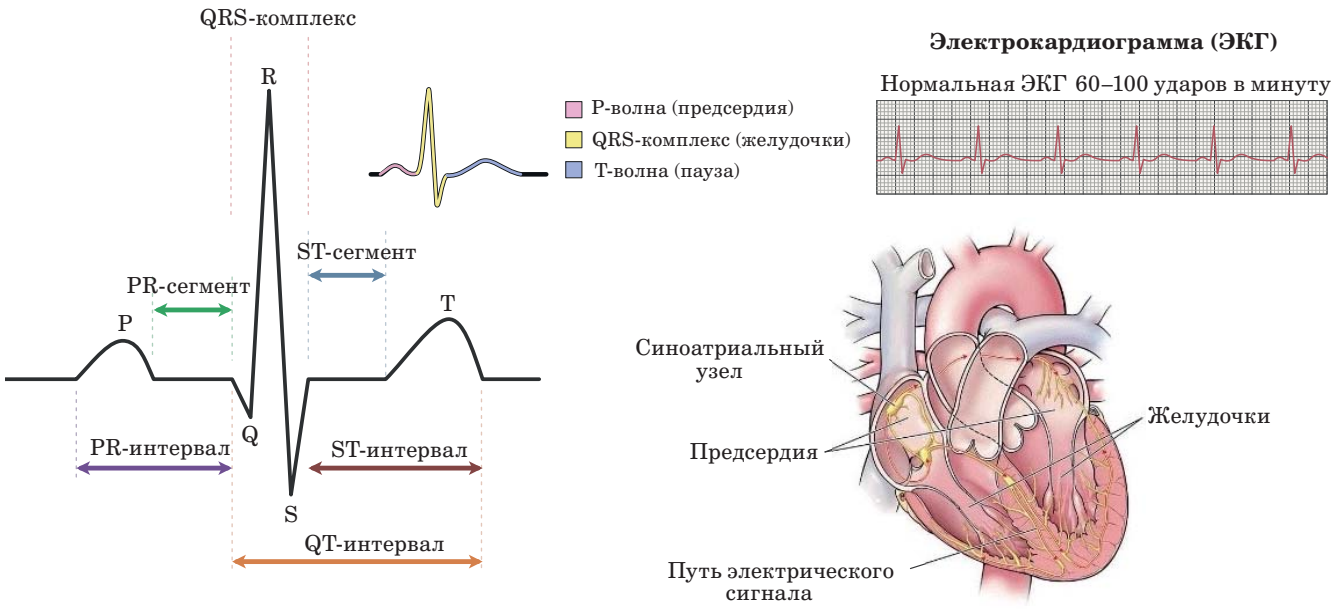
For citation: Chubich V. M., Kotselap E. S. Application of the InceptionTime convolutional neural network to multi-label classification of electrocardiograms. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 85–95 (In Russian). doi:10.31799/1684-8853-2026-5-85-95, EDN: CSPEWE

Введение

По оценкам Всемирной организации здравоохранения, сердечно-сосудистые заболевания являются одной из основных причин смертности во всем мире (https://www.who.int/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds)). Ранняя и точная диагностика является важным фактором для своевременного медицинского вмешательства и снижения летальности. Электрокардиография традиционно выступает наиболее распространенным, неинвазивным и доступным методом оценки функционального состояния сердца.

Стандартный кардиоцикл (рис. 1) состоит из нескольких ключевых элементов (зубцов P, Q, R, S, T и соответствующих интервалов), каждый из которых отражает определенный этап электрической активности миокарда. Тем не менее ручная интерпретация записей электрокардиограмм (ЭКГ) требует высокой квалификации врачей-кардиологов, подвержена субъективности решений и является крайне трудоемким процессом, особенно в условиях постоянного роста объемов цифровых медицинских данных.

В настоящее время методы машинного и глубокого обучения успешно используются в задачах анализа биомедицинских сигналов [1–3] и являются одним из основных направлений автоматического анализа ЭКГ [4, 5]. Проведенные исследования показывают возможность применения глубоких нейронных сетей как для распознавания нарушений ритма по одноканальным амбулаторным ЭКГ [6], так и для диагностики состояний по 12-канальным записям ЭКГ [7]. В более поздних исследованиях рассматриваются задачи интерпретации ЭКГ, классификации нарушений ритма и применения нейросетевых моделей для диагностики сердечно-сосудистых заболеваний [8–10].



■ ***Рис. 1.*** Структура нормального ЭКГ-сигнала и путь электрического импульса в сердце
■ ***Fig. 1.*** Structure of a normal ECG signal and the path of the electrical impulse in the heart

Часто при анализе одномерных временных рядов ЭКГ в качестве базовых подходов используют рекуррентные нейронные сети (RNNs). В [11] проведено сравнение базовой RNN, Long Short-Term Memory (LSTM) и Gated Recurrent Unit (GRU) для классификации ЭКГ. Рекуррентные нейронные сети читают сигнал последовательно, из-за чего плохо улавливают признаки на длинных записях ЭКГ. В [12, 13] показано, что применение сверточных нейронных сетей (CNN) позволяет эффективно улавливать как локальные изменения в форме кардиоцикла (например, подъем сегмента ST при инфаркте), так и глобальные нарушения ритма. В [14] рассмотрена гибридная архитектура CNN-BiLSTM (такие модели часто оказываются сложнее в реализации и требуют большего числа вычислительных ресурсов).

Альтернативой выступают сверточные нейронные сети InceptionTime, которые опираются на идею параллельного извлечения признаков фильтрами разного размера [15]. В [16] описана архитектура InceptionTime, использованная для классификации временных рядов. В сравнительных экспериментах [16] InceptionTime продемонстрировала качество классификации, сопоставимое с HIVE-COTE, при существенно лучшей масштабируемости по объему и длине временных рядов. В работе [17] предложена сверточная модель для классификации ЭКГ Multireceptive Field CNN (MRF-CNN), в которой несколько размеров рецептивного поля помогают учитывать как короткие, так и более протяженные участки сигнала.

В данной работе выбрана архитектура InceptionTime, поскольку она специально разработана для классификации временных рядов, сочетает многомасштабную обработку с остаточными связями и уже применяется в InceptionTime-подобных подходах к анализу ЭКГ [18, 19]. Для ЭКГ такой подход особенно полезен, поскольку диагностические признаки могут проявляться как в коротких элементах сигнала, например в QRS-комплексе, так и в более протяженных изменениях сегмента ST и зубца T.

Для успешного обучения глубоких нейронных сетей требуются крупные и качественно размеченные медицинские наборы данных. Одним из наиболее популярных ресурсов для исследования алгоритмов автоматической диагностики является PTB-XL [20]. В сравнительном исследовании методов глубокого обучения на PTB-XL [21] ResNet- и Inception-подобные сверточные архитектуры показали одни из наиболее высоких результатов среди рассмотренных подходов к анализу ЭКГ. Данный набор включает 12-канальные записи ЭКГ длительностью 10 с и содержит диагностические метки, сформированные с использованием Standard Communications Protocol for Computerized Electrocardiography (SCP-ECG). При этом одной записи могут соответствовать несколько диагностических меток, которые дополнительно объединены в суперклассы и подклассы.

Целью работы является адаптация и экспериментальное исследование архитектуры одномерной сверточной нейронной сети InceptionTime для

автоматической классификации ЭКГ-сигналов по пяти диагностическим суперклассам набора данных PTB-XL с использованием функции взвешенной бинарной кросс-энтропии и подбором индивидуальных порогов классификации.

Постановка задачи. Материалы и методы решения

Задача автоматического анализа ЭКГ заключается в классификации записей с множественными метками. Для входной матрицы сигнала $\mathbf{X} \in \mathbb{R}^{12\times1000}$ (12 — число отведений, 1000 — длина временного ряда после приведения к частоте 100 Гц) требуется найти отображение f: $\mathbf{X}\rightarrow\mathbf{Y}$, где $\mathbf{Y} \in \{0, 1\}^5$ — бинарный вектор принадлежности записи к пяти диагностическим суперклассам. При этом, поскольку классы не являются взаимоисключающими, сумма элементов вектора $\mathbf{Y}$ может быть больше единицы.

Описание набора данных PTB-XL

В качестве базы исследования использовался открытый набор данных PTB-XL версии 1.0.3 [20, 21]. Он содержит 21 799 клинических 12-канальных записей ЭКГ длительностью 10 с, полученных от 18 869 пациентов. В данной работе использовались записи с частотой дискретизации 100 Гц. Выбор указанной частоты обусловлен результатами сравнения значений метрик качества и вычислительных затрат для представлений 100 и 500 Гц при согласованных временных масштабах сверточных ядер.

Оригинальная разметка содержит множество диагнозов, которые для решения поставленной задачи были агрегированы в пять диагностических суперклассов:

— NORM (Normal ECG) — без признаков патологий;

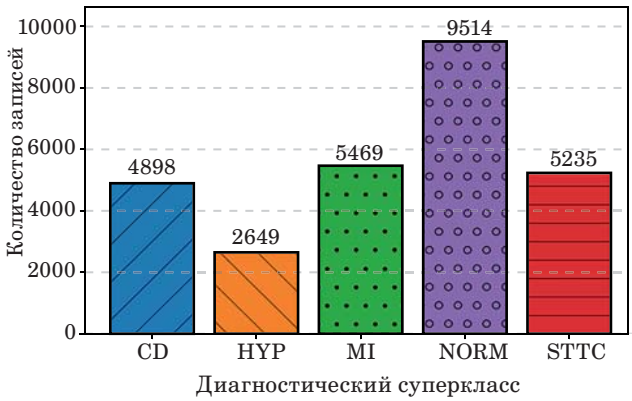
— MI (Myocardial Infarction) — инфаркт миокарда;

— STTC (ST/T Change) — изменения сегмента ST и зубца T;

— CD (Conduction Disturbance) — нарушения проводимости;

— HYP (Hypertrophy) — гипертрофия.

Используемые диагностические суперклассы представляют укрупненные категории электрокардиографических состояний. В рассматриваемой постановке классификация ЭКГ по этим суперклассам предназначена для предварительного выделения крупных групп указанных выше изменений. Результат может использоваться для предварительной сортировки ЭКГ-записей и выделения записей, требующих последующего анализа специалистом, не заменяя детальную интерпретацию ЭКГ врачом.



■ ***Рис. 2.*** Распределение количества ЭКГ-записей по пяти диагностическим суперклассам

■ ***Fig. 2.*** Distribution of ECG records across the five diagnostic superclasses

После проведения анализа были исключены записи, не содержащие диагностические суперклассы, что привело к сокращению итогового объема набора данных до 21 388 записей от 18 617 пациентов.

Распределение количества диагностических меток по суперклассам представлено на рис. 2 (подчеркнем, что одна запись может относиться сразу к нескольким классам). Видно, что набор данных несбалансирован: класс NORM представлен заметно чаще, чем класс HYP.

Предварительная обработка данных

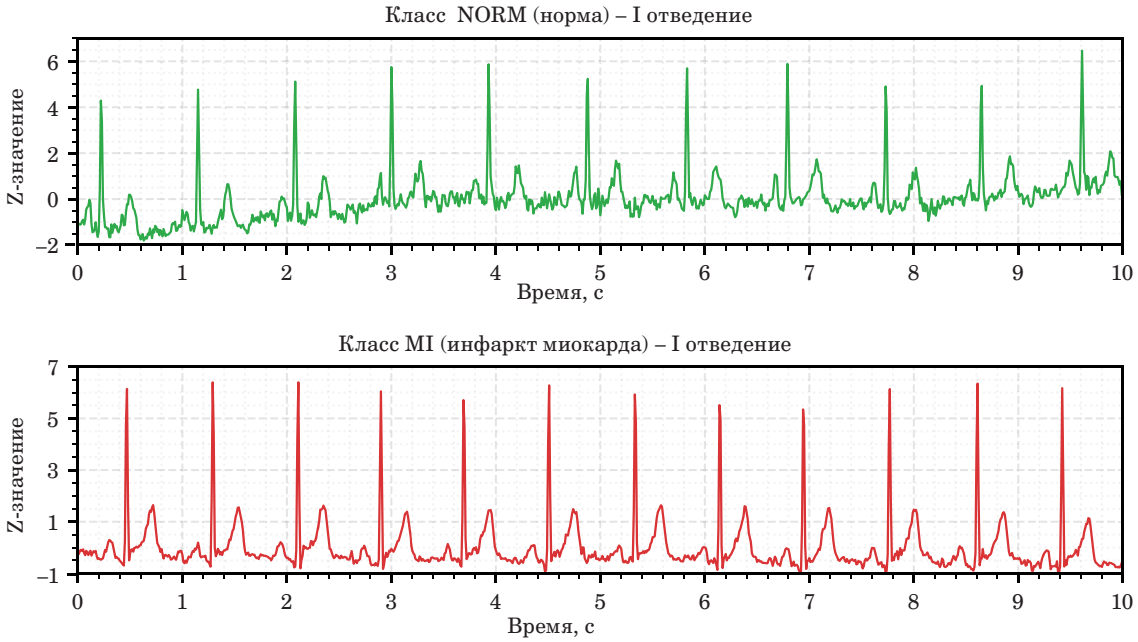
На этапе предварительной обработки выполнялась Z-score нормализация отдельно для каждой ЭКГ-записи. Среднее значение и среднеквадратическое отклонение рассчитывались совместно по всем отсчетам 12 отведений данной записи, после чего полученные общие параметры использовались для нормализации всех каналов. Такое преобразование позволяло привести ЭКГ-записи к сопоставимому численному масштабу и повысить устойчивость процесса обучения нейронной сети. При этом для всех отведений одной записи использовались общие параметры нормализации, поэтому независимое масштабирование отдельных каналов не выполнялось.

Нормализация выполнялась в соответствии с формулой

$$x_i^{'} = \frac{x_i - \overline{x}}{s},$$

где x_i — текущее значение сигнала; $\overline{x}$ — среднее значение сигнала; s — выборочное среднеквадратическое отклонение.

Примеры предварительно обработанных 10-секундных сигналов для нормальной ЭКГ и ЭКГ с инфарктом миокарда приведены на рис. 3.



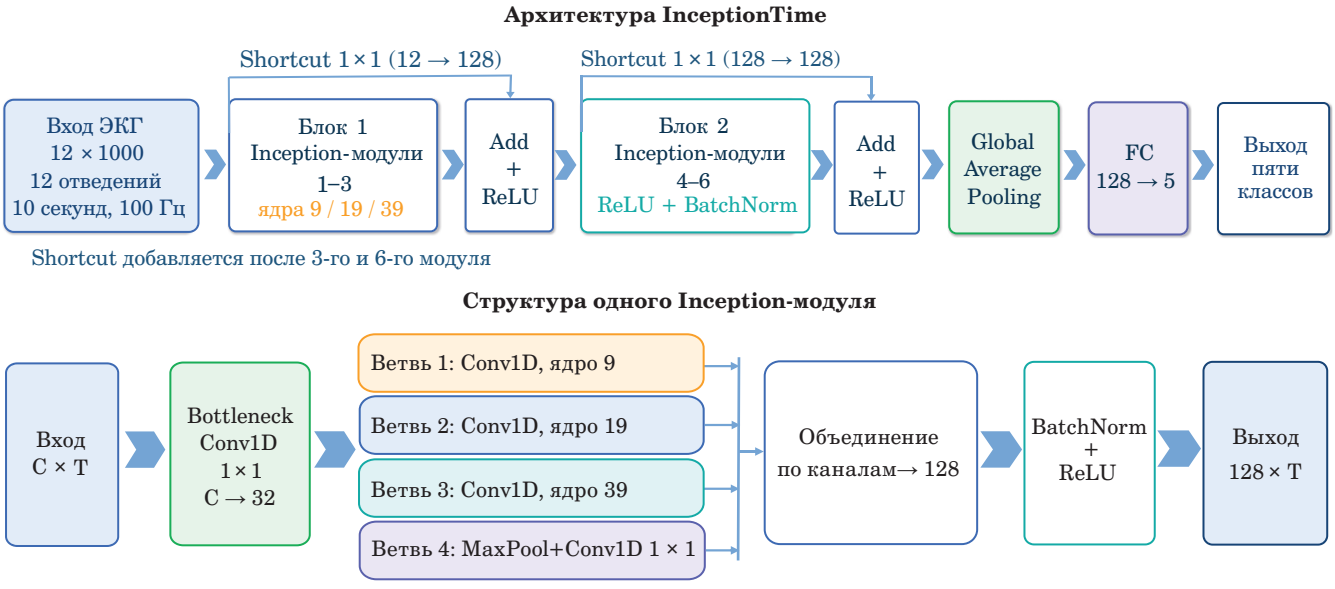
■ ***Рис. 3.*** Примеры предварительно обработанных ЭКГ-сигналов
■ ***Fig. 3.*** Examples of preprocessed ECG signals

Архитектура InceptionTime

Для решения задачи классификации многоканальных временных рядов была выбрана архитектура InceptionTime [16]. Данная архитектура развивает идею Inception-модулей, предложенную в [15], и основана на параллельном применении одномерных сверток с различными размерами ядер к одному и тому же входному сигналу. Схема разработанной модели представлена на рис. 4.

Модель состоит из шести последовательно соединенных Inception-модулей. После третьего и шестого модулей добавляются остаточные связи. Они помогают передавать информацию между блоками напрямую и делают обучение более устойчивым.

Каждый Inception-модуль содержит несколько параллельных ветвей обработки сигнала. Сначала применяется свертка с размером ядра 1 × 1, формирующая 32 признаковых канала,



■ ***Рис. 4.*** Архитектура модели InceptionTime и структура одного Inception-модуля
■ ***Fig. 4.*** Architecture of the InceptionTime model and structure of one Inception module

которые затем поступают в параллельные сверточные ветви. Затем сигнал одновременно проходит через три одномерные свертки с размерами ядер 9, 19 и 39. При частоте дискретизации 100 Гц это соответствует временным окнам около 90, 190 и 390 мс. Конфигурация размеров ядер 9, 19 и 39 была выбрана на этапе предварительной настройки модели по результатам экспериментального сравнения различных вариантов на валидационной выборке. Ядро размером 9 помогает выделять короткие элементы ЭКГ, прежде всего QRS-комплекс. Ядро размером 19 учитывает участки средней длительности, а ядро размером 39 — более протяженные изменения, связанные с сегментом ST и зубцом T. Кроме того, в модуле используется ветвь максимального объединения с последующей сверткой 1×1. Эта ветвь помогает модели быть менее чувствительной к небольшим сдвигам сигнала во времени. После этого выходы всех ветвей объединяются по каналам и проходят через пакетную нормализацию и функцию активации ReLU. На выходе одного Inception-модуля формируется 128 признаковых каналов.

После последнего Inception-модуля значения каждого признакового канала усредняются по всей длине сигнала. В результате для каждого канала остается одно итоговое значение, а полученный вектор поступает на полносвязный слой с пятью выходами — по числу диагностических суперклассов. Для каждого из них затем применяется сигмоидная функция. Она позволяет отдельно оценивать вероятность каждого класса и не требует, чтобы сумма вероятностей была равна единице. Это важно, поскольку одна ЭКГ-запись может одновременно относиться к нескольким диагностическим категориям.

Обучение модели и подбор порогов классификации

Программная реализация модели и процедуры обучения была выполнена на языке Python. Архитектура нейронной сети реализована средствами PyTorch [22]. Для организации процесса обучения, работы с временными рядами, применения преобразований данных и расчета метрик качества использовались библиотеки fastai [23] и tsai [24].

Вычислительные эксперименты проводились в облачной среде Kaggle с использованием графического ускорителя NVIDIA Tesla T4. Для сопоставимой оценки вычислительных затрат время обучения представлений 100 и 500 Гц измерялось на фиксированном интервале в 25 эпох. При 100 Гц обучение заняло 11,88 мин, при 500 Гц с ядрами (9; 19; 39) — 55,63 мин, а в варианте 500 Гц с ядрами (45; 95; 195) — 178,92 мин. Пиковое использование памяти составило 0,88 ГБ для 100 Гц и 3,76 ГБ для варианта 500 Гц с увеличенными ядрами. Поскольку переход от 100 Гц к 500 Гц не обеспечил улучшения Macro-F1, было сохранено представление ЭКГ с частотой дискретизации 100 Гц.

Обучение проводилось мини-пакетами по 64 записи. Использовалось рекомендованное в [20] разбиение набора данных: обучающая выборка — блоки 1–8, валидационная выборка — блок 9, тестовая выборка — блок 10. После исключения записей, не содержащих рассматриваемых диагностических суперклассов, обучающая выборка включала 17 084 записи от 14 823 пациентов, валидационная — 2 146 записей от 1 917 пациентов, тестовая — 2 158 записей от 1 877 пациентов. Проверка идентификаторов пациентов показала отсутствие пересечений между обучающей, валидационной и тестовой выборками, поэтому различные ЭКГ-записи одного пациента не попадали в разные выборки. Валидационная выборка применялась для настройки параметров модели и порогов классификации, а тестовая — только для финальной оценки качества.

Для оптимизации параметров модели использовался алгоритм AdamW [25] с коэффициентом затухания весов 0,1. Скорость обучения изменялась по «политике одного цикла» [26], при этом максимальное значение скорости обучения составляло 10^{-4}. Значения максимальной скорости обучения и коэффициента затухания весов дополнительно проверялись в сравнительных экспериментах на валидационной выборке. Максимальное число эпох было равно 100. Для снижения риска переобучения применялась ранняя остановка: если значение функции потерь на валидационной выборке не улучшалось в течение восьми эпох, обучение прекращалось автоматически. Для итоговой оценки использовалось состояние модели, соответствующее минимальному значению функции потерь на валидационной выборке.

Поскольку в работе решается задача классификации с множественными метками, для обучения использовалась бинарная кросс-энтропия с логитами L_{BCE}. Эта функция рассчитывает ошибку независимо для каждого диагностического суперкласса и не предполагает, что классы являются взаимоисключающими. Для учета дисбаланса классов применялась взвешенная модификация функции потерь, которая вычислялась по формуле

$$L_{\mathrm{BCE}}(\mathbf{y}, \hat{\mathbf{y}}) =$$

$$= -\frac{1}{5}\sum_{i=1}^{5}[w_i \cdot y_i \log(\sigma(\hat{y}_i)) + (1 - y_i)\log\big(1 - \sigma(\hat{y}_i)\big)],$$

где для i-го класса: w_i — весовой коэффициент, компенсирующий дисбаланс путем штрафа за ложноотрицательные предсказания; $y_i \in \{0, 1\}$ — истинная метка (1 — класс присутствует, 0 — класс отсутствует); $\hat{y}_i$ — логит («сырой» выход сети

до функции активации); $\sigma(\hat{y}_i) = \frac{1}{1+e^{-\hat{y}_i}}$ — сигмоидная функция активации, преобразующая логит в вероятность.

При проведении вычислительных экспериментов вектор весов $\mathbf{W} = (w_1; w_2; w_3; w_4; w_5) = (w_{CD}; w_{HYP}; w_{MI}; w_{NORM}; w_{STTC})$ выбирался равным (1,0; 2,0; 2,0; 1,0; 1,5). Повышенные коэффициенты для классов HYP, MI и STTC увеличивали вклад положительных примеров этих классов в функцию потерь и использовались как умеренная мера учета дисбаланса классов. Выбор коэффициентов был проверен экспериментальным сравнением нескольких схем взвешивания.

После обучения выполнялся подбор индивидуальных порогов классификации. Учитывая, что стандартный порог 0,5 не всегда оптимален для несбалансированных медицинских данных (для редких классов модель может выдавать более низкие значения вероятности), целесообразно для каждого диагностического суперкласса на валидационной выборке перебирать значения порога от 0,10 до 0,90 с шагом 0,05. При этом оптимальным считался порог, при котором F1-мера для данного класса достигала наибольшего значения. Найдены индивидуальные оптимальные пороги классификации: NORM — 0,45; MI — 0,50; STTC — 0,50; CD — 0,40; HYP — 0,45.

Результаты экспериментов и их обсуждение

Оценка качества модели осуществлялась на тестовой выборке. Для анализа результатов использовались общая точность (Accuracy), точность положительных предсказаний (Precision), полнота (Recall), F1-мера и макроусредненная F1-мера (Macro-F1), которые рассчитывались по следующим формулам:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN};$$

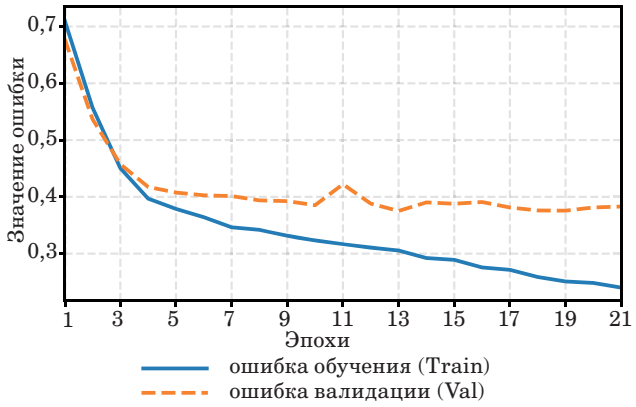
$$Precision = \frac{TP}{TP + FP};$$

$$Recall = \frac{TP}{TP + FN};$$

$$F1 = \frac{2 \times TP}{2 \times TP + FN + FP};$$

$$Macro\text{-}F1 = \frac{1}{5}\sum_{i=1}^{5} \mathrm{F1}_i,$$

где TP, TN, FP и FN — соответственно истинно положительные, истинно отрицательные, ложноположительные и ложноотрицательные решения.



■ ***Рис. 5.*** Динамика изменения функции потерь L_{BCE} при обучении

■ ***Fig. 5.*** Dynamics of the loss function during training

Подчеркнем, что для несбалансированных медицинских данных особое значение имеет полнота, поскольку она отражает долю реально присутствующих патологий.

Графики изменения функции потерь в зависимости от эпохи на обучающей и валидационной выборках представлены на рис. 5. Отметим, что минимальное значение ошибки на валидационной выборке было достигнуто на 13-й эпохе, после чего дальнейшее обучение приводило к переобучению.

Поскольку распределение диагностических классов в используемом наборе данных является несбалансированным, Accuracy в данной работе рассматривается как вспомогательная метрика, характеризующая динамику процесса обучения, и не используется в качестве основного критерия качества модели. Основные выводы о качестве классификации основываются прежде всего на Recall и Macro-F1. График изменения общей точности в зависимости от эпохи на валидационной выборке представлен на рис. 6. Рост значения метрики в первые эпохи и последующая стабилизация свидетельствуют о выходе процесса обучения на устойчивый уровень без дальнейшего существенного изменения данной метрики на валидационной выборке.

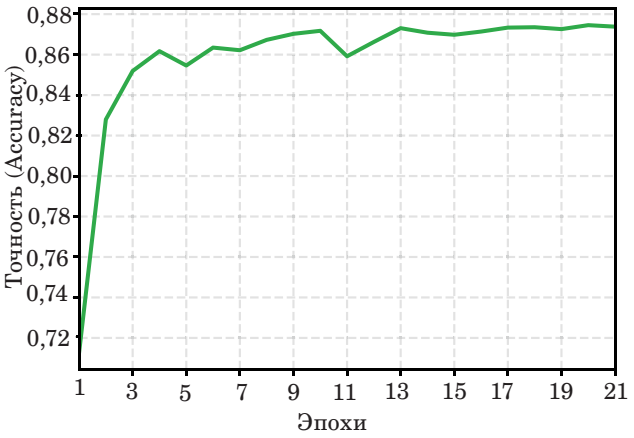
Для проверки эффективности предложенного подхода значения метрик качества модели InceptionTime сравнивались с соответствующими метриками других моделей, применявшихся для анализа ЭКГ на базе PTB-XL (таблица).

Анализ таблицы показывает, что предложенная модель InceptionTime обеспечивает наибольшее значение метрики полноты 0,74 по сравнению с рекуррентными и сверточными моделями. Для задачи предварительного анализа ЭКГ этот результат особенно важен, поскольку Recall отражает способность модели находить реально присутствующие патологические состояния.

■ Сравнение значений метрик качества классификации моделей по пяти диагностическим суперклассам PTB-XL

■ Comparison of classification performance metrics for models across the five PTB-XL diagnostic superclasses

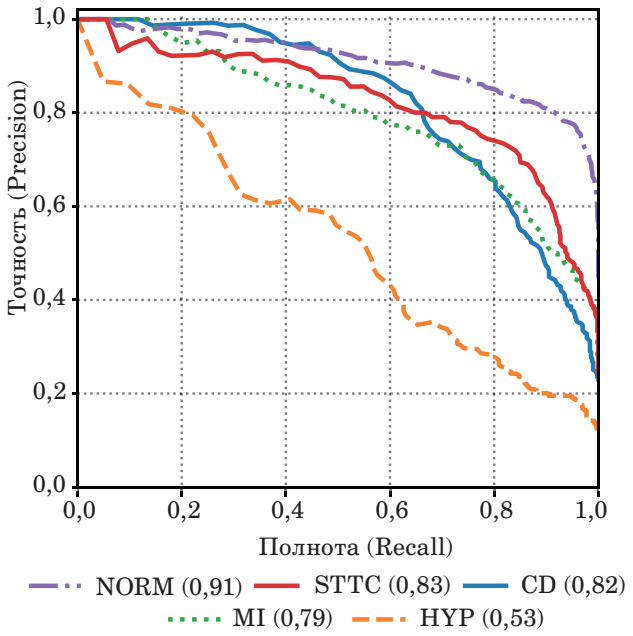
Модель	Accuracy	Precision	Recall	Macro-F1	Источник
RNN	0,76	0,01	0,07	0,09	[11]
GRU	0,86	0,82	0,52	0,62	[11]
LSTM	0,87	**0,82**	0,57	0,66	[11]
CNN	0,72	0,64	0,60	0,61	[12]
SincNet	0,73	0,67	0,59	0,60	[12]
CNN + entropy features	0,77	0,71	0,66	0,68	[12]
MRF-CNN	**0,90**	0,73	0,71	0,72	[17]
Inception-Time	0,87	0,70	**0,74**	**0,72**	Данная работа



■ ***Рис. 6.*** Динамика изменения точности модели на валидационной выборке

■ ***Fig. 6.*** Dynamics of model accuracy on the validation set

По значению метрики Macro-F1 модель InceptionTime превосходит все представленные в таблице модели за исключением MRF-CNN, для которой значения совпадают. Отметим, что модель MRF-CNN демонстрирует более высокую Accuracy, хотя для несбалансированных медицинских данных она не является основной метрикой, поскольку может быть завышена за счет преобладания часто встречающихся классов. Небольшое снижение метрики Precision в модели InceptionTime по сравнению с MRF-CNN связано с повышением чувствительности модели. Такой компромисс допустим для систем предварительного анализа ЭКГ: ложноположительное срабатывание может



■ ***Рис. 7.*** Кривые точности-полноты для пяти диагностических суперклассов

■ ***Fig. 7.*** Precision-recall curves for the five diagnostic superclasses

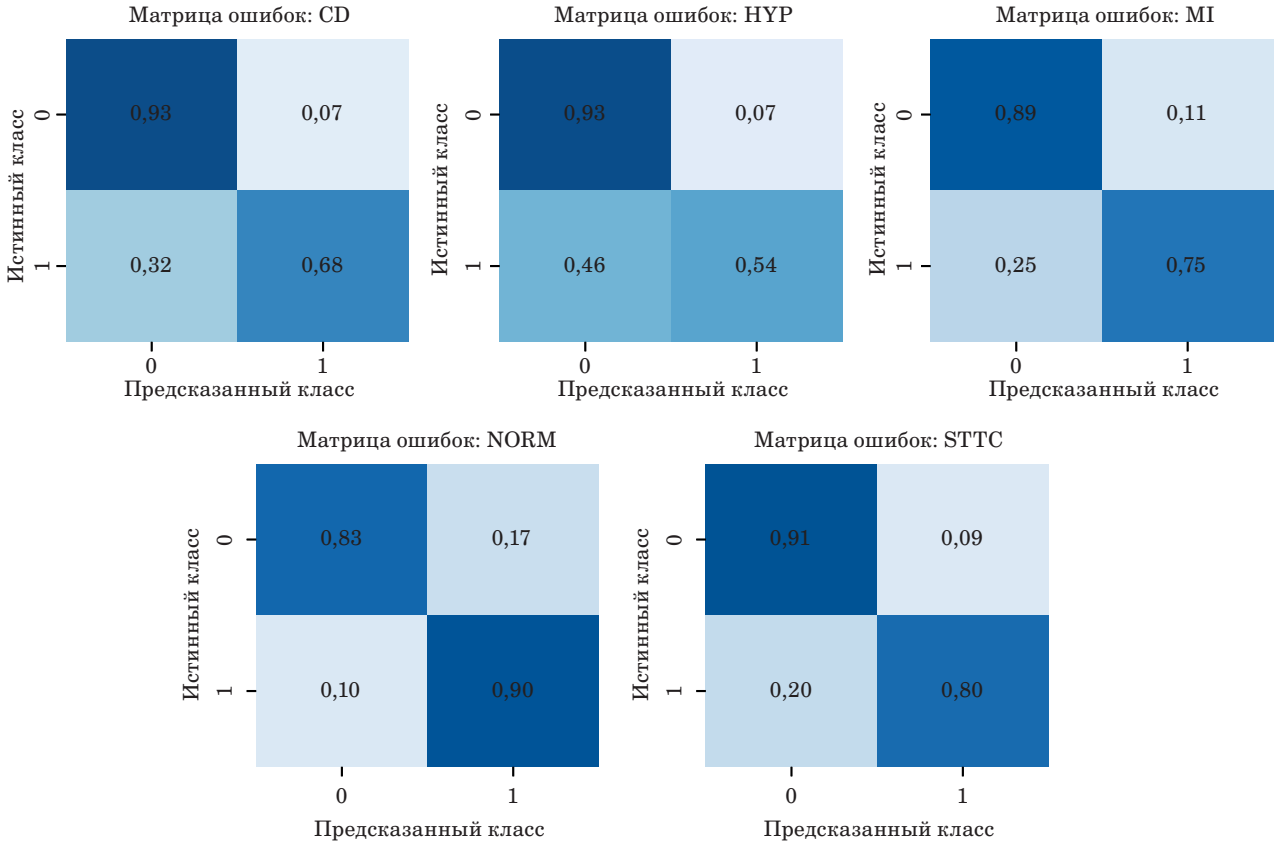
быть дополнительно проверено врачом, в то время как пропуск патологического состояния несет больший риск. В данной работе основной акцент сделан на метрики Recall и Macro-F1, которые лучше отражают качество распознавания патологий в условиях дисбаланса данных.

Для анализа зависимости между точностью Precision и полнотой Recall при различных значениях порога классификации для каждого из пяти диагностических суперклассов были построены кривые точности-полноты (рис. 7); в скобках приведены соответствующие значения площадей под кривыми Precision–Recall (PR-AUC).

Наибольшее значение PR-AUC получено для суперкласса NORM — 0,91. Наименьшее значение PR-AUC, равное 0,53, соответствует суперклассу HYP, который остается наиболее сложным для распознавания среди рассматриваемых диагностических категорий.

Нормализованные матрицы ошибок для диагностических суперклассов (рис. 8) показывают долю верных и ошибочных решений.

Матрицы ошибок подтверждают, что модель уверенно распознает нормальные записи и демонстрирует высокую чувствительность к инфаркту миокарда и изменениям сегмента ST/T. Для суперклассов CD и HYP задача остается более сложной, что связано с меньшим числом записей и большей вариативностью проявлений этих состояний. Подбор индивидуальных порогов позволяет уменьшить число ложноотрицательных решений для таких классов.



■ ***Рис. 8.*** Нормализованные матрицы ошибок для пяти диагностических суперклассов
■ ***Fig. 8.*** Normalized confusion matrices for the five diagnostic superclasses

Заключение

Предложен и экспериментально исследован подход к многометочной классификации 12-канальных ЭКГ-сигналов по пяти диагностическим суперклассам PTB-XL на основе одномерной сверточной нейронной сети InceptionTime.

Основной результат работы состоит в том, что архитектура была адаптирована не только для обработки временных рядов, но и как часть полной схемы классификации несбалансированных медицинских данных, включающей в себя нормализацию ЭКГ-записей, многомасштабное извлечение признаков, взвешенную бинарную кросс-энтропию и индивидуальные пороги классификации для каждого диагностического суперкласса.

Экспериментальная проверка показала, что для предложенной модели InceptionTime на тестовой выборке Macro-F1 = 0,72 и Recall = 0,74. При этом по сравнению с другими моделями InceptionTime представила наибольшее значение Recall и один из лучших результатов по Macro-F1. Отметим, что высокое значение Recall существенно именно для медицинских задач, поскольку оно отражает способность модели выявлять реально присутствующие патологические состояния.

Полученные результаты демонстрируют применимость архитектуры InceptionTime для задачи предварительного многометочного анализа ЭКГ. Разработанная модель обеспечивает одновременное выявление нескольких диагностических категорий и показывает конкурентоспособные результаты по полноте и Macro-F1 в сравнении с рассмотренными подходами. Предложенная схема может служить основой для дальнейшего развития программных средств предварительного анализа ЭКГ и систем поддержки врачебных решений. При этом модель рассматривается именно как инструмент предварительного анализа, дополняющий интерпретацию специалиста, а не как автономная система постановки диагноза.

Дальнейшие исследования в рамках рассмотренной задачи могут быть направлены на повышение качества распознавания наиболее сложных и менее представленных диагностических классов. Представляется целесообразной адаптация сверточной нейронной сети InceptionTime к другим видам биомедицинских сигналов (анализ электроэнцефалограмм, оценка уровня стресса и эмоций человека и др.).

Литература

1. **Ayano Y. M., Schwenker F., Dufera B. D., Debelee T. G.** Interpretable machine learning techniques in ECG-based heart disease classification: A systematic review. *Diagnostics,* 2023, vol. 13, no. 1, art. 111. doi:10.3390/diagnostics13010111
2. **Marwa S. R., Shakir M. A.** Improving ECG signals classification by using deep learning techniques: A review. *ITM Web of Conferences*, 2024, vol. 64, art. 01023. doi:10.1051/itmconf/20246401023
3. **Wang L., Bi T., Hao J., Zhou T. H.** Heart diseases recognition model based on HRV feature extraction over 12-lead ECG signals. *Sensors*, 2024, vol. 24, no. 16, art. 5296. doi:10.3390/s24165296
4. **Petmezas G., Stefanopoulos L., Kilintzis V., Tzavelis A., Rogers J. A., Katsaggelos A. K., Maglaveras N.** State-of-the-art deep learning methods on electrocardiogram data: Systematic review. *JMIR Medical Informatics*, 2022, vol. 10, no. 8, e38454. doi:10.2196/38454
5. **Martínez-Sellés M., Marina-Breysse M.** Current and future use of artificial intelligence in electrocardiography. *Journal of Cardiovascular Development and Disease*, 2023, vol. 10, no. 4, art. 175. doi:10.3390/jcdd10040175
6. **Hannun A. Y., Rajpurkar P., Haghpanahi M., Tison G. H., Bourn C., Turakhia M. P., Ng A. Y.** Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network. *Nature Medicine*, 2019, vol. 25, no. 1, pp. 65–69. doi:10.1038/s41591-018-0268-3
7. **Ribeiro A. H., Ribeiro M. H., Paixão G. M. M., Oliveira D. M., Gomes P. R., Canazart J. A., Ferreira M. P. S., Andersson C. R., Macfarlane P. W., Meira W. Jr., Schön T. B., Ribeiro A. L. P.** Automatic diagnosis of the 12-lead ECG using a deep neural network. *Nature Communications*, 2020, vol. 11, art. 1760. doi:10.1038/s41467-020-15432-4
8. **Ose B., Sattar Z., Gupta A., Toquica C., Harvey C., Noheria A.** Artificial intelligence interpretation of the electrocardiogram: A state-of-the-art review. *Current Cardiology Reports*, 2024, vol. 26, no. 6, pp. 561–580. doi:10.1007/s11886-024-02062-1
9. **Wu Z., Guo C.** Deep learning and electrocardiography: Systematic review of current techniques in cardiovascular disease diagnosis and management. *BioMedical Engineering OnLine*, 2025, vol. 24, art. 23. doi:10.1186/s12938-025-01349-w
10. **Gustafsson S., Ribeiro A. H., Gedon D., Abreu P. E. O. G. B., Pielawski N., Paixão G. M. M., Gutierrez M. A., Krieger J. E., Dias F. M., Ribeiro A. L. P., Lindholm D., Schön T. B., Sundström J.** A deep learning ECG model for identification and localization of occlusion myocardial infarction. *Nature Communications*, 2026, vol. 17, art. 4336. doi:10.1038/s41467-026-73023-1
11. **Sæther S.** *Comparing Recurrent Neural Networks for ECG Analysis*: Master's thesis. Oslo, Oslo Metropolitan University, 2023. 61 p. https://home.simula.no/~paalh/students/SanderSaether-OsloMet-2023.pdf (дата обращения: 12.05.2026).
12. **Śmigiel S., Pałczyński K., Ledziński D.** ECG signal classification using deep learning techniques based on the PTB-XL dataset. *Entropy*, 2021, vol. 23, no. 9, art. 1121. doi:10.3390/e23091121
13. **Lekkas G., Vrochidou E., Papakostas G. A.** Time-frequency transformations for enhanced biomedical signal classification with convolutional neural networks. *BioMedInformatics*, 2025, vol. 5, no. 1, art. 7. doi:10.3390/biomedinformatics5010007
14. **Jaiswal G. K., Mitra S.** Hybrid CNN–BiLSTM Model for ECG signal classification and accurate arrhythmia detection (MIT-BIH and PTB-XL Validation). *International Journal of Computational and Experimental Science and Engineering*, 2025, vol. 11, no. 4, pp. 10058–10067. doi:10.22399/ijcesen.4575
15. **Szegedy C., Liu W., Jia Y., Sermanet P., Reed S., Anguelov D., Erhan D., Vanhoucke V., Rabinovich A.** Going deeper with convolutions. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, pp. 1–9. doi:10.1109/CVPR.2015.7298594
16. **Ismail Fawaz H., Lucas B., Forestier G., Pelletier C., Schmidt D. F., Weber J., Webb G. I., Idoumghar L., Muller P.-A., Petitjean F.** InceptionTime: Finding AlexNet for time series classification. *Data Mining and Knowledge Discovery*, 2020, vol. 34, no. 6, pp. 1936–1962. doi:10.1007/s10618-020-00710-y
17. **Feyisa D. W., Debelee T. G., Ayano Y. M., Kebede S. R., Assore T. F.** Lightweight multireceptive field CNN for 12-lead ECG signal classification. *Computational Intelligence and Neuroscience*, 2022, vol. 2022, art. 8413294. doi:10.1155/2022/8413294
18. **Crocker H. J., Costall A. W.** An inceptiontime-inspired convolutional neural network to detect cardiac abnormalities in reduced-lead ECG data. *Computing in Cardiology*, 2021, vol. 48, pp. 1–4. doi:10.23919/CinC53138.2021.9662678
19. **Borra D., Andalò A., Severi S., Corsi C.** On the application of convolutional neural networks for 12-lead ECG multi-label classification using datasets from multiple centers. *Computing in Cardiology*, 2020, vol. 47, pp. 1–4. doi:10.22489/CinC.2020.349
20. **Wagner P., Strodthoff N., Bousseljot R.-D., Kreiseler D., Lunze F. I., Samek W., Schaeffter T.** PTB-XL, a large publicly available electrocardiography dataset. *Scientific Data*, 2020, vol. 7, art. 154. doi:10.1038/s41597-020-0495-6
21. **Strodthoff N., Wagner P., Schaeffter T., Samek W.** Deep learning for ECG analysis: Benchmarks and Insights from PTB-XL. *IEEE Journal of Biomedical and Health Informatics*, 2021, vol. 25, no. 5, pp. 1519–1528. doi:10.1109/JBHI.2020.3022989

22. **Paszke A., Gross S., Massa F., Lerer A., Bradbury J., Chanan G., Killeen T., Lin Z., Gimelshein N., Antiga L., Desmaison A., Köpf A., Yang E., DeVito Z., Raison M., Tejani A., Chilamkurthy S., Steiner B., Fang L., Bai J., Chintala S.** PyTorch: An imperative style, high-performance deep learning library. arXiv preprint, 2019. doi:10.48550/arXiv.1912.01703
23. **Howard J., Gugger S.** Fastai: A layered API for deep learning. *Information*, 2020, vol. 11, no. 2, art. 108. doi:10.3390/info11020108
24. **Oguiza I., Rodriguez-Fernandez V., Neoh D., filipj8, J-M., Kainkaryam R., Mistry D., Yang Z., Williams D., Cho R., geoHeil, Versek C., samlloydig, Mistry D., imilas, Golinski A., Muhr D., H J., MichaelDee, Sachdeva K., Capelle T.** timeseriesAI/tsai: v0.3.9 [Software]. *Zenodo*, 2024. doi:10.5281/zenodo.10647659
25. **Loshchilov I., Hutter F.** Decoupled weight decay regularization. *International Conference on Learning Representations*, New Orleans, LA, USA, 2019. https://openreview.net/forum?id=Bkg6RiCqY7 (дата обращения: 12.05.2026).
26. **Smith L. N., Topin N.** Super-convergence: Very fast training of neural networks using large learning rates. *Proceedings of SPIE*, 2019, vol. 11006, art. 1100612. doi:10.1117/12.2520589

UDC 004.032.26; 616.12-073.7
doi:10.31799/1684-8853-2026-5-85-95
EDN: CSPEWE

Application of the InceptionTime convolutional neural network to multi-label classification of electrocardiograms

V. M. Chubich[a], Dr. Sc., Tech., Professor, orcid.org/0000-0003-2006-0046, chubich@ami.nstu.ru
E. S. Kotselap[a], Student, orcid.org/0009-0008-6142-3580
[a]Novosibirsk State Technical University, 20, K. Marks Pr., 630073, Novosibirsk, Russian Federation

Introduction: The challenge of multi-label electrocardiogram classification arises due to several diagnoses corresponding to a single record. Rare diagnoses have fewer examples, while their features appear in signal segments of different durations. Consequently, a single analysis scale and a common decision threshold increase the risk of bias toward frequent conditions and the risk of missing rare pathologies. **Purpose:** To adapt and experimentally evaluate a one-dimensional InceptionTime convolutional neural network for multi-label electrocardiogram classification. **Results:** The study develops a classification scheme combining multiscale feature extraction, weighted binary cross-entropy with logits, and individual thresholds for five diagnostic superclasses. We evaluate the model on ten-second, twelve-lead electrocardiograms representing records without pathology, myocardial infarction, repolarization abnormalities, conduction disturbances, and hypertrophy. On the test set, recall reaches 0.74, while the macro-averaged harmonic mean of precision and recall reaches 0.72. Comparison with recurrent and convolutional architectures shows that the InceptionTime-based model has achieved the highest recall and one of the highest macro-averaged harmonic means of precision and recall. **Practical relevance:** The adapted model can underpin a software module for preliminary electrocardiogram analysis and clinical decision support systems. Independent assessment of diagnostic conditions enables the detection of several pathologies in one record, while class-specific thresholds help reduce the risk of missing rare pathologies and identify records for specialist review. **Discussion:** The study identifies improving the recognition of rare classes and evaluating the model on other biomedical signals, including electroencephalograms and signals related to stress and emotions, as priorities for further research.

Keywords — convolutional neural network, InceptionTime, deep learning, binary cross-entropy, electrocardiography, class imbalance, multi-label classification, cardiovascular diagnostics.

For citation: Chubich V. M., Kotselap E. S. Application of the InceptionTime convolutional neural network to multi-label classification of electrocardiograms. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 85–95 (In Russian). doi:10.31799/1684-8853-2026-5-85-95, EDN: CSPEWE

References

1. Ayano Y. M., Schwenker F., Dufera B. D., Debelee T. G. Interpretable machine learning techniques in ECG-based heart disease classification: A systematic review. *Diagnostics*, 2023, vol. 13, no. 1, art. 111. doi:10.3390/diagnostics13010111
2. Marwa S. R., Shakir M. A. Improving ECG signals classification by using deep learning techniques: A review. *ITM Web of Conferences*, 2024, vol. 64, art. 01023. doi:10.1051/itmconf/20246401023
3. Wang L., Bi T., Hao J., Zhou T. H. Heart diseases recognition model based on HRV feature extraction over 12-lead ECG signals. *Sensors*, 2024, vol. 24, no. 16, art. 5296. doi:10.3390/s24165296
4. Petmezas G., Stefanopoulos L., Kilintzis V., Tzavelis A., Rogers J. A., Katsaggelos A. K., Maglaveras N. State-of-the-art deep learning methods on electrocardiogram data: Systematic review. *JMIR Medical Informatics*, 2022, vol. 10, no. 8, e38454. doi:10.2196/38454
5. Martínez-Sellés M., Marina-Breysse M. Current and future use of artificial intelligence in electrocardiography. *Journal of Cardiovascular Development and Disease*, 2023, vol. 10, no. 4, art. 175. doi:10.3390/jcdd10040175
6. Hannun A. Y., Rajpurkar P., Haghpanahi M., Tison G. H., Bourn C., Turakhia M. P., Ng A. Y. Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network. *Nature Medicine*, 2019, vol. 25, no. 1, pp. 65–69. doi:10.1038/s41591-018-0268-3
7. Ribeiro A. H., Ribeiro M. H., Paixão G. M. M., Oliveira D. M., Gomes P. R., Canazart J. A., Ferreira M. P. S., Andersson C. R., Macfarlane P. W., Meira W. Jr., Schön T. B., Ribeiro A. L. P. Automatic diagnosis of the 12-lead ECG using a deep neural network. *Nature Communications*, 2020, vol. 11, art. 1760. doi:10.1038/s41467-020-15432-4
8. Ose B., Sattar Z., Gupta A., Toquica C., Harvey C., Noheria A. Artificial intelligence interpretation of the electrocardio-

gram: A state-of-the-art review. *Current Cardiology Reports*, 2024, vol. 26, no. 6, pp. 561–580. doi:10.1007/s11886-024-02062-1
9. Wu Z., Guo C. Deep learning and electrocardiography: Systematic review of current techniques in cardiovascular disease diagnosis and management. *BioMedical Engineering OnLine*, 2025, vol. 24, art. 23. doi:10.1186/s12938-025-01349-w
10. Gustafsson S., Ribeiro A. H., Gedon D., Abreu P. E. O. G. B., Pielawski N., Paixão G. M. M., Gutierrez M. A., Krieger J. E., Dias F. M., Ribeiro A. L. P., Lindholm D., Schön T. B., Sundström J. A deep learning ECG model for identification and localization of occlusion myocardial infarction. *Nature Communications*, 2026, vol. 17, art. 4336. doi:10.1038/s41467-026-73023-1
11. Sæther S. *Comparing Recurrent Neural Networks for ECG Analysis*: Master's thesis. Oslo, Oslo Metropolitan University, 2023. 61 p. Available at: https://home.simula.no/~paalh/students/SanderSaether-OsloMet-2023.pdf (accessed 12 May 2026).
12. Śmigiel S., Pałczyński K., Ledziński D. ECG signal classification using deep learning techniques based on the PTB-XL dataset. *Entropy*, 2021, vol. 23, no. 9, art. 1121. doi:10.3390/e23091121
13. Lekkas G., Vrochidou E., Papakostas G. A. Time-frequency transformations for enhanced biomedical signal classification with convolutional neural networks. *BioMedInformatics*, 2025, vol. 5, no. 1, art. 7. doi:10.3390/biomedinformatics5010007
14. Jaiswal G. K., Mitra S. Hybrid CNN–BiLSTM Model for ECG signal classification and accurate arrhythmia detection (MIT-BIH and PTB-XL Validation). *International Journal of Computational and Experimental Science and Engineering*, 2025, vol. 11, no. 4, pp. 10058–10067. doi:10.22399/ijcesen.4575
15. Szegedy C., Liu W., Jia Y., Sermanet P., Reed S., Anguelov D., Erhan D., Vanhoucke V., Rabinovich A. Going deeper with convolutions. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, pp. 1–9. doi:10.1109/CVPR.2015.7298594
16. Ismail Fawaz H., Lucas B., Forestier G., Pelletier C., Schmidt D. F., Weber J., Webb G. I., Idoumghar L., Muller P.-A., Petitjean F. InceptionTime: Finding AlexNet for time series classification. *Data Mining and Knowledge Discovery*, 2020, vol. 34, no. 6, pp. 1936–1962. doi:10.1007/s10618-020-00710-y
17. Feyisa D. W., Debelee T. G., Ayano Y. M., Kebede S. R., Assore T. F. Lightweight multireceptive field CNN for 12-lead ECG signal classification. *Computational Intelligence and Neuroscience*, 2022, vol. 2022, art. 8413294. doi:10.1155/2022/8413294
18. Crocker H. J., Costall A. W. An inceptiontime-inspired convolutional neural network to detect cardiac abnormalities in reduced-lead ECG data. *Computing in Cardiology*, 2021, vol. 48, pp. 1–4. doi:10.23919/CinC53138.2021.9662678
19. Borra D., Andalò A., Severi S., Corsi C. On the application of convolutional neural networks for 12-lead ECG multi-label classification using datasets from multiple centers. *Computing in Cardiology*, 2020, vol. 47, pp. 1–4. doi:10.22489/CinC.2020.349
20. Wagner P., Strodthoff N., Bousseljot R.-D., Kreiseler D., Lunze F. I., Samek W., Schaeffter T. PTB-XL, a large publicly available electrocardiography dataset. *Scientific Data*, 2020, vol. 7, art. 154. doi:10.1038/s41597-020-0495-6
21. Strodthoff N., Wagner P., Schaeffter T., Samek W. Deep learning for ECG analysis: Benchmarks and Insights from PTB-XL. *IEEE Journal of Biomedical and Health Informatics*, 2021, vol. 25, no. 5, pp. 1519–1528. doi:10.1109/JBHI.2020.3022989
22. Paszke A., Gross S., Massa F., Lerer A., Bradbury J., Chanan G., Killeen T., Lin Z., Gimelshein N., Antiga L., Desmaison A., Köpf A., Yang E., DeVito Z., Raison M., Tejani A., Chilamkurthy S., Steiner B., Fang L., Bai J., Chintala S. PyTorch: An imperative style, high-performance deep learning library. arXiv preprint, 2019. doi:10.48550/arXiv.1912.01703
23. Howard J., Gugger S. Fastai: A layered API for deep learning. *Information*, 2020, vol. 11, no. 2, art. 108. doi:10.3390/info11020108
24. Oguiza I., Rodriguez-Fernandez V., Neoh D., filipj8, J-M., Kainkaryam R., Mistry D., Yang Z., Williams D., Cho R., geoHeil, Versek C., samlloydig, Mistry D., imilas, Golinski A., Muhr D., H J., MichaelDee, Sachdeva K., Capelle T. timeseriesAI/tsai: v0.3.9 [Software]. *Zenodo*, 2024. doi:10.5281/zenodo.10647659
25. Loshchilov I., Hutter F. Decoupled weight decay regularization. *International Conference on Learning Representations*, New Orleans, LA, USA, 2019. Available at: https://openreview.net/forum?id=Bkg6RiCqY7 (accessed 12 May 2026).
26. Smith L. N., Topin N. Super-convergence: Very fast training of neural networks using large learning rates. *Proceedings of SPIE*, 2019, vol. 11006, art. 1100612. doi:10.1117/12.2520589

СВЕДЕНИЯ ОБ АВТОРАХ

АНИКИН
Дмитрий
Александрович



Начальник отдела Главного центра Министерства обороны Российской Федерации, Москва.
В 2011 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Радиоэлектронные системы», в 2023 году – Российскую академию народного хозяйства и государственной службы при Президенте Российской Федерации по специальности «Государственное и муниципальное управление».
Является автором двух научных публикаций.
Область научных интересов – информационная безопасность, искусственный интеллект, национальная безопасность в информационной сфере, радиоэлектроника.
Эл. адрес: donanikin@yandex.ru

ВАСИЛЬЕВ
Владимир
Иванович



Профессор кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий.
В 1980 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Электронные вычислительные машины».
В 1990 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 400 научных публикаций и 14 свидетельств о регистрации программ для ЭВМ.
Область научных интересов — интеллектуальные системы управления, информационная безопасность.
Эл. адрес: vas0015@yandex.ru

ГУСЕВ
Максим
Михайлович



Магистрант Национального исследовательского университета «Высшая школа экономики», старший инженер по информационной безопасности в Яндексе, Москва.
В 2025 году окончил с отличием Национальный исследовательский университет «Высшая школа экономики» по направлению «Информационная безопасность».
Является автором четырех научных публикаций.
Область научных интересов – информационная безопасность, безопасность больших языковых моделей, состязательное машинное обучение, обеспечение безопасности систем ИИ.
Эл. адрес: mmgusev_1@edu.hse.ru

БОЛОТСКИХ
Ульяна
Алексеевна



Магистрант Санкт-Петербургского государственного университета аэрокосмического приборостроения, стажер ООО КНС ГРУПП, Санкт-Петербург.
В 2024 году окончила бакалавриат Санкт-Петербургского государственного университета аэрокосмического приборостроения по специальности «Инфокоммуникационные технологии и системы связи».
Область научных интересов – системы хранения данных.
Эл. адрес:
bolotsckix.ulia@yandex.ru

ВУЛЬФИН
Алексей
Михайлович



Профессор кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий.
В 2008 году окончил Уфимский государственный нефтяной технический университет по специальности «Программное обеспечение вычислительной техники и автоматизированных систем».
В 2022 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 200 научных публикаций, 34 свидетельств о регистрации программ для ЭВМ и одного патента на изобретение.
Область научных интересов — интеллектуальный анализ данных, моделирование сложных технических систем.
Эл. адрес: vulfin.alexey@yandex.ru

КИРИЛЛОВА
Анастасия
Дмитриевна



Старший преподаватель кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий.
В 2015 году окончила бакалавриат по специальности «Информационная безопасность», в 2017 году — магистратуру по специальности «Информатика и вычислительная техника» Уфимского государственного авиационного технического университета.
В 2023 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 80 научных публикаций и 17 свидетельств о регистрации программ для ЭВМ.
Область научных интересов — информационная безопасность, автоматизированные системы управления, управление рисками, когнитивное моделирование.
Эл. адрес:
kirillova.andm@gmail.com

КНЯЗЕВ Максим Андреевич



Аспирант университета «МИРЭА – Российский технологический университет», старший системный инженер компании «К2 Кибербезопасность», Москва.
В 2024 году окончил университет «МИРЭА – Российский технологический университет» по специальности «Компьютерная безопасность».
Является автором четырех научных публикаций.
Область научных интересов – информационная безопасность, безопасность интернета вещей, управление функциональными возможностями устройств интернета вещей, применение машинного обучения для защиты интеллектуальных устройств.
Эл. адрес: maxiknyaz@mail.ru

КРЯГИН Владимир Александрович



Преподаватель кафедры космической радиолокации и радионавигации Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 2004 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Организация и технология защиты информации».
Является автором 11 научных публикаций.
Область научных интересов – защита информации в радиотехнических системах сбора, обработки и передачи информации, радионавигация.
Эл. адрес: vovella@yandex.ru

КУЗЬМЕНКО Александр Александрович



Аспирант Института вычислительных систем и программирования Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2025 году окончил Волгоградский государственный технический университет по специальности «Электронные вычислительные машины».
Область научных интересов – системный анализ и моделирование медицинских информационных систем, удаленный мониторинг пациентов, IoMT, обработка биомедицинских сигналов, искусственный интеллект и машинное обучение в медицине, разработка медицинских аппаратно-программных комплексов.
Эл. адрес: skvotcher@yandex.ru

КОЦЕЛАП Екатерина Сергеевна



Студент факультета прикладной математики и информатики Новосибирского государственного технического университета.
Является автором одной научной публикации.
Область научных интересов – искусственный интеллект, глубокое машинное обучение, нейронные сети.
Эл. адрес:
kocelap.2023@stud.nstu.ru

КРЫЛОВ Даниил Романович



Аспирант, ассистент кафедры инфокоммуникационных технологий и систем связи Института радиотехники и инфокоммуникационных технологий Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2024 году окончил магистратуру Санкт-Петербургского государственного университета аэрокосмического приборостроения по специальности «Инфокоммуникационные технологии и системы связи».
Является автором шести научных публикаций.
Область научных интересов – системы хранения данных, оптимизационные алгоритмы.
Эл. адрес:
daniil12244892@mail.ru

ЛУЦКОВИЧ Андрей Иванович



Старший преподаватель кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий.
В 2001 году окончил Уфимский государственный авиационный технический университет по специальности «Организация и технология защиты информации».
Является автором 14 научных публикаций.
Область научных интересов – интеллектуальные системы противодействия мошенничеству, методы машинного обучения при мониторинге информационной безопасности.
Эл. адрес: ceo@frodex.ru

НАЗАРОВ Владимир Андреевич



Магистрант Университета ИТМО, Санкт-Петербург.
В 2025 году окончил бакалавриат Университета ИТМО по направлению «Прикладная математика и информатика».
Область научных интересов – информационные технологии, конечные автоматы.
Эл. адрес: nazarov.vladimir.a@gmail.com

ТОПЧИЙ Павел Николаевич



Преподаватель кафедры космических радиотехнических систем Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 1990 году окончил Военный инженерный Краснознаменный институт им. А. Ф. Можайского по специальности «Радиоэлектронные средства».
Является автором 38 научных публикаций.
Область научных интересов – космические радиосистемы передачи информации.
Эл. адрес: pawel-topchy@yandex.ru

ЧУБИЧ Владимир Михайлович



Профессор, заведующий кафедрой теоретической и прикладной информатики Новосибирского государственного технического университета.
В 1984 году окончил с отличием Новосибирский электротехнический институт по специальности «Прикладная математика».
В 2014 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 120 научных и учебно-методических публикаций, включая две монографии.
Область научных интересов – стохастические системы, линейная и нелинейная фильтрация, квадратно-корневая фильтрация, идентификация систем, математическое моделирование, анализ данных, машинное обучение, искусственные нейронные сети.
Эл. адрес: chubich@ami.nstu.ru

СЕРГЕЕВ Михаил Борисович



Профессор, заведующий кафедрой вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения, почетный работник высшего профессионального образования РФ.
В 1980 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Электронные вычислительные машины».
В 2001 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 200 научных публикаций, 21 патента на изобретения и восьми монографий.
Область научных интересов – теория разрядных вычислений, ортогональные преобразования в телекоммуникациях, прикладной искусственный интеллект и др.
Эл. адрес: mbse@mail.ru

ТЮРЛИКОВ Андрей Михайлович



Профессор, ведущий научный сотрудник, заведующий кафедрой инфокоммуникационных технологий и систем связи Института радиотехники и инфокоммуникационных технологий Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 1980 году окончил Ленинградский институт авиационного приборостроения по специальности «Информационные системы управления».
В 2011 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 100 научных публикаций.
Область научных интересов – многоабонентные системы передачи данных.
Эл. адрес: turlikov@guap.ru

ШАЛЫТО Анатолий Абрамович



Профессор факультета информационных технологий и программирования Университета ИТМО, Санкт-Петербург, ученый секретарь НПО «Аврора».
В 1971 году окончил Ленинградский электротехнический институт им. В. И. Ульянова (Ленина) по специальности «Автоматика и телемеханика».
В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 250 научных публикаций, трех монографий и 70 изобретений.
Область научных интересов — системы логического управления, автоматное программирование.
Эл. адрес: shalyto@mail.ifmo.ru

ШТАНЬКО Сергей Владимирович



Доцент кафедры космической радиолокации и радионавигации Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 1999 году окончил Военный инженерно-космический университет им. А. Ф. Можайского по специальности «Радиоэлектронные системы».
В 2021 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором 57 научных публикаций и четырех свидетельств о регистрации программ для ЭВМ.
Область научных интересов — защита информации в радиотехнических комплексах управления, сбора и передачи информации.
Эл. адрес: craft2001@mail.ru

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Текст рукописи должен быть оригинальным, а цитирование и самоцитирование корректно оформлено.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, ORCID и электронный адрес одного из авторов. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени.

Простые **формулы** набирайте в Word, сложные с помощью редактора Mathtype или Equation. Для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта в Mathtype никогда не пользуйтесь вкладкой Other, Smaller, Larger, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; пробелы в формуле ставьте только после запятых при перечислении с помощью Ctrl+Shift+Space (пробел); не отделяйте пробелами знаки: + = – ×, а также пространство внутри скобок; для выделения греческих символов в Mathtype полужирным начертанием используйте Style → Other → bold.

Для набора формул в Word никогда не используйте вкладки: «Уравнение», «Конструктор», «Формула» (на верхней панели: «Вставка» — «Уравнение»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Подробнее см. http://i-us.ru/index.php/ius/author-guide

Иллюстрации:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Adobe Illustrator (*.ai); Coreldraw (*.cdr, версия не выше 15); Excel (*.xls); Word (*.docx); AutoCad, Matlab (экспорт в PDF, EPS, SVG, WMF, EMF); Компас (экспорт в PDF); веб-портал DRAW.IO (экспорт в PDF); Inkscape (экспорт в PDF);

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей и названий таблиц на русском и английском языках обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png, *.jpg с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение;

— экспортное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц, doi;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц, doi;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules): Литература и References.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Руководство для авторов» – http://i-us.ru/index.php/ius/author-guide.

Контакты

Куда: 190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru