ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

27. 2026 (ИЮНЬ)

Издание включено в перечень ВАК (специальности: 2.3.2, 2.3.6, 2.3.8, 5.2.4)

ВЕСТНИК

СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

№27
ИЮНЬ 2026

www.c3da.org

ISSN 2686-9373

Издатель: *Ассоциация РКЦФА*

Адрес редакции и издателя: 125167, Москва,
Ленинградский проспект, 43, стр.2, оф. 128
Тел.: +7 (499) 1573734

Подписано в печать 25.06.2026 г.
Тираж 500 экз.
Подписной индекс в каталоге «Пресса России»: 79111

Свидетельство о регистрации СМИ
ПИ № ФС 77-76187 от 08.07.2019 г.

Журнал включен в перечень рецензируемых научных изданий ВАК, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.
(2.3.2) Вычислительные системы и их элементы
(2.3.6) Методы и системы защиты информации, информационная безопасность
(2.3.8) Информатика и информационные процессы
(5.2.4) Финансы

РЕДАКЦИОННЫЙ СОВЕТ

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Современные процессы в области цифровизации и создания интеллектуальных систем настоятельно требуют углубленных фундаментальных исследований и в первую очередь – определения корпуса терминов в этих областях.

По мнению нашего уважаемого члена Редакционного совета Валерия Конявского, заведующего кафедрой "Защита информации" МФТИ, для работы над терминами необходимо создание экспертной группы. Как говорит Валерий Аркадьевич, о терминах бесполезно спорить, о них нужно договариваться.

В законодательстве без труда можно отыскать десятки и сотни различных определений одной сущности. При этом в вычислительной технике по сей день "ходячим анекдотом" является цитата из первого словаря на эту тему, получившая по имени научного редактора собственное наименование: «цикл Колмогорова» — «Информатика — см. Кибернетика, Кибернетика – см. Информатика».

Также и в сфере информационной безопасности на протяжении многих лет ведущие специалисты даже не могут договориться о том, от чего следует защищаться — от атак или от угроз. Научные школы только формируются, окончательная система терминов не установлена, что, конечно, не способствует выработке общих подходов.

В связи с этим по инициативе кафедры "Защита информации" МФТИ начинается работа по согласованию терминов глоссария в сфере ИБ с ориентацией в первую очередь на корректное описание защиты объектов критической инфраструктуры. В последствии сформированный и согласованный глоссарий будет применяться для дообучения больших языковых моделей с ориентацией на достижение экспертного уровня. Сформировано ядро коллектива экспертов, выбран инструментальный комплекс экспертной работы в системе управления знаниями (СУЗ).

Для повышения эффективности работы в экспертную группу приглашаются специалисты, которые готовы спорить с признанными авторитетами в этой сфере. Обязательные требования — ученая степень, наличие публикаций по направлению 2.3.6. в рейтинговых журналах, знание нормативных правовых документов в области информационной безопасности, а также стремление устранить имеющиеся противоречия в нормативных и нормативно-технических документах.

Полагаем, что ряд результатов будет обсуждаться и публиковаться на страницах нашего журнала.

Возвращаясь к основному содержанию двадцать седьмого выпуска, отметим, что в современном контексте цифровые технологии выступают не только в виде совокупности инструментов, но и в качестве новой среды человеческого присутствия. В таких условиях безопасность интеллектуальных систем требует нового языка расчёта, ответственности и доверия, деньги теряют вещественность и становятся знаком цифровой эпохи, а цифровая трансформация перестаёт быть отвлечённым сценарием будущего и становится повседневной практикой.

Выпуск открывает статья Ильи Лившица **«К вопросу оценивания экономической эффективности при реализации проектов обеспечения информационной безопасности систем ИИ»** раскрывает нам сферы, где искусственный интеллект оказывается не только источником новых возможностей, но и зоной нарастающей уязвимости. На пересечении экономики, нормативного анализа и информационной безопасности автор предлагает методику, позволяющую перевести риски систем ИИ в язык сценариев, численных оценок и управленческих решений. Здесь безопасность мыслится не как внешнее приложение к технологии, а как внутреннее, имманентное условие её надёжного и ответственного существования — от анализа угроз, стандартов и остаточных рисков до расчёта потерь, стоимости защитных мер и самой целесообразности инвестиций в устойчивость цифровых систем.

Исследование, представленное в статье Александра Обыдённова **«Интерпретация сущности денег: цифровой аспект»**, посвящено природе денег в современном мире, где привычные экономические формы уже невозможно понять вне логики электронных записей, токенов и цифрового рубля. При этом немаловажно, что деньги выступают не только в качестве средства расчёта, но и особой формой символического доверия, всё заметнее переходящего из материального мира в пространство цифровых кодов, платформ и новых правовых смыслов.

Весьма интересной и актуальной проблеме посвящена статья **«Эра персонального звука: от универсального мастеринга к адаптивным аудиоландшафтам на основе искусственного интеллекта»**. Публикация знакомит читателя с моделью, в которой универсальный мастеринг уступает место адаптивным аудиоландшафтам, рождающимся на стыке искусственного интеллекта, психоакустики и цифровой обработки сигналов. В

рассматриваемой модели звук воспроизводится с учётом особенностей слуха пользователя, типа устройства, характеристик пространства и даже контекста повседневной жизни, достигается цель сохранения художественного замысла и индивидуализации восприятия.

Материал **«Защита SIP-регистраций от атак методом динамической смены портов»** коллектива авторов переводит внимание читателя в ту зону цифровой инфраструктуры, где незаметные, на первый взгляд, технические параметры определяют устойчивость, безопасность и непрерывность связи. Авторы рассматривают IP-телефонию не просто как удобный корпоративный сервис, а как уязвимую среду, в которой предсказуемость стандартной точки входа облегчает атаки на регистрацию, и предлагают проактивный метод динамической смены портов как способ усложнить автоматизированное сканирование и снизить успешность злоумышленных воздействий.

Работа **«Взаимосвязи криптографии и лингвистики в историческом аспекте»** Игоря Кириллова и Екатерины Гончаренко обращает внимание читателя к историческому времени, где поэзия, шифр и филологический анализ оказываются родственными искусствами. От акростихов Эпихарма и скрытых смыслов античной литературы до трактата Аль-Кинди и изобретений Леона Баттисты Альберти перед читателем разворачивается история о том, как язык не только выражает мысль, но и умеет её скрывать, защищать и заново раскрывать.

Статья **«Использование искусственного интеллекта в правоохранительных органах КНР: опыт внедрения и перспективы»** знакомит читателя с пространством, в котором цифровая трансформация уже перестала быть отвлечённым сценарием будущего и становится повседневной практикой государственной власти. Здесь искусственный интеллект выступает не просто как технический инструмент ускорения юридических процедур, но и как новая форма институционального действия, в которой алгоритм, данные, экспертное знание и юридическая ответственность оказываются включены в единую, но ещё не до конца устойчивую систему.

В качестве логического продолжения темы использования цифровых технологий для развития общественных отношений представлен короткий комментарий (мнение) редакции **«О применениях искусственного интеллекта: от правоохранительной сферы к системе социального рейтинга»** о проактивном использовании искусственного интеллекта в широких социальных целях.

В статье **«Лемма Пошебякина и крах трансгуманизма»** главного редактора нашего журнала Андрея Щербакова, посвященной изучению вопросов потенциального увеличения продолжительности жизни, с давних пор волнующих человечество, на фоне смелых идей трансгуманизма на первый план выступает гипотеза о конечности самого человеческого сознания. В ходе анализа культурного аспекта, нейрофизиологических данных и математических аппроксимаций показано, что продление жизни не тождественно сохранению человека, а горизонт в 210-230 лет становится не только расчётной границей, но и метафорой предела человеческой ментальности.

Таким образом, складывается целостный рисунок номера, включающий несколько субстанциальных маршрутов через современность, в которой персонализируется звук, переосмысливается предел человеческого, расшифровывается история языка, меняется сущность денежного обращения и заново определяется цена безопасности интеллектуальных систем. У представленных вниманию читателя текстов есть одна общая черта – стремление понять, как в XXI веке меняются формы присутствия человека в мире, когда всё более значимыми становятся не только вещи, но и сигналы, структуры, коды, решения и пределы доверия к ним.

СОДЕРЖАНИЕ

УДК: 004.094

К вопросу оценивания экономической эффективности при реализации проектов обеспечения информационной безопасности систем ИИ

I.I. Livshitz

On the Issue of Assessing the Economic Efficiency of Implementing Projects to Ensure Information Security for AI Systems

Abstract. *This article examines the problem of assessing the economic efficiency of information security (IS) projects in modern artificial intelligence (AI) systems. Various approaches to building AI systems exist, but IS assessments for such projects are very limited. Economic efficiency aspects are considered even less frequently, as comparing the costs of IS measures and the results is extremely difficult to formalize due to the ambiguity of economic evaluation rules. These problems require an analysis of various solution options and the development of approaches to determining the numerical indicators of the economic efficiency of IS measures applied in modern AI systems. The most important result of the study is a new methodology for assessing the economic efficiency of IS projects in AI systems. The scientific novelty lies in the analysis of the requirements of various standards for assessing the efficiency of technical (software) AI systems and the unification of the approach for assessing the economic efficiency of new AI systems when selecting appropriate IS measures. This article will be of interest to specialists implementing IS projects for AI systems and experts assessing the efficiency of such projects.*

Keywords: *information security, artificial intelligence, residual risks, information security threats, information security measures.*

И.И. Лившиц
Доктор технических наук, профессор практики Университета ИТМО.
E-mail: Livshitz.il@yandex.ru

Аннотация. *В статье рассматривается проблема оценивания экономической эффективности при реализации проектов обеспечения информационной безопасности (ИБ) в современных системах искусственного интеллекта (ИИ). Существуют различные подходы к построению систем ИИ, но оценки ИБ в таких проектах представлены весьма ограниченно. Аспекты экономической эффективности рассматриваются еще реже, поскольку сопоставление затрат на меры ИБ и полученного результата весьма сложно формализовать по причинам неоднозначности экономических правил оценивания. Указанные проблемы требуют анализа различных вариантов решения и формирования подходов к определению численных показателей экономической эффективности мер ИБ, применяемых в современных системах ИИ. Наиболее важным результатом исследования является новая методика оценивания экономической эффективности при реализации проектов обеспечения ИБ в системах ИИ. Научная новизна заключается в анализе требований различных стандартов для оценивания эффективности технических (программных) систем ИИ и унификации подхода для оценивания экономической эффективности новых систем ИИ при выборе соответствующих мер ИБ. Статья будет интересна специалистам, реализующим проекты обеспечения ИБ для систем ИИ, и экспертам, выполняющим оценки эффективности таких проектов.*

Ключевые слова: *информационная безопасность, искусственный интеллект, остаточные риски, угрозы безопасности информации, меры информационной безопасности.*

ВВЕДЕНИЕ

Целью данной работы является оценка экономической эффективности при реализации проектов безопасности для систем ИИ. Оценку предполагается выполнять исходя из сценарного подхода, при котором типовые варианты негативного воздействия на системы ИИ могут быть приняты из нормативных документов, например, базы данных угроз (БДУ) ФСТЭК. В настоящее время представлены различные подходы к построению систем ИИ, но объективные оценки ИБ в таких проектах представлены весьма ограниченно. В частности, в ГОСТ Р 59898-2021[1] рассматриваются метрики качества систем ИИ, но введены значительные ограничения по существенным (значимым) характеристикам систем ИИ, которые критически ограничивают возможность применения данного национального стандарта РФ для оценки мер ИБ в составе «неделимой» единой системы ИИ.

В равной мере весьма ограниченно можно рассматривать известные стандарты ISO/IEC серии 42001, в которых приведены системные требования к созданию, внедрению и эксплуатации систем ИИ, но не приведено никаких требований для про-

[1] https://rosgosts.ru/file/gost/11/040/gost_r_59898-2021.pdf

верки критически важного «разумно предсказуемого неправильного использования» *(reasonably foreseeable misuse)* и соответствующего выбора мер ИБ [1,2,3]. В свою очередь, «классический» стандарт ISO/IEC серии 27001 не содержит конкретных мер по обеспечению ИБ для систем ИИ, хотя, при определенных ограничениях, некоторые организационные (А.5) и технические (А.8) меры ИБ могут рассматриваться.

Аспекты экономической эффективности рассматриваются еще реже, поскольку сопоставление затрат на меры ИБ и полученного результата защиты конкретной системы весьма сложно формализовать по причинам неоднозначности экономических правил оценивания. Стандарт ISO/IEC серии 42005 описывает влияние систем ИИ *(Artificial intelligence system impact assessment)*, но не устанавливает ни метрик, ни специфических процедур в отношении мер ИБ.

В рамках данной работы выполнен переход от простой оценки возможных потерь (хорошо известной по российским и иностранным публикациям и основанной на классических стандартах ISO/IEC серии 22301 (обеспечение непрерывности бизнеса), ISO/IEC серии 42005 (оценивание влияния систем ИИ), ISO/IEC серии 27001 (системы менеджмента ИБ) и иных. Рассматривается новая методика, которая оперирует численными оценками затрат на меры ИБ и показателями экономической эффективности, что совокупно позволяет оценить целесообразность реализации проекта обеспечения ИБ для конкретной системы ИИ.

Формализация объекта исследования

Объектом исследования является система ИИ. Особенность данного объекта – высокая неопределённость «генерирования» выходного результата, не позволяющая надежно верифицировать функции безопасности (встроенные или «наложенные») в компонентах ИИ, что может негативно воздействовать на объекты критической инфраструктуры (КИИ), в состав которых встраиваются эти компоненты. Представленное исследование продолжает работы автора по тематике оценивания уровня обеспечения ИБ для объектов КИИ [4,5].

Постановка задачи

В представленной публикации в рамках поставленной проблемы рассматриваются следующие практические задачи применительно к системам ИИ:

- систематизация научных подходов, применяемых при оценке последствий инцидентов ИБ;
- расчет потенциальных потерь от реализации инцидентов ИБ;
- оценка стоимости внедрения и эксплуатации мер ИБ;
- оценка экономической эффективности инвестиций в меры ИБ.

Ограничения методики

Основными ограничениями представленной новой методики являются:

• выбор мер ИБ из национальной базы ФСТЭК России;

• оценка рисков (остаточных рисков) по международным стандартам ISO/IEC;

• апробация ограничена расчетным примером с указанием диапазонов всех значений переменных с сопоставлением объективных данных по серии кейсов из рассматриваемой предметной области.

Для снижения рисков применения новой методики дополнительно применены следующие процедуры верификации: оценка логической непротиворечивости, оценка расчетных показателей по сравнению с граничными условиями, оценка корреляции полученных результатов с доступными (экспертными) оценками. В чем ограничение?

Анализ погрешностей представленной методики

В представленной новой методике принимаются следующие основные источники погрешностей применительно к системам ИИ:

• неопределенность длительности простоя бизнес-процессов по причине инцидента ИБ;

• различия в стоимости конкретных реализаций систем ИИ;

• сложность оценки нематериальных потерь (репутация и пр.);

• зависимость последствий (потерь) от масштаба инцидента ИБ.

В отличие от формальной оценки защищенности (например, по методике ФСТЭК[2] 2025 г.), экономическая оценка систем ИИ носит объективный вероятностный (апостериорный) характер. Для снижения влияния погрешностей во всех расчетах далее применяется сценарный подход, включающий 3 дискретных оценочных уровня:

• минимальные потери (консервативный сценарий);

• наиболее вероятные потери (базовый сценарий);

[2] https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-noyabrya-2025-g

• максимальные потери, катастрофа (стресс-сценарий).

Поиск и систематизация научно-методических ресурсов

В представленной работе 1-й практической задачей является систематизация научных подходов, применяемых при оценке последствий инцидентов ИБ. Для решения этой задачи применяются методические подходы, основанные на:

• сценарном анализе;

• оценке потерь при инциденте ИБ;

• расчете эффективности инвестиций.

Нормативно-методическую базу предлагается формализовать в следующем составе:

• БДУ ФСТЭК (угрозы безопасности информации (УБИ) применительно к системам ИИ);

• ISO/IEC (ГОСТ Р ИСО/МЭК) серии 27001 (меры ИБ, оценка рисков и остаточных рисков);

• ISO/IEC (ГОСТ Р ИСО/МЭК) серии 42001 (требования к системам менеджмента ИИ);

• ISO/IEC (ГОСТ Р ИСО/МЭК) серии 42005 (оценка влияния систем ИИ).

Сценарный подход применяется в связи с высокой неопределенностью последствий инцидентов ИБ (особенно в системах ИИ) и позволяет учитывать различные уровни воздействия на компоненты систем высшей иерархии (например, объекты КИИ), в которые могут быть встроены системы ИИ. Таким образом, в предложенной методике реализуется аналитический механизм, позволяющий связать значение уровня ИБ с экономическими (численными) показателями систем ИИ.

ОБЗОР ЛИТЕРАТУРЫ

По представленной проблеме рассмотрим кратко доступные публикации. Известны работы российских специалистов [6 – 9], касающиеся объекта исследования.

В работе [6] кратко рассмотрена эволюция научных школ в области экономики ИБ и ограниченно изучены экономические показатели технологических инвестиций применительно к защите информации. Среди показателей перечислены: «традиционный» ROI, сбалансированная система показателей (система Нортона-Каплана), стоимостной инжиниринг и иные. Однако никаких нормативных требований (стандартов) или системы прослеживаемости от требований до выбираемых мер защиты не представлено.

В публикации [7] представлены значения индекса готовности отраслей к внедрению ИИ, при этом отмечено, что в 2021 г. такой индекс составил 3,2 балла (из 10), в 2023 г. – 3,7 баллов, а в 2024 г. – только 3,3 балла. Примечательно, что для 80% исследуемых отраслей значение индекса не превышает 4 баллов, что может указывать на системные недостатки при экономической оценке проектов ИИ. К сожалению, в представленной работе нет никаких метрик, по которым можно было бы оценивать применение систем ИИ и, соответственно, нет никаких показателей (качественных или количественных), характеризующих обеспечение ИБ.

В источнике [8] приведены общие соображения о целях, методах и влиянии цифровизации на экономическую безопасность, отражены зависимости финального результата от угроз технологической зависимости, уязвимостей данных и киберрисков. Отметим, что в данной работе нет никаких численных данных или метрик, по которым можно было бы оценивать влияние современных технологий (включая ИИ), и также нет никаких показателей (качественных или количественных), характеризующих меры ИБ.

В статье [9] рассматривается влияние ИИ на систему авиационной безопасности, а также преимущества и риски, вызванные внедрением этого типа систем. Даются общие рекомендации по предотвращению потенциальных преступлений и обеспечению безопасности пассажиров и сотрудников. Однако никаких нормативных требований (федеральных авиационных норм, правил и стандартов) или системы экономической оценки для выбираемых мер ИБ не представлено.

По исследуемому вопросу известны работы зарубежных специалистов [10 – 13].

В исследовании [10] приводятся примеры применения систем ИИ для решений в области управления учётными записями и правами доступа (Identity and Access Management, IAM). Отмечается влияние показателей (выявление аномалий, масштабирование, соответствие регуляторным требованиям и пр.) на общие показатели производительности и надежности. К достоинствам работы можно отнести внимание к «аудиторскому следу» (audit trail), что дает основание оценивать уровень ИБ в новых решениях с участием компонент ИИ.

В работе [11] представлены оценки влияния технологий ИИ для конкретного объекта – аэропорта. Заявленное улучшение результативности систем ИБ на базе компонентов ИИ рассматривается как прямое влияние на общую операционную эффективность. К достоинствам работы можно отнести внимание к «человеческому» фактору (интеграция и адаптация систем ИИ) и общей «готовности» при-

менения новых решений для обеспечения безопасности международного аэропорта.

В статье [12] приведены общие соображения о влиянии современных технологий (ИИ и блокчейн) на системы передачи финансовых данных. Поставленная задача затрагивает оптимизацию управления высокоскоростных систем с учетом требований безопасности, регулирования и технических решений. Работа ограничена рассмотрением комбинации систем ИИ и блокчейна, но без каких-либо обобщенных оценок экономической эффективности мер ИБ.

В публикации [13] рассматривается гибридный поход к анализу данных, размещённых в облачной инфраструктуре и в локальных (on-premises) центрах обработки данных (ЦОД). Предлагается применять системы ИИ для управления сетевой инфраструктурой по единым унифицированным правилам при выполнении аудитов на примере глобальной сети ритейла. К достоинствам работы можно отнести внимание к специфике требований ИБ в сложной инфраструктуре (сегментация, управление обновлениями безопасности, выявление уязвимостей и пр.), а также соблюдение требований регуляторов (например, PCI-DSS и GDPR).

Отдельно приведём работы в области «AI safety governance»[3] [14,15,16].

В работе [14] рассматриваются вопросы применения технических мер защиты и политик для обеспечения операционной устойчивости в различных структурах: крупных ЦОД (Google), облачных и локальных. Соответственно, управление рисками потребует адаптации мер защиты к локальным приложениям ИИ, а также распространения политик ИИ на разные типы экосистем, в том числе с учетом государственных систем регулирования.

В статье [15] рассматривается проблема существенных финансовых причин для уклонения от государственного контроля в области применения систем ИИ, отмечается, что текущая ситуация не позволяет изменить правила корпоративного управления. Представленный подход предполагает, что работники компаний играют важную роль в разработке безопасных систем ИИ, а государственный надзор – при обеспечении независимого тестирования по требованиям безопасности.

В работе [16] отмечен риск применения современных моделей менеджмента, который заключается в невозможности обеспечения безопасности систем ИИ обычными системами защиты. Системы ИИ дают значительные преимущества для оптимизации безопасности в облачных решениях, в том числе при обнаружении атак, предсказании уязвимостей до наступления инцидентов и адаптивных стратегий защиты. Примечательно, что в данной публикации отмечена роль систем шифрования на базе решений ИИ в новой системе интеллектуального управления ключами и дифференцированных методов обеспечения конфиденциальности.

Кроме того, представляют определенный интерес работы в области «Cyber risk quantification»[4] [17- 20].

В публикации [17] рассмотрены примеры интеграции физических (physical) и цифровых (digital) технологий в рамках 4-й индустриальной революции. Соответственно, показано увеличение поверхностей атак на киберфизические системы (производства, склады, логистические комплексы и пр.). Для противодействия таким атакам предложено применять FAIR методологию как известный подход для количественной оценки рисков применительно к крупнейшим логистическим комплексам Скандинавии.

В статье [18] представлен анализ практики применения оценки рисков для сегмента малого и среднего бизнеса. Отмечается, что чувствительность данного сегмента к киберугрозам более чем в шестьдесят раз превышает уровень крупных компаний. Эта ситуация объясняется тем, что малые предприятия часто игнорируют затраты на инфраструктуру кибербезопасности, поэтому важно формировать скоринговые модели рисков для выполнения количественных оценок и сопоставления с финансовыми потерями.

В работе [19] показано, как метод количественной оценки рисков позволяет предоставить более точные и объективные результаты по сравнению с традиционными качественными методиками. Предлагаемый подход базируется на количественной оценке рисков кибербезопасности, что позволяет обеспечивать численные показатели вероятностей киберугроз и операционного ущерба. Данный подход признается важным компонентом корпоративной системы управления рисками с фокусом на обеспечение защиты критически важных активов.

Оценка степени готовности кибербезопасности как способности организации к цифровой трансформации при увеличении поверхности атак и регуляторных ограничений дается в публикации [20]. В отличие от существующих подходов, уровень готовности рассматривается не только как функция технических мер защиты и зрелости уровня зако-

[3] Система процессов, стандартов и инструментов, обеспечивающих безопасное и этичное применение искусственного интеллекта.

[4] Процесс перевода киберрисков в измеримые, объективные финансовые или операционные показатели.

нодательного соответствия, но как способность высшего менеджмента формировать устойчивую систему восстановления. Соответственно, требуется обеспечение количественных оценок рисков, и разработка стратегии, состоящей их 4 элементов: приверженность руководства (на входе), механизм принятия решений, интеграция с требованиями регуляторов и измеримые оценки кибербезопасности (на выходе).

ОБЗОР БАЗЫ ДАННЫХ УГРОЗ ФСТЭК ПО ОБЛАСТИ ИИ

Для целей данной публикации рассмотрим описание УБИ применительно к системам ИИ, в соответствии с БДУ ФСТЭК России[5]. Указано, что исключены из рассмотрения УБИ, связанные с качеством моделей ИИ. Следует принять во внимание, что известный национальный стандарт ГОСТ Р 59898-2021[6], устанавливающий требования к качеству систем ИИ, исключает специальные характеристики (в том числе ИБ) из перечня верифицированных. Этот аспект будет более подробно рассмотрен далее. Кратко приведём несколько способов реализации УБИ применительно к системам по методике ФСТЭК (Таблица 1).

В документах ФСТЭК России не содержится численных методов оценивания УБИ, соответственно, оценка возможности реализации УБИ систем ИИ проводится в соответствии с Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России[7] 2021 г.

Таблица 1

Способы реализации УБИ применительно к системам ИИ

№	УБИ	Способ реализации
1	УБИ в инфраструктуре разработчика системы ИИ	СП.5 – Несанкционированная модификация (отравление) наборов обучающих данных СП.6 – Несанкционированная модификация параметров (весов) модели машинного обучения и LoRA, а также данных RAG
2	УБИ в инфраструктуре оператора системы ИИ	СП.4 – Модификация (изменение) параметров (весов) модели машинного обучения в целях нарушения функционирования системы ИИ СП.5 – Модификация конфигураций модели машинного обучения и агентов (например, системного промпта) в целях нарушения функционирования сис- темы ИИ

Следует отметить, что хотя в указанной методике (п. 2.7 а) упоминается привлечение специалистов, обладающих знаниями основ оценки рисков, тем не менее, нет требований по оценке применяемых мер ИБ, нет установленных критериев оценки и, соответственно, нет оценки остаточных рисков. К сожалению, указанная методика ФСТЭК России существенно отстает по уровню методологии обеспечения ИБ от актуальных стандартов ISO/IEC и соответствующих национальных стандартов ГОСТ (например, серии 27001 и 42001).

Примечательно, что в работах [2,3] отражены аспекты выявления и оценивания рассмотренных выше УБИ и конкретных способов реализации для систем ИИ, и в работах [21,22,23] – для АСУТП, соответственно.

СТАНДАРТ ГОСТ Р 59898-2021

Национальный стандарт ГОСТ Р 59898-2021 устанавливает общие требования к качеству систем ИИ и может быть принят как руководство по анализу различных решений по критериям (например, точность, полнота, избирательность и пр.). Однако для конкретной цели оценивания мер ИБ в системах ИИ этот стандарт, к сожалению, неприменим по ряду существенных причин:

1. В разделе 1 отмечено, что настоящий стандарт не может быть использован для систем «сильного» или «общего» ИИ, однако именно для систем ИИ такого класса предусмотрены меры ИБ, гарантирующие отсутствие недопустимого риска («остаточного риска» в терминах ISO/IEC 27001). Как отмечалось выше, ФСТЭК России также не предусматривает установления критериев и оценку остаточного риска.

2. Определение «безопасность» (*safety*, п. 3.4) как свойство системы ИИ сохранять состояние, характеризующееся отсутствием недопустимого риска, при использовании ее по назначению в условиях, предусмотренных изготовителем.

3. Определение «существенные (значимые) характеристики системы ИИ» как характеристики сис-

[5] https://bdu.fstec.ru/threat/ai

[6] https://rosgosts.ru/file/gost/11/040/gost_r_59898-2021.pdf

[7] https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

темы ИИ, определяющие ее функциональность, надежность и безопасность при решении конкретной прикладной задачи. Подтверждение соответствия установленным требованиям должно быть выполнено потребителем системы или организациями, ответственными за регулирование вопросов создания и применения систем ИИ (п. 3.21). Для данного определения критически важно примечание: характеристики систем ИИ, подтверждение соответствия которых установленным требованиям может быть выполнено исключительно разработчиком системы, не относятся к существенным.

В таблице 2 рассматриваемого стандарта приведены примеры существенных характеристик и субхарактеристик систем ИИ. В частности, для группы характеристик **«Безопасность»** установлена существенная характеристика – **«Защищенность»** (в оригинале *security*) и предложены следующие субхарактеристики:

- конфиденциальность (*confidentiality*);
- целостность (*integrity*);
- неотказуемость (*non-repudiation*);
- подотчетность (*accountability*);
- подлинность (*authenticity*).

Определенно, группа **«Безопасность»** не может быть просто сведена к одной простейшей существенной характеристике **«Защищенность»**. Это противоречит как требованиям ФСТЭК России, так и известным стандартам: международным (ISO/IEC) и национальным (ГОСТ Р ИСО/МЭК) серии 27001, 22301 и 20000-1. С учетом критически важного примечания по п. 3.21, как было показано выше, ситуация с оценкой мер ИБ объективно неопределенная, т.к., во-первых, не все производители выполняют такие оценки в рамках внутренних процедур, и во-вторых – практически отсутствуют результаты внешних независимых тестов систем ИИ по требованиям ИБ.

СТАНДАРТ ISO/IEC СЕРИИ 42005

Стандарт ISO/IEC 42005:2025[8] определяет аспекты влияния систем ИИ, и для целей данной публикации необходимо рассмотреть ключевое понятие – «разумно предсказуемое неправильное использование» (*reasonably foreseeable misuse*, п. 3.6), как использование систем ИИ способом, изначально не предусмотренным разработчиком (поставщиком), но которое может быть результатом предсказуемого поведения конечных пользователей. С учетом данного определения рассмотрим контекст рассматриваемого стандарта и сформируем примеры метрик, которые могут быть применены при оценивании мер ИБ в отсутствие прямых аналогов в существующих международных стандартах ISO/IEC:

1) ожидания заинтересованных сторон (включая пользователей) применительно к оценкам воздействия систем ИИ (п. 5.4.1. e);

2) распределение обязанностей по организации процесса утверждения и эскалации при необходимости (п. 5.6. f);

3) определение функциональных возможностей системы ИИ, например, прогнозы, типы данных, алгоритмы, модели (п. 6.3.2. a);

4) определение показателей, используемых для оценки эффективности моделей, например, точность, матрица ошибок, среднеквадратичная ошибка (6.5.4. g);

5) примеры ущерба:

- утечка персональных данных (ПДн), использованных при обучении моделей;
- повторное использование ПДн в других системах, где их обработка не предусмотрена;
- эксплуатация уязвимостей системы ИИ, которые могут позволить использовать ее в непреднамеренных (незаконных и непредусмотренных) целях.

ЭКОНОМИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ

Для решения 2-й практической задачи – расчета потенциальных потерь, необходим перевод результатов оценки в бизнес-метрики. Для этого используется экономическая модель, в которой потенциальные потери от инцидента ИБ определяются как:

$$Loss_R = \sum_{j=1}^{m} Loss_j k_j$$

$$\sum_{j=1}^{m} k_j = 1$$

где:

$Loss_R$ – результирующая оценка потерь;

$Loss_j$ – оценка по виду потерь;

k_j – весовой коэффициент каждого вида потерь;

m – количество видов потерь, учитываемых в экономической модели.

В представленной работе предлагается учитывать следующие виды потерь, которые ранее кратко были рассмотрены в публикациях [24,25], результаты представлены в таблице 2:

[8] https://www.iso.org/standard/42005

Таблица 2

Виды потерь по причине инцидента ИБ в системе ИИ

Индекс, j	Обозначение	Значение
1	$Loss_1$	Прямые потери от простоя
2	$Loss_2$	Потери на восстановление
3	$Loss_3$	Потери на компенсации (страховые выплаты)
4	$Loss_4$	Потери на логистику (закупка и доставка)
5	$Loss_5$	Потери на тестирование и комплексирование
6	$Loss_6$	Потери на резервное копирование и тестирование
7	$Loss_7$	Потери на репутацию

Оценка инцидентов ИБ в системах ИИ

Для оценки «стоимости» инцидентов ИБ рассмотрим наиболее релевантные кейсы применительно к системам ИИ:

1. В экспертной оценке ExploitDog «ИИ ускорил атаки быстрее, чем компании успели перестроить защиту»[9] показано, что ущерб от одного киберинцидента в 2025 г. в среднем составляет 100–200 млн. руб., и это только прямые финансовые потери (без учета репутационного ущерба), при этом 30% утечек в 2025 г. — результат использования ИИ сотрудниками.

2. Согласно данным AI Index Report 2025, количество зарегистрированных инцидентов достигло рекордного показателя – 233 случая в 2024 г., что на 56,4% больше по сравнению с 2023 г. [1]. Из таблицы «Дипфейки и манипуляции с медиаконтентом» видно, что самая большая доля 28% — это доля инцидентов ИИ (что подтверждает предыдущий кейс).

3. В отчете «Code Red 2026: Актуальные киберугрозы для российских организаций»[10] Positive Securities отмечеается, что в ближайшие годы активная цифровизация и внедрение систем ИИ будут расширять поверхность атак, что может привести к большему количеству успешных компрометаций и, соответственно, ущербу.

4. В обзоре «Искусственный интеллект в промышленности: страхование рисков»[11] научного журнала «Промышленные страницы» приведены примеры критических сбоев в работе систем ИИ:

• В 2023 г. в Магнитогорске произошёл сбой системы ИИ, отвечающей за контроль качества продукции на металлургическом заводе. В результате потребителям была поставлена некачественная сталь, что привело к ущербу более 50 млн. руб.

• В 2024 г. на химическом заводе в Казани система ИИ, управляющая АСУТП, допустила ошибку, что привело к выбросу вредных веществ и травмам 12 рабочих, а только страховые выплаты превысили 15 млн. руб.

С учетом приведенных объективных данных статистики, можно полагать «стоимость» одного инцидента ИБ в системах ИИ в РФ равной 50 млн. руб. (только прямые затраты, без нематериального ущерба). По иностранным данным оценки ущерба несопоставимы (67,4 млрд. долларов при 233 инцидентах дают средний ущерб около 289 млн. долларов для одного инцидента), но эта оценка включает все затраты, в том числе существенные нематериальные издержки. В качестве базовой оценки «стоимости» одного инцидента ИБ в системах ИИ для решения 2-й практической задачи обоснованно принято значение 50 млн. руб. (как доля 28% по кейсам №1 и №2 и как ущерб, равный по номинал по кейсу № 4).

Сценарный подход

Для учета неопределенности и диапазонов возможных последствий от инцидентов ИБ в системах ИИ используется сценарный анализ:

• консервативный сценарий — локальный инцидент;

• базовый сценарий — типовой инцидент;

• стресс-сценарий — масштабный отказ инфраструктуры (катастрофа).

Спецификации сценариев для учета потерь по причине инцидента ИБ в системах ИИ приведены в таблице 3.

[9] https://hi-tech.mail.ru/articles/142000-ii-uskoril-ataki-bystree-chem-kompanii-uspeli-perestroit-zashitu/

[10] https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id2

[11] https://indpages.ru/tech/iskusstvennyj-intellekt-v-promyshlennosti-strahovanie-riskov

Таблица 3

Спецификации сценариев для учета потерь по причине инцидента ИБ в системе ИИ

Сценарий	Консервативный	Базовый	Стресс-сценарий
Тип инцидента	Разовый	Двойной (каскадный)	Системный отказ
Распространение	Локально	Локально	Масштабный отказ
MTPD, час	2	6	24
RTO, час	1	2	8
Стоимость инцидента ИБ (экспертная оценка), млн. руб.	50	100	220
Доля затрат меры ИБ (тестирование, валидация и пр.), %	1	5	10

Методика оценки эффективности мер ИБ для систем ИИ

Предложенная новая методика определяет результирующую оценку эффективности мер ИБ по формуле (1):

$$R_{IT-Security} = \frac{Loss_R - (Sec_{Emb} + Sec_{Add})}{Loss_R} \quad (1)$$

$$R_{IT-Security} \geq 0$$

где:

$R_{IT\text{-}Security}$ — результирующая оценка эффективности мер ИБ (%);

$Loss_R$ — результирующая оценка потерь;

Sec_{Emb} — совокупная стоимость встроенных (security by design) мер ИБ;

Sec_{Add} — совокупная стоимость дополнительных («наложенных») мер ИБ.

Показатель $R_{IT\text{-}Security}$ отражает экономическую эффективность внедрения мер ИБ, увязывая результирующую оценку потерь и две отдельные метрики стоимости мер ИБ – встроенные (Sec_{Emb}) и дополнительные («наложенных») меры ИБ (Sec_{Add}). Представленная формула (1) учитывает, что при разработке конкретной системы ИИ обеспечены определенные встроенные функции ИБ (безопасность кода, тестирование, управление конфигурациями и пр.), а также могут быть дополнительно реализованы иные меры ИБ. Но следует признать, что, объективно, ни одна мера ИБ или комплекс мер ИБ не дают абсолютной защиты, что приводит к определенному ущербу, соответственно, знаменатель формулы (1) никогда не будет равен нулю. Далее это обстоятельство будет рассмотрено более подробно на отдельном примере. Представленная методика позволяет объединить сценарный подход и экономическую оценку, что обеспечивает количественную оценку последствий на принятом «финансовом языке» бизнеса.

Выбор и обоснование мер ИБ для систем ИИ

Для решения 3-й практической задачи рассмотрим различные типы мер ИБ для систем ИИ по двум основным группам – регуляторным и техническим. Среди регуляторных мер рассмотрим актуальный закон РФ о страховании рисков от внедрения ИИ[12] в рамках работы экспериментальных правовых режимов (ЭПР). Закон позволяет учреждать ЭПР в различных сферах, включая проектирование, производство и эксплуатацию транспортных средств, строительство, промышленное производство и иные направления по решению правительства. В КНР[13] известны оценки инвестиций в ИИ (4,9 млрд. долларов в 2018 г. и до 140 млрд. долларов в прогнозе до 2030 г.). С учетом данных McKinsey, приведенных выше, логично предположить долю затрат на меры защиты ИБ в том же порядке – десятки миллиардов долларов.

Вторая группа мер ИБ определяется регуляторами в РФ, например, ФСТЭК России. Для анализа дополнительных («наложенных») мер защиты рассмотрим актуальный приказ ФСТЭК России[14] № 117. Поскольку иные нормативные документы, устанавливающие какие-либо меры ИБ применительно к системам ИИ, в настоящее время в РФ не утверждены, примем данный Приказ ФСТЭК как базовый для систем ИИ. С учетом постановки третьей практической задачи рассмотрим также и наиболее релевантные меры защиты ИБ по ГОСТ Р ИСО/МЭК 27001, применимые для систем ИИ (таблица 4):

[12] https://www.interfax.ru/russia/967980

[13] https://www.itsjournal.ru/articles/special-report/iskusstvennyy-intellekt-zashchitit-i-zashchititsya/

[14] https://normativ.kontur.ru/document?moduleId=1&documentId=500478

Таблица 4

Меры ИБ, применимые для систем ИИ

№	Мера	Норматив	
		Приказ ФСТЭК 117	ГОСТ Р ИСО/МЭК 27001
1	Обеспечение защиты информации при использовании ИИ	п. 34. т)	А.5.1
2	Выполнение мониторинга ИБ с применением доверенных технологий ИИ	п. 49	А.5.22
3	Исключение несанкционированного доступа к информации или воздействия на ИС, а также использования ИС не по их назначению за счет воздействия на наборы данных, применяемые модели ИИ и их параметры, процессы и сервисы по обработке данных и поиску решений	п. 60	А.5.10
4	Определение шаблонов запросов пользователей, направляемых в системы ИИ и обеспечение контроля соответствия запросов установленным шаблонам	п. 61 а)	А.8.26
5	Разработка статистических критериев для выявления недостоверных ответов систем ИИ для последующего сбора и анализа недостоверных ответов	п. 61 в)	А.8.28 А.8.33
6	Обеспечение реагирования на недостоверные ответы систем ИИ посредством ограничения области принимаемых решений и (или) реализации функций ИС на основе недостоверных ответов систем ИИ	п. 61 г)	А.8.33 А.8.34
7	Проведение регулярного независимого аудита ИБ	-	9.2.2
8	Выполнение оценки и обработки рисков (остаточных рисков) ИБ	-	6.1.3

Оценка эффективности мер ИБ в проектах систем ИИ

Для решения 4-й практической задачи рассмотрим 3 сценария и оценки эффективности мер ИБ в системах ИИ на следующем примере (таблица 5).

Все оценки ущерба $Loss_R$ и затрат (раздельно представлены Sec_{Add} и Sec_{Emb}) даны в млн. руб. Значения $R_{IT\text{-}Security}<0$ не соответствуют граничным условиям и исключены из рассмотрения.

Таблица 5

Оценка эффективности мер ИБ

Сценарий 1 (Консервативный)				Сценарий 2 (Базовый)				Сценарий 3 (Стресс-тестирование)			
$Loss_R$	Sec_{Emb}	Sec_{Add}	$R_{IT\text{-}Sec}$, %	$Loss_R$	Sec_{Emb}	Sec_{Add}	$R_{IT\text{-}Sec}$, %	$Loss_R$	Sec_{Emb}	Sec_{Add}	$R_{IT\text{-}Sec}$, %
50,00	1	5,00	88	100,00	5	10,00	85	200,00	20	20,00	80
25,00	1	2,50	86	50,00	5	5,00	80	100,00	20	10,00	70
12,50	1	1,25	82	25,00	5	2,50	70	50,00	20	5,00	50
6,25	1	0,63	74	12,50	5	1,25	50	25,00	20	2,50	10
3,13	1	0,31	58	6,25	5	0,63	10	12,50	20	1,25	-
1,56	1	0,16	26	3,13	5	0,31	-	6,25	20	0,63	-
0,78	1	0,08	-	1,56	5	0,16	-	3,13	20	0,31	-

Очевидно, что $R_{IT\text{-}Security}$ по формуле (1) равен нулю при равенстве оценок ущерба $Loss_R$ и затрат Sec_{Add}, но на практике владельцы бизнеса крайне редко «вкладывают» заранее в безопасность и полное покрытие всех возможных ущербов, поскольку реализуется эффективная стратегия управления апостериорными рисками. Графический результат оценки эффективности мер ИБ по формуле (1) представлен на рис. 1, что позволяет выявить следующую закономерность: при фиксировании затрат на меры ИБ (Sec_{Add}) по норме 10% от стоимости предполагаемого ущерба и фиксировании затрат на встроенные меры Sec_{Emb} по нормам для различных сценариев (таблица 3) оценка эффективности $R_{IT\text{-}Security}$ смещается «наверх», т.е. обеспечивается защита от большего числа УБИ для систем ИИ.

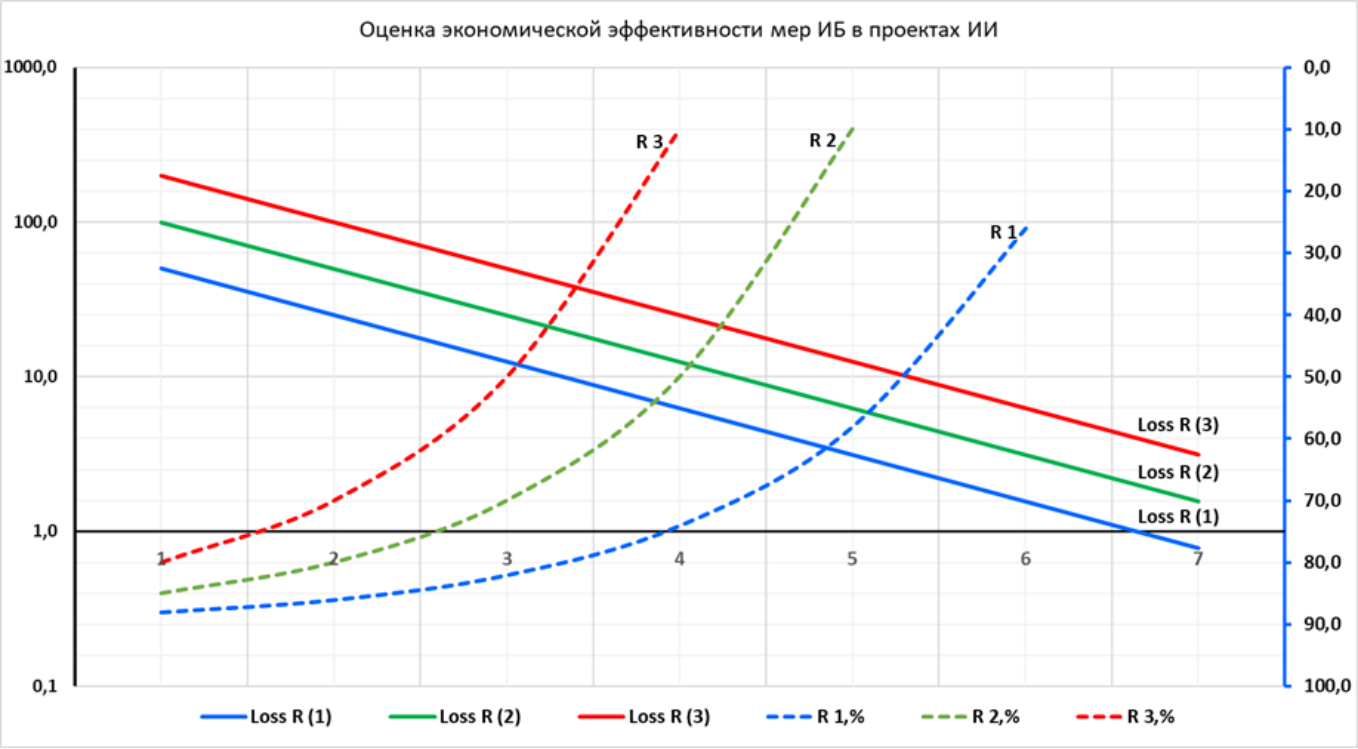

Рис. 1. Оценка эффективности мер ИБ в проектах ИИ

Представляется более интересным исследовать зависимость итогового значения $R_{IT\text{-}Sec}$ от Sec_{Emb}, принимая во внимание предположение, что методы разработки всех систем ИИ основаны на подходе «security by design». Соответственно, рассмотрим предположение, что значение Sec_{Emb} объективно может оказывать большее влияние, чем дополнительные («наложенные») меры ИБ (Sec_{Add}), которые, как правило, имеют установленные бюджетные ограничения эксплуатирующих организаций.

Для более детальной оценки экономического обоснования мер ИБ рассмотрим исследование[15], которое выявило тренд финансовых издержек среди компаний из РФ. Примечательно, что в данном исследовании отмечается «исчерпание» риск-ориентированного подхода, поскольку утечки данных являются неизбежными и важнее не выполнить оценку рисков, а определить «финансовый возврат». Более детальное обоснование мер ИБ может быть выполнено с учётом исследования 2025 г.[16]. Представлен важный вывод, что для крупного бизнеса 1 руб., потраченный на кибербезопасность, позволяет предотвратить до 3,5 руб. прямого ущерба. Этот показатель можно ввести как мультипликатор μSec при исследовании проблемы оценивания экономической эффективности при реализации проектов обеспечения ИБ в современных системах ИИ в дальнейшем.

С учетом мультипликатора μ_{Sec} рассмотрим уточненную формулу для расчета $R'_{IT\text{-}Security}$ с учетом зависимости только от $Sec_{Emb.}$

$$R'_{IT-Security} = \frac{Loss_R - (Sec_{Emb} \cdot \mu_{Sec})}{Loss_R + (Sec_{Emb} \cdot \mu_{Sec})} \quad (2)$$

$$R'_{IT-Security} \geq 0$$

[15] https://companies.rbc.ru/news/vB5R3l06S1/rossijskie-kompanii-peresmatrivayut-podhod-k-zakupke-szi/

[16] https://www.securitylab.ru/news/570739.php

Представленная формула (2) описывает оценку эффективности $R'_{IT\text{-}Sec}$ с учётом только встроенных мер ИБ (Sec_{Emb}), допуская, что при разработке конкретной системы ИИ достаточно реализации подхода «security by design». При Sec_{Emb}=0 или μ_{Sec}=0 формула (2) обеспечивает $R'_{IT\text{-}Sec}$=1, т.е. базовые начальные условия, как условия логической валидации метода.

При фиксированном мультипликаторе μ_{Sec}=3,5, фиксировании затрат на встроенные меры Sec_{Emb} по нормам для различных сценариев (таблица 3) и фиксированной переменной Sec_{Add}=0, обеспечивается нелинейное снижение $R'_{IT\text{-}Sec}$, результаты представлены в таблице 6. Значения $R'_{IT\text{-}Security}$<0 не соответствуют граничным условиям и исключены из рассмотрения.

Таблица 6

Оценка эффективности мер ИБ при фиксированном Sec_{Add}

Сценарий 1 (Консервативный)					Сценарий 2 (Базовый)					Сценарий 3 (Стресс-тестирование)				
$Loss_R$	Sec_{Emb}	Sec_{Add}	$R_{IT\text{-}Sec}$, %	$R'_{IT\text{-}Sec}$, %	$Loss_R$	Sec_{Emb}	Sec_{Add}	$R_{IT\text{-}Sec}$, %	$R'_{IT\text{-}Sec}$, %	$Loss_R$	Sec_{Emb}	Sec_{Add}	$R_{IT\text{-}Sec}$, %	$R'_{IT\text{-}Sec}$, %
200,00	1	0,00	99,50	96,56	200,00	5	0,00	97,50	83,91	200,00	10	0,00	95,00	70,21
100,00	1	0,00	99,00	93,24	100,00	5	0,00	95,00	70,21	100,00	10	0,00	90,00	48,15
50,00	1	0,00	98,00	86,92	50,00	5	0,00	90,00	48,15	50,00	10	0,00	80,00	17,65
25,00	1	0,00	96,00	75,44	25,00	5	0,00	80,00	17,65	25,00	10	0,00	60,00	–
12,50	1	0,00	92,00	56,25	12,50	5	0,00	60,00	–	12,50	10	0,00	20,00	–
6,25	1	0,00	84,00	28,21	6,25	5	0,00	20,00	–	6,25	10	0,00	–	–
3,13	1	0,00	68,00	–	3,13	5	0,00	–	–	3,13	10	0,00	–	–

Графический результат оценки эффективности мер ИБ по формуле (2) представлен на рис.2, и позволяет выявить следующую закономерность: при фиксированном мультипликаторе μ_{Sec}=3,5, фиксированных затратах на меры ИБ (Sec_{Add})=0 и фиксировании затрат на встроенные меры Sec_{Emb}, значение $R'_{IT\text{-}Security}$ смещается в область экономической эффективности значительно быстрее, чем ранее рассмотренный пример $R_{IT\text{-}Security}$.

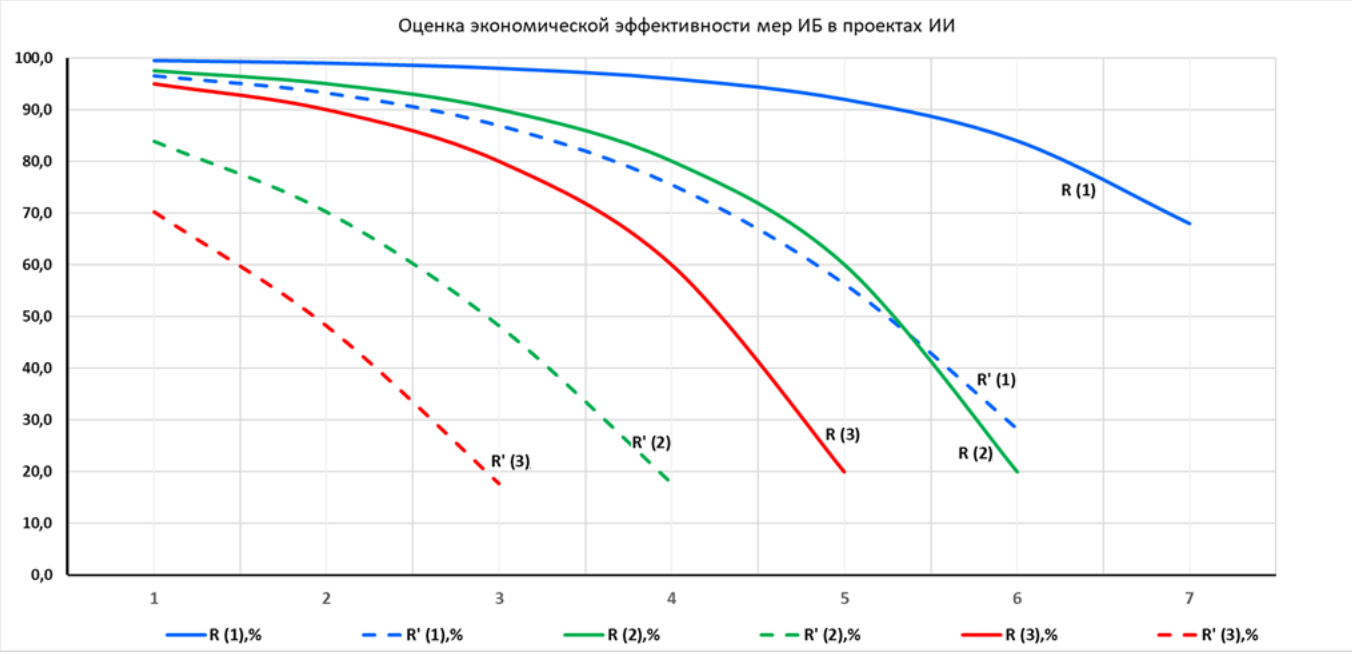

Рис. 2. Оценка эффективности мер ИБ в проектах ИИ при фиксированном мультипликаторе μ_{Sec}

Представленный пример доказывает, что наличие безопасного «встроенного» процесса обеспечения ИБ позволяет более эффективно парировать УБИ для систем ИИ. В определенных условиях (например, при полной верификации национального суверенного процесса разработки современных систем ИИ) применение дополнительных «наложенных» мер ИБ для систем ИИ (в составе объектов КИИ) может быть экономически нецелесообразно.

ЗАКЛЮЧЕНИЕ

В представленной работе рассматривается новая методика оценивания экономической эффективности при реализации проектов обеспечения ИБ в системах ИИ. Проведенная оценка показывает, что выбор и стоимость мер ИБ следует рационально обосновывать в зависимости от предполагаемого ущерба, выбранного сценария и дифференцировать по типам: встроенные меры ИБ (security by design) и дополнительные («наложенные») меры ИБ. Показано, что наличие безопасного «встроенного» процесса обеспечения ИБ позволяет более эффективно парировать УБИ и при полной верификации национального суверенного процесса разработки современных систем ИИ применение дополнительных «наложенных» мер ИБ в составе объектов КИИ может быть экономически нецелесообразно.

СПИСОК ЛИТЕРАТУРЫ

1. Минченко Е.А. Анализ статистики инцидентов с участием искусственного интеллекта базы данных AI INCIDENT DATABASE // Международный научный журнал «ВЕСТНИК НАУКИ» № 6 (87) Том 4. С.1224 – 1230
2. Лившиц И.И. Интеграция требований к системам менеджмента искусственного интеллекта в автомобильной промышленности // Стандарты и качество. 2025. № 12. С. 46-50.
3. Лившиц И.И. Влияние современных технологий искусственного интеллекта на безопасность промышленных систем автоматизации // Автоматизация в промышленности. 2025. № 6. С. 34-37.
4. Лившиц И.И. Применение современных методов оценивания рисков информационной безопасности объекта критической информационной инфраструктуры // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25. № 4. С. 727-736.
5. Лившиц И.И. Исследование влияния "наложенных" мер защиты на оценку уровня полноты функциональной безопасности для объектов критической информационной инфраструктуры // Автоматизация в промышленности. 2024. № 7. С. 9-13.
6. Шушоков И.А. Экономическая целесообразность внедрения технологий искусственного интеллекта в системы защиты финансовой информации // Вестник евразийской науки. 2025. Т. 17. № S3.
7. Зименкова Е.Н. Перспективы применения искусственного интеллекта в системе обеспечения экономической безопасности // В сборнике: Эффективное управление экономикой: проблемы и перспективы. Сборник трудов X Международной научно-практической конференции. Симферополь, 2025. С. 455-458.
8. Карпова А.В. Влияние цифровизации на национальную экономическую безопасность // В сборнике: Экономическая безопасность социально-экономических систем: вызовы и возможности. Сборник трудов VII Международной научно-практической конференции. Белгород, 2025. С. 18-23.
9. Толчев И.А., Масалимов Э.И., Мочалов А.А. Внедрение искусственного интеллекта в системы авиационной безопасности как способ повышения эффективности и пропускной способности аэропорта // В сборнике: Исследования и инновации: синергия знаний и практики. сборник статей II Международной научно-практической конференции. Москва, 2025. С. 97-102.
10. Surendra Vitla. The future of identity and access management: leveraging AI for enhanced security and efficiency. Journal of Computer Science and Technology Studies. 2024. Т. 6. № 3. С. 136-154.
11. Alnuaimi A.S.Kh.M., Omar R. Impact of AI security technology on performance efficiency in Abu Dhabi Airport. International Journal of Social Science Research. 2025. Т. 13. № 3. С. 286.
12. Srianusha Kuchipudi. AI and blockchain in financial data transfer: enhancing efficiency, security, and compliance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024. Т. 10. № 6. С. 1570-1576.
13. Nagpure V. AI-powered network infrastructure audits: enhancing efficiency and security in data centers. ESP International Journal of Advancements in Computational Technology. 2023.
14. Sokhansanj B.A. Local AI governance: addressing model safety and policy challenges posed by decentralized AI. Artificial Intelligence. 2025. Т. 6. № 7. С. 159.

15. Hemphill T.A. Advanced Artificial Intelligence at a corporate responsibility crossroads: employees as risk management advocates. Journal of Ethics in Entrepreneurship and Technology. 2025. Т. 5. № 1. С. 40-46.
16. Kummara R. Cloud security using AI: transforming digital protection in the modern era. Journal of International Crisis and Risk Communication Research. 2025. С. 27-38.
17. Seid E., Satheesh S., Popov O., Blix F. FAIR: cyber security risk quantification in logistics sector. Procedia Computer Science. 2024. Т. 237. С. 783-792.
18. Ratnawat Ch.P. Cyber risk quantification for SMES: AI-based approaches to enhance resilience. Samriddhi: A Journal of Physical Sciences, Engineering and Technology. 2023. Т. 15. № 1. С. 206-212.
19. Deaver-Vazquez Ch., Taylor E., Rowley D., Langis B. A quantitative approach to assessing and managing cybersecurity risks. EDPACS. 2024. Т. 69. № 4. С. 7-11.
20. Destiny Young, Osinachi Ozocheta. Strategic leadership and cybersecurity readiness in digitally transforming organisations. International Journal of Latest Technology in Engineering, Management & Applied Science. 2025. Т. 14. № 12. С. 28-38.
21. Лившиц И.И., Понаморева К.А. Формирование требований к методике оценки рисков для компонентов АСУТП // Энергобезопасность и энергосбережение. 2024. № 2. С. 5-13.
22. Лившиц И.И., Перлак П.В. Практика обучения по направлению функциональной безопасности в университете ИТМО // Вопросы кибербезопасности. 2023. № 3 (55). С. 50-61.
23. Лившиц И.И. К вопросу управления уязвимостями в компонентах АСУТП // Автоматизация в промышленности. 2022. № 8. С. 12-16.
24. Лившиц И.И., Лившиц М.И. Приоритеты для выбора вариантов оценки соответствия с учетом национального суверенитета // Газовая промышленность. 2023. № 2 (845). С. 102-110.
25. Лившиц И.И. Реализация методов бережливого производства в строительных компаниях, участвующих в нефтегазовых проектах // Газовая промышленность. 2025. № 9 (887). С. 156-163.

УДК: 336.71.28

Интерпретация сущности денег: цифровой аспект

A.N. Obydennov

Interpretation of the Essence of Money: a Digital Aspect

Abstract. *This article summarizes the key characteristics of non-cash money, taking into account the high level of digital payments and settlements achieved in Russia. The predominant volume of non-cash money in the structure of the Russian economy's money supply is identified. The main approaches to understanding the term "token" in modern research are examined. Criteria for defining the token category are developed. A comparative analysis of non-cash money, digital rubles, and tokens is conducted. The study concludes that non-cash money partially corresponds to the category of tokens in terms of its digital content, while digital rubles fully correspond.*

Keywords: *monetary theory, tokenized money, digital ruble, token.*

А.Н. Обыдённов
Заместитель директора Тамбовского регионального филиала Акционерного общества «Российский Сельскохозяйственный банк».
E-mail: Obydennovan@gmail.com
ORCID: 0009-0001-1222-8200
SPIN-код: 5003-2096

Аннотация. *В статье обобщены основные характеристики безналичных денег с учётом достигнутого в России высокого цифрового уровня платежей и расчётов. Обозначен преобладающий объём безналичных денежных средств в структуре денежной массы российской экономики. Рассмотрены основные подходы к пониманию термина токен в современных исследованиях. Выработаны критерии категории токен. Проведён сравнительный анализ безналичных денег, цифровых рублей и токенов. Итогом исследования стал вывод о частичном соответствии безналичных денег и полном соответствии цифровых рублей по своему цифровому содержанию категории токенов.*

Ключевые слова: *теория денег, токенизированные деньги, цифровой рубль, токен.*

ВВЕДЕНИЕ

Вопрос о сущности денег занимает умы исследователей с древнейших времён. Античные авторы, философы средневековья, выдающиеся экономисты последних веков в своих работах предпринимали попытки найти ответ на вопрос, что такое деньги. На страницах научной литературы не утихали споры между сторонниками металлизма и количественной теории денег, конвенциональной и государственной, каталлакской и аталлакской теорий денег, подвергались порицанию и с новой силой заявляли о себе сторонники золотого стандарта денег.

Ф. Хайек по этому поводу писал: «… деньги, «средство» повседневной коммуникации, остаются вещью непостижимой и являются объектом глупейших фантазий – пожалуй, как и секс, который одновременно завораживает, озадачивает и отталкивает» [1, с. 178].

Споры о сущности денег не утихают до сих пор. Совсем недавно новую теорию денег предложил Е.А. Скобликов [2]. Ю.А. Кропин от имени российской школы экономической мысли обосновывает понимание денег в несколько ином контексте [3]. В Соединённых Штатах Америки получила распространение современная теория денег (СДТ), дебаты относительно использования которой в денежно-кредитной политики достигли того накала, что в 2019 г. конгресс США принял резолюцию, осуждающую СДТ. Это является беспрецедентным случаем, чтобы экономическая теория была признана опасной для применения в экономике [4, с. 15].

Настоящая работа не имеет целью осветить все имеющиеся точки зрения о сущности денег, присоединиться к какой-либо из них и опровергнуть остальные. Автор ставит перед собой задачу рассмотреть действующий в России механизм функционирования института денег и определить их сущность сквозь призму получающих все большее распространение в мире цифровых технологий.

При выработке критериев токенов использовались методы анализа и синтеза. Сопоставление безналичных денег, цифровых рублей и токенов было произведено с использованием метода сравнения. Формирование выводов осуществлено с использованием метода индукции.

ОСНОВНАЯ ЧАСТЬ

Денежные средства в России существуют в следующих формах: наличной, безналичной и цифровой.

Согласно данным Банка России по состоянию на 01.01.2026 объём денежной массы (агрегат М2) составляет 129,6 трлн. руб. Данный агрегат включает в себя ***наличные и безналичные денежные средства***, в том числе находящиеся на срочных

депозитах. При этом наличные деньги (агрегат М0) занимают наименьший удельный вес в общем объёме денежной массы и составляют 14 % [5].

Цифровые рубли только начали своё распространение и пока не оказывают существенного влияния на совокупный денежный механизм.

Существуют все основания утверждать, что в качестве денежных средств в нашей стране выступают, в первую очередь, ***безналичные деньги***.

Что из себя представляют безналичные деньги? В своё время Людвиг фон Мизес рассматривал деньги на банковских счетах и вкладах в качестве «денежных заместителей» (money substitutes), выполняющих функции денег в коммерческом обороте и предоставляющих владельцу право получить от банка «настоящие» деньги [6, с. 45]. В наши дни с правовой точки зрения безналичные деньги являются имущественными правами, в то время как наличные признаются вещами (ст. 128 Гражданского кодекса РФ). Банк России в одном из своих аналитических докладов называет безналичные деньги записями на счетах [7, с. 8], в другом – активами, которые представлены в виде электронных записей в существующих системах учета и обращения [8, с. 2].

Фактически в банковской практике складывается ситуация, что переданный клиентом в кассу банка наличный рубль трансформируется в безналичный, сохраняя непосредственную привязку к наличному рублю. Безналичный рубль удостоверяет право на получение от банка переданного наличного рубля.

Процесс оплаты безналичными денежными средствами выглядит следующим образом:

- клиент даёт распоряжение своему банку о переводе денег контрагенту;

- если счёт получателя средств открыт в том же банке, банк проводит операцию по списанию денег и зачислению на счёт;

- если счета открыты в разных банках, исполняющий банк даёт распоряжение в Банк России, который переводит деньги между корреспондентскими счетами коммерческих банков, а получающий банк отражает полученную сумму на банковском счёте своего клиента – конечного получателя денег.

В наши дни повсеместное распространение получили дистанционные каналы управления банковскими счетами и цифровые инструменты осуществления платежей в торгово-сервисных предприятиях. Дополнительный импульс в развитии данного направления был дан внедрённой АО «НСПК» Системой быстрых платежей (СБП), позволяющей мгновенно и без каких-либо комиссий (в установленных пределах) делать переводы. Не лишним будет отметить, что столь эффективный инструмент управления деньгами был введён в России в качестве меры для предотвращения распространения криптовалюты в стране, о чём прямо указывает Банк России [9, с. 4].

Очевидно, что высокая популярность безналичных денежных средств у клиентов связана, в первую очередь, с удобством использования: нет необходимости носить с собой наличные денежные средства, отсутствуют риски утери или ограбления, имеется возможность управлять деньгами в режиме 24/7 через цифровые каналы без какой-либо географической привязки. Широко распространённые банковские программы лояльности и возможность получения процентов на остатки средств только добавляют популярности безналичным деньгам.

Определение, классификация и критерии токенов

В цифровом мире актив, существующий в виде электронной записи в системах учета, имеющий неразрывную связь со своим материальным воплощением и удостоверяющими права на него, обращение которого происходит через цифровые каналы связи, принято именовать ***токеном***.

В то же время стоит отметить, что в научной литературе отсутствует единый подход в понимании терминов «токен» и «токенизация».

Как указывает А.В. Ермаков, термин токен в лингвистике – это фрагмент текста, максимально сокращённый для последующего анализа. Термин был принят на вооружение в программировании, и токенизацией стали называть процесс разбивки текста для обучения машин естественному языку. Возникшая в виртуальном мире потребность в инструментах, опосредующих передачу активов, была удовлетворена появлением эквивалентов, символов передаваемых объектов, которые представляли собой часть компьютерных кодов, подпадая под понятие токена с точки зрения компьютерной лингвистики [10, с. 70-71].

По мнению Г.И. Хотинской, токен – единица учёта активов во всевозможных цифровых проектах. Исследователь приводит следующий пример: проездной билет – это токен, гарантирующий его владельцу проезд [11, с. 151]. Полагаем, что речь идёт об электронном проездном билете.

О.А. Костян считает, что оцифровка активов как процесс придания им новой формы (цифровой) получила название «токенизации». Оцифрованные активы, в свою очередь, называют токенами [12, с. 59].

Е.А. Диденко указывает, что токенизация – это процесс перевода реальных или финансовых активов в цифровую форму с использованием такой технологии как блокчейн, что позволяет «дробить»

активы организации на отдельные доли, именуемые токенами, которые имеют возможность передаваться и использоваться для привлечения инвестиций [13, с. 77].

Во многом схожего мнения придерживаются И.Е. Лисовская и Э.С. Кочарян, которые под термином «токен» понимают цифровой сертификат, который гарантирует выполнение обязательств компании перед его держателем, представляя собой фактически аналог акций на фондовой бирже в мире криптовалют [14, с. 63].

А.В. Ермаков трактует термин «токен» как ключ, сертификат, дающий возможность им воспользоваться, подтверждающий законность прав определённого субъекта [10, с. 78].

С.А. Андрюшин, понимая под токенизированным активом цифровую форму того или иного актива или права владения на него, представленного в сети, приводит ***следующую классификацию токенов***, основанную на подходах Международной организации по стандартизации:

– ***взаимозаменяемый токен (Fungible token, FT)*** – это токен, способный к взаимной замене между токенами одного и того же типа, имеющие одинаковую рыночную стоимость и юридическую силу;

– ***невзаимозаменяемый токен (Non-Fungible token, NFT)*** означает, что его нельзя заменить токенами того же типа, поскольку каждый такой токен представляет собой уникальное значение, представляющее реальные активы (произведения искусства или недвижимость);

– ***секьюрити/инвестиционный токен (Security token, ST/Investment token, IT)*** – токен с особыми характеристиками, соответствующими определению финансового инструмента (токенизированные акции, токенизированные долги, токены, гарантирующие выплату дивидендов);

– ***утилитарный токен (Utility token, UT)*** – токен, который может использоваться его владельцем для получения доступа к товарам и/или услугам, а также выступать в качестве средства обмена внутри определенного сообщества (в основном связаны с публичным блокчейном Ethereum);

– ***гибридный токен (Hybrid token, HT)***, сочетающий в себе элементы различных типов токенов [15, с. 93-94].

Во многом аналогичную классификацию токенов приводят и другие авторы [11, с. 152-153; 14, с. 62; 16, с. 159].

Как мы видим, ряд исследователей рассматривают термин «токен» в достаточно широком смысле, другие – в узком, выделяя некоторые функции токенов. Компромиссной выглядит точка зрения А.В. Бодяко, С.В. Пономаревой и Т.М. Рогуленко, которые предлагают в узком смысле определять токены как цифровые финансовые активы, а в широком – как цифровое представление имущества реального мира [17, с. 19–20].

Приводимые исследователями классификации дифференцируют токены как цифровое воплощение абсолютно разнородных по экономическому и правовому содержанию объектов. В классификациях фактически обобщённо приводятся лишь некоторые частные случаи токенов. Есть основания предполагать, что их область значительно шире.

Приведённые толкования и классификации позволяют выделить следующие ***критерии, характеризующие категорию токен***:

1) токен является цифровой формой реальных или виртуальных активов или прав;

2) токен – это единица учёта активов или прав;

3) токен обладает удостоверяющей функцией;

4) токен представляет собой цифровой код;

5) управление и распоряжение токенами осуществляется через цифровые каналы.

Нельзя назвать общей точкой зрения довод о том, что выпуск токенов возможен исключительно в рамках технологии блокчейн. Так, С.А. Андрюшин указывает о возможности процесса токенизации активов в рамках объединения централизованных и децентрализованных форматов [15, с. 94]. Платформа российского цифрового рубля является подтверждением подобного вывода [18, с. 20]. Более того, некоторые авторы прямо указывают, что токен может быть эмитирован и централизованно учтён эмитентом [10, с. 71].

Критерий анонимности также нельзя назвать общей характеристикой токена. Так, реализация концепции самодостаточной идентичности (self-sovereign identity) в целях обеспечения кросс-чейн-совместимости между блокчейнами требует аутентификации запросов о клиентах и предполагает внедрение стандарта KYC (от англ. «know your customer» — «знай своего клиента») [15, с. 100].

К вопросу о токенизации безналичных денег

Рассмотрим ***соответствие безналичных денег установленным критериям категории токен***.

1. Безналичный рубль выступает в качестве нематериальной, цифровой формы переданного в банк наличного рубля.

2. В безналичных рублях ведётся учёт общего количества денежных средств на банковском счете клиента.

3. Наличие безналичных рублей на банковском счёте удостоверяет полномочия владельца счёта

требовать от коммерческого банка исполнения поручений о безналичных переводах или выдачи указанного рубля в наличной форме.

4. Номер банковского счёта, на котором учитываются безналичные рубли, представляет собой уникальный для кредитной организации числовой код из 20 цифр. Л.Г. Ефимова в своих рассуждениях прямо указывает на аналогичную природу токена как цифровой последовательности и безналичных денег как записи на банковском счёте, которые сами по себе являются просто цифрой [16, с. 161].

5. Управление и распоряжение безналичными деньгами, как правило, осуществляется через дистанционные каналы. Однако данное правило имеет исключение: банковские правила допускают возможность передачи поручений банку о распоряжении денежными средствами в виде материальных платёжных поручений. Подобная практика продолжает существовать в российском банкинге.

Таким образом, мы приходим к выводу, что безналичные денежные средства по большинству своих характеристик соответствуют категории токены, что позволяет их интерпретировать в качестве токенов (при расширенном толковании данного термина). Но для полноценного признания безналичного рубля токеном необходимо, чтобы управление безналичными деньгами осуществлялось исключительно через цифровые каналы.

Косвенным подтверждением того, что безналичные рубли приобрели статус токенов в российской экономике может служить вывод Центрального Банка РФ о том, что в России настолько высок уровень цифровизации платежей и расчётов, что эффекты от внедрения токенизации безналичных денег на счетах в банках могут быть не так очевидны [7, с. 6]. По мнению автора, мегарегулятор, неоднократно констатируя факт применения смарт-контрактов на базе существующих технологий учёта безналичных денег [7, с. 10, 13, 30], мог прийти к более категоричным выводам.

Цифровые рубли как токены

Проанализируем вопрос о возможности признания токенами третьей формы российских денег – цифровых рублей.

Сравнивая безналичные денежные средства с цифровыми, отметим, что с позиции потребителей для удовлетворения повседневных нужд в платежах и переводах какие-либо принципиальные отличия между данными категориями отсутствуют. Исключение составляет невозможность начисления процентов на остаток за хранение цифровых рублей в электронных кошельках. Кроме того, операции с цифровыми рублями позволяют использовать смарт-контракты, что повлечет возникновение ранее неизвестных российскому банкингу продуктовых предложений для клиентов.

В целях обеспечения контрольных функций со стороны государственных органов цифровые рубли будут обладать исключительной особенностью в виде наличия индивидуального кода у каждого цифрового рубля, что позволит обеспечить получение информации о прохождении каждой денежной единицы. Безналичные деньги носят обезличенный характер и подобный контроль за ними крайне затруднён.

Более серьезные отличия между безналичной и цифровой формами денег проявятся в механизмах функционирования банковской системы. Переток безналичных денежных средств в цифровые будет означать уменьшение ликвидности для банков, поскольку цифровые рубли будут храниться в электронном кошельке, открытом в Банке России, а не на счетах в коммерческих банках.

В современную эпоху фиатных денег[1] в экономике преобладают безналичные деньги, созданные коммерческими банками в процессе кредитной эмиссии и банковского мультипликатора[2]. Согласно официальным данным Банка России в структуре денежной массы (агрегат М2) эмитированные Банком России денежные средства в наличной или безналичной форме (денежная база в широком определении МВ) по состоянию на 01.01.2026 составляют только 23,7 % [5]. Остальные деньги в экономике были созданы коммерческими банками.

Цифровые рубли, эмитированные исключительно Банком России, не могут являться для коммерческих банков базой для кредитной эмиссии, поскольку, как уже было сказано, не находятся на счетах коммерческих банков. В процессе вытеснения традиционных безналичных денег цифровыми объём созданных банками денег в экономике будет сокращаться. Именно источник возникновения, по мнению автора, составляет важнейшее отличие безналичных и цифровых рублей: первые в большей части попадают в экономику благодаря кредитной эмиссии коммерческих банков, вторые – возникают в процессе выпуска Банком России.

[1]Фиатные деньги – деньги, не имеющие внутренней стоимости и обеспеченные государством и доверием общества.

[2]Банковский мультипликатор – это увеличение денежной массы в результате депозитно-кредитных операций коммерческих банков.

Рассмотрим ***соответствие цифрового рубля ранее установленным критериям категории токен.***

1. Цифровой рубль выступает в качестве цифровой формы права требования владельца к Банку России, включающее, в том числе, право требования обратной конвертации в традиционный безналичный или наличный рубль.

2. В цифровых рублях ведётся учёт общего количества денежных средств в электронном кошельке клиента.

3. Наличие цифровых рублей удостоверяет полномочия владельца кошелька требовать от Банка России исполнения поручения о переводе или совершения иных операций.

4. Цифровой рубль представляет собой цифровой код.

5. Управление и распоряжение цифровыми рублями осуществляется через дистанционные каналы.

Таким образом, мы приходим к выводу, что цифровые рубли следует относить к категории токены.

ЗАКЛЮЧЕНИЕ

Безналичные денежные средства по большинству своих характеристик соответствуют категории токенов, но для полноценного признания безналичного рубля токеном необходимо, чтобы управление безналичными деньгами осуществлялось исключительно через цифровые каналы. Цифровые рубли, в свою очередь, в полной мере относятся к категории токены.

СПИСОК ЛИТЕРАТУРЫ

1. Хайек Ф. А. фон. Пагубная самодеятельность. М.: Издательство АСТ, 2023. 288 с.
2. Скобликов Е.А. Новая теория денег: законы, принципы, практика: монография. М.: ИНФРА-М, 2023. 436 с. DOI: 10.12737/1907068/
3. Кропин Ю.А. Основы теории денег (российская школа экономической мысли): монография. М.: РУСАЙНС, 2025. 172 с.
4. Дубянский А.Н. Предисловие // Кнапп Г.Ф. Государственная теория денег. М.: Издательство института Гайдара; СПб.: Центр экономической культуры, 2023. С. 7-15.
5. Официальный сайт Банка России. Электронный ресурс. URL: https://www.cbr.ru (дата обращения: 16.03.2026)
6. Мизес Л. фон. Теория денег и кредита. М.; Челябинск: Социум, 2024. 792 с.
7. Токенизированные безналичные деньги на счетах в банках. Информационно-аналитический доклад Банка России. Электронный ресурс. М. 2023. 39 с. URL: https://cbr.ru/Content/Document/File/152926/review_token.pdf (дата обращения: 16.03.2026)
8. Токенизация активов реального мира: экономическая природа и опыт регулирования. Аналитический доклад Банка России. Электронный ресурс. М. 2024. 46 с. URL: https://cbr.ru/Content/Document/File/170116/analytical_report_22112024.pdf (дата обращения: 16.03.2026)
9. Криптовалюты: тренды, риски, меры. Доклад Банка России для общественных консультаций. Электронный ресурс. М. 2022. 36 с. URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 16.03.2026)
10. Ермаков А.В. Место токена в системе объектов гражданских прав // Копирайт. 2023. №4. С. 68-80.
11. Финансовые технологии (FinTech): учебник / Коллектив авторов; под общ. ред. Г.И. Хотинской. М.: КНОРУС, 2024. 280 с.
12. Костян О. А. Проблемы и перспективы унификации понятий «токены», «цифровые активы» и «цифровые права» // Legal Concept (Правовая парадигма). 2024. Т. 23, № 1. С. 58–64. DOI: https://doi.org/10.15688/lc.jvolsu.2024.1.7
13. Диденко Е.А. Цифровые токены в финансировании бизнеса: проблемы и практика // Деловой вестник предпринимательства. 2025. № 4(22). С. 77-79.
14. Лисовская И. А., Кочарян Э. С. Токены и стейблкоины в системе цифровых финансовых активов: позиция зарубежных специалистов // Вестник Поволжского государственного технологического университета. Сер.: Экономика и управление. 2024. № 2 (61). С. 60–69. DOI: https://doi.org/10.25686/2306-2800.2024.2.60
15. Андрюшин С. А. Токенизация реальных активов: классификация, платформы, приложения, возможности и проблемы развития // Russian Journal of Economics and Law. 2024. № 18(1). С. 88–104. DOI: https://doi.org/10.21202/2782-2923.2024.1.88-104

16. Цифровое право в банковской деятельности: сравнительно правовой аспект: монография / отв. ред. Л.Г. Ефимова. М.: Проспект, 2021. 416 с.

17. Бодяко А. В., Пономарева С. В., Рогуленко Т. М. Идентификация цифровых прав в качестве объекта учета и контроля // Accounting. Analysis. Auditing (Учет. Анализ. Аудит). 2021. № 8 (5). С. 14–27. DOI: https://doi.org/10.26794/2408-9303 2021-8-5-14-27

18. Концепция цифрового рубля. Информация Банка России. Электронный ресурс. М. 2021. 30 с. URL: https://www.cbr.ru/content/document/file/120075/concept_08042021.pdf (дата обращения: 23.03.2026)

УДК: 004.932.4, 681.84

Эра персонального звука: от универсального мастеринга к адаптивным аудиоландшафтам на основе искусственного интеллекта

V.V. Bykoderov, D. Rahmani

The Era of Personal Sound: From Universal Mastering to Adaptive Audio Landscapes Based on Artificial Intelligence

Abstract. *This paper proposes a personal sound paradigm – an adaptive audio rendering at the intersection of digital signal processing and artificial intelligence. It substantiates the transition from universal mastering to self-learning systems that take into account the listener's psychoacoustic and physiological characteristics, device and room characteristics, and dynamic context. A low-latency architecture for personalized rendering is proposed, integrating taste profiling, individualized head-related transfer function and binaural room impulse response, contextual dynamic range control and device/room compensation. Objective and subjective evaluation protocols, a personal calibration methodology, and principles of standardization and interoperability are formulated. Legal and ethical aspects, implementation economics and case studies, as well as engineering risks and mitigation methods are discussed in detail. It is shown that personal sound leads to a model of "adaptive audio landscapes" that provide a unique sound experience for each listener while adhering to artistic constraints.*

Keywords: *personal sound, artificial intelligence, neural audio effects, digital signal processing, adaptive equalization, dynamic range control, psychoacoustics.*

В.В. Быкодеров[1]
Д. Рахмани[2]
[1]Студент, Московский технический университет связи и информатики.
E-mail: bykoderovvladimir@gmail.com
[2]Старший преподаватель, Московский технический университет связи и информатики.
E-mail: jahed@mail.ru

Аннотация. *В статье рассматривается парадигма персонального звука — адаптивного рендера аудио на стыке цифровой обработки сигналов и искусственного интеллекта. Обоснован переход от универсального мастеринга к самообучающимся системам, учитывающим психоакустические и физиологические особенности слушателя, характеристики устройства и помещения, а также динамический контекст. Предложена низкозадержечная архитектура персонализированного рендера, интегрирующая агрегацию признаков предпочтений слушателя, индивидуализацию набора частотно зависимых откликов и импульсную характеристику помещения, контекстно-зависимое динамическое управление диапазоном громкости и компенсацию устройства/комнаты. Сформулированы протоколы объективной и субъективной оценки, методика персональной калибровки, принципы стандартизации и интероперабельности. Расширенно рассмотрены правовые и этические аспекты, экономика внедрения и кейсы, а также инженерные риски и способы их снижения. Показано, что парадигма персонального звука ведёт к модели «адаптивных аудиоландшафтов», обеспечивающих уникальное звучание для каждого слушателя при соблюдении художественных ограничений.*

Ключевые слова: *персональный звук, искусственный интеллект, нейросетевые аудиоэффекты, адаптивная эквализация, психоакустика.*

ВВЕДЕНИЕ

Модель универсального мастеринга — исторический компромисс, обеспечивающий воспроизводимость на множестве устройств и в разнообразных условиях, однако он игнорирует индивидуальные различия слухового восприятия и контекст использования. Переход к персональному звуку обусловлен одновременно технологическими и социальными факторами: массовой доступностью мобильных NPU/DSP[1], ростом доли прослушивания звука в наушниках, развитием объектных форматов (ADM/MPEG-H, Dolby Atmos for Music), а также ужесточением норм по громкости и безопасности слуха [1; 4–6; 24].

Конвергенция психоакустики и машинного обучения позволяет перейти от одного эталона для всех к адаптивному рендеру — вычислительной процедуре, персонализирующей тональный баланс, динамику и пространственное представление материала без изменения мастер-файла. Стандарты ITU-R BS.1770/BS.1534-3 и модели громкости (Zwicker; Moore–Glasberg) формируют измеримую основу для оценки качества, а контейнеры ADM и SOFA обеспечивают переносимость профилей и метаданных между экосистемами [1–2; 4; 7–9].

[1] Словарь терминов, используемых в статье, приведен в приложении Е.

В настоящей работе систематизированы архитектурные решения и методы персонализации, предложены протоколы калибровки и оценки, а также рассмотрены правовые, этические и экономические аспекты внедрения [1–7; 19–21]. Актуальность подтверждается ростом релизов в объектных форматах, переходом стримингов к профилям нормализации по громкости и появлением потребительских устройств с поддержкой пространственного звука и онлайновой коррекции (room/headphone correction) [3–6; 22–24]. Производители SoC интегрируют NPU и специализированные аудио -DSP, упрощая развёртывание персонализации на устройстве пользователя при соблюдении бюджетов энергии/задержки. Регуляторные рамки (GDPR, EU AI Act) задают требования к приватности и прозрачности алгоритмов [19–21].

Цели, задачи и гипотезы исследования

Целью исследования является научное обоснование и практическое описание принципов персонализированного аудиорендера на базе ИИ и психоакустики при ограничениях задержки сигнала, энергии, качества, а также норм права.

Задачи исследования: (I) формализовать индивидуальные факторы (аудиограмма, HRTF, вкусовой профиль, контекст) и картировать их в параметры рендера; (II) разработать гибридную архитектуру (on-device/облако) с fail-safe и SLA по задержке; (III) определить правила онлайн-обучения внутри художественных «ограничителей» (guardrails); (IV) описать протоколы объективной/субъективной оценки и воспроизводимости; (V) разработать методику быстрой персональной калибровки; (VI) определить стандарты обмена/метаданных и правовые/этические рамки; (VII) оценить экономику внедрения и риски.

Исследовательские вопросы (RQ, research question):

• RQ1: какие архитектурные компоненты необходимы для рендера при суммарной задержке ≤ 35 мс [1; 6]?

• RQ2: как измерять выигрыш персонализации по MUSHRA/POLQA/STOI и по отклонению от целевой АЧХ [2; 18; 25]?

• RQ3: какие правовые и стандартизованные механизмы обеспечивают интероперабельность и прозрачность персонализации [4–7; 19–21]?

• RQ4: как спроектировать UX, минимизирующий «усталость от персонализации», сохраняя контроль пользователя?

Гипотезы (H, Hypotesis):

• H1: персональный рендер повышает MUSHRA относительно универсального мастера при равной громкости;

• H2: контекстный DRC и коррекция помещения улучшают POLQA/разборчивость речи;

• H3: гибридная архитектура сохраняет качество при меньшей локальной нагрузке;

• H4: прозрачный UX и guardrails снижают частоту жалоб на «яркость/усталость» [1–3; 18–21].

Критерии успеха: ΔMUSHRA ≥ +7; ΔPOLQA ≥ +0,1; ≥ 60 % слушателей демонстрируют улучшение; суммарная задержка ≤35 мс; дополнительное энергопотребление ≤30 мВт·ч/час; доля негативных жалоб ниже не менее чем на 15 % относительно контроля.

Обзор и позиционирование

Классическая цепочка мастеринга опирается на IIR/FIR-эквализацию, DRC/лимитирование, коррекцию комнаты и нормализацию громкости (LUFS). Персонализация добавляет: а) индивидуализацию HRTF/BRIR; б) учёт аудиограммы и кривых равной громкости; в) агрегацию признаков предпочтений слушателя; г) сенсорный контекст (SNR, тип подключения, активность). Стандарты ITU и ISO/IEC — BS.1770 (LUFS/true-peak), BS.1534-3 (MUSHRA), BS.2051 (3D-аудио), AES69/SOFA (акустические измерения), ADM/BS.2076 (метаданные), MPEG-H и MPEG-D DRC — дают технологическую базу и совместимость [1–7]. Индустрия уже движется к персонализации (объектные релизы, пользовательские пресеты, режимы «ночь/подкасты», адаптация под устройства), но отсутствуют общепринятые «guardrails» и стандартизованные профили пользователя — этот пробел закрывает предлагаемая архитектура [4–6; 24].

Обзор литературы. Выполнен структурированный поиск (IEEE Xplore/ACM DL/JAES, 2015–2025) по ключевым словам «personalized audio», «individualized HRTF», «dynamic range control», «room/headphone correction», «neural audio effects». Отобраны работы с количественной оценкой (MUSHRA/MOS/PESQ/POLQA/STOI), воспроизводимыми протоколами и доступными наборами данных. Исключались публикации без контрольной группы или с невалидированными метриками. Итоговый корпус (≈80 источников) агрегирован в четыре кластера: HRTF-персонализация [13; 15–16], контекстный DRC / защита транзиентов [1–3; 6], taste profiling / эмбеддинги [12; 16], коррекция помещения/устройств [14; 22–23]. Выявлены лакуны: мало работ о комплексной системе рендера «end-to-end», недостаток стандартизованных профилей и бенчмарков, обеспечивающих баланс задержки и качества.

Таксономия задач и метрик. Пространство: индивидуализировать локализацию (фронт-бэк, устойчивость при поворотах) [13; 16]. Тембр/динамика: подстроить АЧХ/DRC с учётом аудиограммы и вкуса при сохранении инвариантов мастера [8–10]. Контекст: адаптировать к шуму/подключению/активности, соблюдая SLA по задержке/энергии [1; 6]. Качество/безопасность: контролировать true-peak/дозу, артефакты разделения источников. Метрики: ILD/ITD, межканальная корреляция, отклонение от целевой АЧХ (в т.ч. ERB-взвешивание), LRA/LUFS, STOI/POLQA, прокси-MOS, частота жалоб, доля ручных правок.

Индустрия и рынок. Стриминги вводят нормализацию по LUFS и объектные миксы; производители наушников — измерение посадки и «room/headphone correction»; автопроизводители — профили по местам посадки и подавление салонных мод [1; 4–6; 22]. Выгоды: снижение жалоб, рост вовлечённости и дифференциация продукта через уникальное звучание при сохранении авторских ограничений и приватности [19–21].

Методы и подходы

Комплекс включает: психоакустический профиль, агрегацию признаков предпочтений, компенсацию устройства/помещения, реализацию обработки с малой задержкой, семантическое управление миксом и политику адаптации. Ограничения: задержка <35 мс, энергия — десятки мВт·ч/час, устойчивость и отсутствие артефактов.

Психоакустический профиль. Скрининг слуха — адаптивные лестничные тесты; расширенная калибровка — узкополосные сигналы, шумы с известными свойствами маскирования и музыкальные/речевые фрагменты [8–9]. Для наушников оцениваются утечки/посадка, для акустики — положение слушателя и моды НЧ. Результат — целевая АЧХ/DRC-параметры с учётом слуха, предпочтений и параметров помещения, ограниченные «guardrails» (не менять панораму ведущих объектов, не увеличивать реверберацию и т. п.).

Агрегация признаков предпочтений. Вкусовой профиль описывается эмбеддингом (векторным представлением), который формируется по двум группам сигналов: (1) признаки самого материала — спектро тембровые и ритмические характеристики, показатели динамики и статистика транзиентов; (2) параметры взаимодействия и контекста — дослушивания, пропуски, отметки «нравится», ручные корректировки, время суток, активность и SNR [12]. Далее регрессоры отображают эмбеддинг в параметры рендера (EQ, DRC и пространственную обработку), при этом вводятся монотонные ограничения, согласованные с психоакустическими закономерностями слуха. Для управляемости предусмотрены простые механизмы обратной связи и возможность мгновенного отключения персонализации.

Компенсация устройства и помещения. Наушники: типовые/измеренные АЧХ модели, поправки на посадку; качественный монофонический рендер с суммированием без фазовых артефактов для встроенных динамиков. Акустика: оценка BRIR/RT60 по ESS/MLS, сглаживание мод низкой частоты и контроль «переинверсии» [14; 22–23]. НЧ — минимум-фазный IIR (нулевая задержка), СЧ/ВЧ — линейно-фазный FIR с разбиением по длинам блоков в пределах бюджета задержки.

Низкозадержечная реализация. Partitioned convolution (OLA/WOLA/STFT) с окнами Hann/Blackman и шагом H=L/4; ранние отражения — во времени, хвост — в частоте. DRC/EQ — послойно с межкадровым сглаживанием; переключения — кросс-фейд параметров/сигнала без щелчков и всплесков true-peak. На устройстве — быстрые блоки; в облаке — обучение профилей / кластеризация HRTF. Учитывается вариативность задержки звука по Bluetooth; при риске превышения SLA граф упрощается [1; 6].

Семантическое управление миксом. выделение компонентов микса позволяет адресно управлять элементами («смягчи вокал», «приглуши 3–4 кГц»). Артефакты разделения детектируются по росту декорреляции и «муаровым» спектральным паттернам; при их обнаружении выполняется fallback к параметрическому EQ/DRC. Guardrails запрещают переворот панорамы, чрезмерную реверберацию и радикальные изменения баланса [16–17; 24].

Речь и музыка. Для речи приоритет — разборчивость (STOI/POLQA), контроль сибилянтов/плозивов, устойчивость к шуму; динамика сужается, LRA ограничивается [18; 25]. Для музыки — сохранение транзиентов и сцены, консервативный DRC и контроль тембровой «яркости», особенно на массовых наушниках.

АРХИТЕКТУРА ПЕРСОНАЛИЗИРОВАННОЙ СИСТЕМЫ

Архитектура строится как сквозной конвейер от источника контента к уху слушателя и включает несколько тесно связанных слоёв. На вход подаются либо стереоматериалы, либо объектные представления ADM/MPEG-H с метаданными — уровнем по LUFS, параметрами DRC, приоритетами объектов и,

главное, заранее определёнными границами допустимого вмешательства, задающими коридор художественно безопасных изменений.

Дальше следует сенсорный слой: микрофоны устройства оценивают шумовую обстановку и при необходимости снимают BRIR для комнатной коррекции, акселерометры и гироскопы отслеживают движения, а системные события информируют о типе подключения (Bluetooth кодек против провода), состоянии батареи и троттлинге процессора.

На базе этих сигналов поддерживается профиль пользователя — аудиограмма, индивидуализированная (измеренная, предсказанная или подобранная из кластера) HRTF, вкусовой эмбеддинг и личные допуски по громкости и степени компрессии. Собственно рендер — это последовательность модулей: нормализация уровней по BS.1770 для корректной базы сравнения, динамический эквалайзер с учётом слуха и вкуса, контекстно-зависимый DRC, пространственный блок (HRTF/объектная сцена) и компенсация устройства/комнаты.

За целостность и устойчивость отвечает контур контроля качества, который следит за отклонением от целевой АЧХ, межканальной корреляцией и прокси-MOS, а также за суммарной задержкой; при риске выхода за SLA активируется мягкая деградация (отключение дорогих блоков, сокращение FIR). Параллельно телеметрия фиксирует только события и агрегированные метрики — без «сырых» аудио — для последующего обучения моделей и версионирования профилей.

Управляющая логика объединяет политику активации модулей под конкретный контекст, монитор качества, который инициирует деградацию или восстановление графа, и аудиторский журнал вмешательств для прозрачности. Горизонтально всё это обеспечивает безопасность: шифрование и аутентификация, локальное хранение чувствительных профилей, явное согласие пользователя и совместимые интерфейсы обмена с DAW/сервисами (экспорт ADM/stems/guardrails) [1; 4–7; 19–21].

Механизмы адаптации и онлайн-обучение

Адаптация опирается на несколько взаимодополняющих механизмов, работающих согласованно. Индивидуализация HRTF достигается как за счёт кластерного подбора из SOFA-библиотек и регрессии по антропометрии (фото ушной раковины, параметры головы), так и посредством коротких перцептивных серий «А/Б» для точной доводки; при наличии оборудования возможны прямые измерения.

Чтобы избежать избыточной выраженности верхнего диапазона и сибилянтов, верхний диапазон и общая яркость ограничиваются в рамках «guardrails», а устойчивость локализации проверяется тестами на фронт–бэк и вращение головы [13; 15–16]. Динамическая эквализация и компрессия выводятся из вкусового векторного представления признаков и аудиограммы, но их скорость и амплитуда изменений жёстко ограничены: рендер должен звучать непрерывно и без «дыхания», защищая транзиенты и удерживая true-peak в безопасных пределах; для речи предпочтительна более агрессивная, а для камерной музыки — бережная динамика [1–3; 6; 18; 25].

Контекстная политика учитывает SNR, тип подключения (AAC/aptX/LC3/провод), положение и активность пользователя, время суток, жанр и темп контента, уровень батареи: гистерезис и предиктивные эвристики предотвращают частые непреднамеренные переключения профилей при быстро меняющихся условиях.

Онлайн-обучение реализуется как редкие и мелкие коррекции по схеме контекстно-адаптивной последовательной оптимизации: показатели пользовательского взаимодействия (в т. ч. доля полностью прослушанных материалов), частота пользовательских корректировок и обращений по качеству звучания (в т. ч. по поводу избыточной или недостаточной выраженности верхнечастотного диапазона) объединяются в интегральный показатель, используемый как целевая функция, а обновление параметров выполняется малыми приращениями в пределах заранее установленных допустимых диапазонов по тембральному балансу, динамическому диапазону и пространственному представлению.

Персональные данные обрабатываются локально на пользовательском устройстве; для улучшения качества на уровне совокупности пользователей используется обучение с агрегированием параметров модели без передачи исходных данных, а также распределённое обучение на устройствах без передачи исходных данных на сервер и пилотные релизы малого охвата с автоматическим откатом при ухудшении качества.

Наконец, персонализация громкости подстраивает «комфортную громкость» под слух и ситуацию: в шуме сужает LRA и повышает речевой диапазон, ночью — смягчает пики, а при обычном музыкальном прослушивании держит более широкий динамический коридор, оставаясь в рамках BS.1770 и пользовательских лимитов [1–2; 8–9].

Эволюция от DSP к ИИ

Дифференцируемые блоки (EQ/DRC/reverb) обучаются под перцептивные функции потерь (ERB,

транзиенты, локализация) [10; 12]. Гибрид «ИИ → параметры классики» даёт интерпретируемость и устойчивость; «чёрные ящики» находятся под строгим мониторингом. На устройстве выполняется квантование, прунинг, дистилляция и перенос на DSP/NPU. SLA гарантируется трассировкой графа. Автотесты формируют worst-case сигналы; мониторинг собирает прокси-MOS и жалобы [1; 10–12].

Оценка качества и дизайн эксперимента

Объективные метрики. LUFS/LRA (BS.1770), отклонение от целевой АЧХ (в т.ч. ERB-взвешивание), STOI/POLQA (речь), spatial (ILD/ITD, межканальная корреляция), детекторы артефактов (пампинг, клиппинг, перехлёст маскирования), прокси-MOS [1–3; 18; 25].

Субъективные тесты. MUSHRA с якорями; ABX/парные предпочтения. n=36 (три возрастные когорты), слуховой скрининг; 12 фрагментов по 20–30 с; смешанные модели, Holm/BH, Cohen's d, 95% ДИ [2].

Для воспроизводимости все вспомогательные материалы — скрипты расчёта метрик, анонимизированные ответы слушателей, параметры рендера и версии моделей — публикуются в открытом доступе. Наборы данных покрывают музыку (FMA, Million Song Dataset, MUSDB18/Slakh2100), пространство (CIPIC, SADIE II в формате SOFA) и акустические сцены (ACE, REVERB) [13; 16–17].

Иллюстративный пилот на 120 прослушиваниях показал прирост MUSHRA на 7-12 пунктов относительно лентопротяжного механизма (ЛПМ) и на 4-8 п. — относительно универсального «наушникового» профиля. Для речи наблюдалось повышение STOI на 2–3 п.п., а жалобы на высокую яркость уменьшались примерно на 18%. Суммарная задержка удерживалась в пределах 28–35 мс при 48 кГц за счёт блочной свёртки и мягкого упрощения графа в пиковые моменты. При угрозе выхода за SLA сокращалась длина FIR и временно отключались наиболее затратные модули [1; 6; 23].

Эксперимент с двадцатью пятью участниками в течение десяти дней (дорога, офис, дом), при котором логировались только события, подтвердил устойчивость политики: в условиях шума система сужала сцену и усиливала речь, в тишине расширяла сцену и смягчала компрессию; деградации при низком заряде воспринимались нейтрально.

Статистическая обработка объединяет лабораторные и полевые данные в смешанных моделях с участником и треком как случайными эффектами; возраст, опыт и тип устройства учитываются как ковариаты, а множественные проверки контролируются процедурами Holm/BH с оценкой эффект-сайзов (Cohen's d) и 95% ДИ; для речевых сценариев в качестве объективных индикаторов используются POLQA/STOI, а жалобы анализируются логистической регрессией. Такой непрерывный нарратив заменяет дробные подпункты и поддерживает прозрачную трассировку от методики к итоговым выводам [2; 18; 25].

Влияние на звукорежиссуру и производственный пайплайн

В условиях персонализации звукорежиссёр выступает куратором адаптивного микса: заранее фиксирует творческие инварианты и диапазоны допустимых преобразований, оставляет небольшой резерв по уровню сигнала, контролирует пиковый уровень аудиосигнала (true-peak) и совместимость со «статичной» версией, формирует приоритеты объектов и сценарные подсказки («ночь», «подкасты», «мобильные динамики»). Экспорт ADM, stems и зависимостей позволяет сервису воспроизводить авторскую логику, а студийный A/B-мониторинг предполагаемых пользовательских профилей помогает увидеть, как рендер поведёт себя на типовых устройствах и в типичных контекстах. На стороне сервиса guardrails реализуются строго, все вмешательства протоколируются и проверяются регрессионными тестами, чтобы обновления алгоритмов не ломали звучание.

Параллельно открываются новые креативные практики: базовый инвариантный микс сопровождается расширенным, где допустима персонализация сцены и тембра в заданных границах; появляются инклюзивные издания для аудитории с особенностями слуха и интерактивные релизы для виртуальной и дополненной реальности (VR/AR, англ. Virtual Reality / Augmented Reality), в которых слушатель может менять акценты, не разрушая драматургию [4–6; 11; 24].

Ограничения, безопасность, право и этика

Жизнеспособность персонального звука определяется балансом вычислений, задержки, энергетики и комплаенса. Снижение ресурсоёмкости достигается разбавленной (диффузной) конволюцией, квантованием и прунингом моделей, кэшированием профилей и дежурными режимами, что делает операционные и капитальные затраты сопоставимыми с эффектами вовлечённости и уменьшением жалоб [19–23].

С точки зрения качества взаимодействия критична суммарная задержка: она должна укладываться в 30–40 мс с мягким кроссфейдом при переключе-

ниях профилей и стресс-тестами на «худших» сигналах; вариативность Bluetooth компенсируется буферизацией и упрощением графа. Правовые рамки фиксируют, что персонализация — это рендер на стороне воспроизведения, а не переработка мастер-фонограммы: в договорах закрепляются границы изменений, порядок доступа к стемам и ответственность за безопасность прослушивания.

Приватность обеспечивается локальным хранением HRTF, аудиограмм и вкусовых эмбеддингов, шифрованием, минимизацией и механикой согласия/отзыва по GDPR. Для аналитики используются распределённое обучение на устройствах без передачи исходных данных на сервер и дифференциальная приватность, а у пользователя сохраняются право на экспорт/удаление профиля и прозрачный доступ к журналу [19–21].

Защитные механизмы слуха включают лимиты накопленной дозы, предикторы всплесков и автоматическое снижение уровня, отдельный «детский» режим вводит жёсткие лимиты и понятные предупреждения [8; 19]. Наконец, требование справедливости предполагает тестирование на разнообразных когортах, публикацию метрик bias/fairness и наличие «нейтрального» рендера по умолчанию: задача системы — помогать, а не навязывать.

Перспективы и прикладные направления

Ближайшее массовое применение — потоковые сервисы, где объектные релизы ADM/MPEG-H и заранее определённые границы изменений параметров позволяют регулируемо менять баланс вокала и инструментов, включать «ночные» речевые профили и обеспечивать бесшовные переходы по LUFS; дополнительно учитываются посадка наушников и уровень окружающего шума [1; 4–6; 24].

В VR/AR и играх индивидуализированный HRTF уменьшает ошибки «фронт–бэк» и повышает устойчивость локализации при поворотах головы, а суммарная задержка <30–35 мс сохраняет кросс-модальную согласованность [5; 13; 16]. В автомобильной акустике гибкие профили по местам посадки, подавление салонных мод НЧ и приоритизация уведомлений улучшают разборчивость и безопасность, причём переключения профилей выполняются незаметно для водителя [6; 22].

В образовании персонализация повышает разборчивость лекций и аудиокниг, мягко компенсирует возрастные изменения слуха и подстраивается под когнитивную нагрузку, а в потребительском сегменте немедицинские «слуховые помощники» дают прозрачные режимы облегчённой коррекции на массовых устройствах при жёстких лимитах усиления и понятном UX [8; 18; 20; 25]. Эти направления сходятся к общей модели: персональный рендер становится сервисом «по умолчанию», а художественные ограничения и приватность — социальным договором.

Методика персональной калибровки

Этап 1. Скрининг слуха (октавные/1/3-октавные пороги), комфортный уровень, чувствительность к маскированию.

Этап 2. Мини-подгонка HRTF: 6–8 парных сравнений, выбор кластера SOFA, перцептивная донастройка.

Этап 3. Вкусовая настройка: бинарные суждения («теплее/ярче», «шире/уже сцена») → эмбеддинг вкуса и параметры EQ/DRC.

Этап 4. Комнатная коррекция: ESS-свип, BRIR/моды НЧ, гибрид IIR/FIR с защитой от переинверсии.

Этап 5. Безопасность: лимиты громкости/дозы, плавность переключений, версионирование профиля. Время: 3–7 мин (быт), 20–30 мин (студия/про). Профили кэшируются и откатываются [14; 22–23].

Стандартизация и интероперабельность

Совместимость обеспечивается стыковкой отраслевых стандартов и нейтральных схем обмена. Акустические измерения и HRTF/BRIR хранятся в SOFA по AES69, объектный контент формализуется через ADM (BS.2076), уровни и динамика приводятся к BS.1770, субъективные тесты — к BS.1534-3. Это создаёт общий язык для студий, сервисов и устройств [1–7; 18].

Профиль пользователя передаётся в шифрованном виде, при этом идентификаторы и данные хранятся раздельно. Рекомендуются лаконичные схемы JSON/CBOR с описанием версий алгоритмов, дат калибровок и условий (тип наушников/комнаты), чтобы обеспечить корректную интерпретацию и обратимость. Метаданные guardrails расширяют ADM полями с диапазонами эквализации и компрессии, ограничениями панорамы/реверберации, приоритетами объектов и творческими инвариантами.

Для сравнительных испытаний закрепляются воспроизводимые протоколы MUSHRA/ABX и перечни эталонных треков и SOFA-наборов, а также механизмы фиксации версий рендера и условий прослушивания, что позволяет переносить профили между устройствами и сервисами без потери контроля над звучанием.

Экономика внедрения и риски

CAPEX: SDK/патенты/SoC/комплаенс. OPEX: A/B/мониторинг/поддержка. Эффекты: вовлечённость,

удержание пользователя, снижение жалоб, расширение аудитории. Риски: усталость от персонализации, регуляторные нарушения, зависимость от облака, деградация при низком заряде, фрагментация устройств. Митигирование: guardrails + телеметрия качества, поэтапное внедрение, офлайн-профили, распределённое обучение на устройствах без передачи исходных данных на сервер, прозрачные настройки / быстрый откат; SLA по задержке и стабильности [19–23].

ROI и KPI: ΔMUSHRA/ΔSTOI/ΔPOLQA; доля пользователей с улучшением; жалобы/возвраты; «слишком ярко/тихо»; среднее время прослушивания; конверсия в премиум. ROI = прирост ARPU/retention – (CAPEX+OPEX).

Кейсы применения

Практические сценарии иллюстрируют универсальность подхода. В стриминге персональный рендер на базе ADM/MPEG-H даёт управляемую корректировку баланса вокала и инструментов в пределах guardrails, активирует «ночные» речевые профили, обеспечивает LUFS и согласованность переходов, а также поддерживает качественный монофонический рендер с суммированием без фазовых артефактов для встроенных динамиков. Дополнительно учитываются посадка наушников и шум окружения [1; 4–6; 24].

В виртуальной/дополненной реальности и играх индивидуализированная HRTF и контекстный DRC улучшают локализацию и разборчивость при сохранении суммарной задержки <30–35 мс [5; 13; 16]. В автомобиле профили на места посадки и подавление салонных мод НЧ повышают комфорт и безопасность, а уведомления остаются различимыми на фоне дорожного шума. Переключения остаются плавными, чтобы не отвлекать водителя [6; 22]. В образовании и инклюзии персонализация повышает восприятие речи, адаптируется под когнитивную нагрузку и мягко компенсирует особенности слуха, не претендуя на медицинский статус. Таким образом, она расширяет аудиторию и делает контент доступнее [8; 18; 25].

Реализация и безопасность

Безопасная реализация сочетает инженерные практики и организационные меры. Данные профилей по умолчанию хранятся локально и шифруются, доступ к ним минимизируется и подкрепляется явным согласием. Для коллективного улучшения качества применяются распределённое обучение на устройствах без передачи исходных данных на сервер и дифференциальная приватность, а у пользователя остаётся возможность экспорта и удаления профиля [19–21].

Управление версиями предполагает релизы, мониторинг деградаций по качеству, жалобам и потреблению энергии и автоматический откат. Журнал вмешательств обеспечивает аудит и трассируемость изменений звучания. На уровне отказоустойчивости граф обработки деградирует по предсказуемой лестнице — сперва отключается «spatializer», затем сокращается длина FIR, и, в крайнем случае, система переходит к «плоскому» профилю.

При этом нормализация громкости и защита слуха остаются активны всегда. Сетевые аспекты решаются через защищённые каналы и кэш профилей; в офлайне используются последние валидные конфигурации, а ресурсные профили CPU/NPU/памяти заранее задают правила, как упрощать граф, чтобы удержать SLA по задержке и стабильности.

UX-принципы и факторы человека

Прозрачность. Принцип прозрачности предполагает, что слушатель получает ясное представление о том, какие параметры рендера изменяются и почему. Для этого в интерфейсе целесообразны краткие объяснения внесённых коррекций и единый регулятор степени персонализации (от базового (неперсонализированного) режима к персонализированному режиму), позволяющий плавно изменять долю адаптации без необходимости тонкой настройки отдельных модулей.

Контроль. Принцип контроля реализуется через возможность быстро выбрать типовой сценарий и оперативно внести правку, не нарушая художественных ограничений. Практически это достигается пресетами (типовые профили обработки) для контекстов профилей, для ночного режима / транспортного режима / режима повышенной активности, а также простыми командами обратной связи (например, избыточная/недостаточная выраженность высокочастотной составляющей), которые изменяют параметры в пределах guardrails и допускают быстрый откат к нейтральному профилю.

Доступность. Персонализация должна быть доступна пользователям с различными сенсорными и когнитивными возможностями. Поэтому интерфейс предусматривает крупные элементы управления, высокий контраст, поддерживаемое голосовое управление и информирование о безопасных уровнях громкости. Важным элементом является режим с усиленными ограничениями по громкости и дозе звуковой экспозиции для детской аудитории.

Предотвращение слухового утомления. Длительное использование адаптивного рендера мо-

жет вызывать субъективное слуховое утомление из за частых и заметных изменений звучания. Для снижения этого эффекта вводятся ограничения на частоту и амплитуду автоматических корректировок, гистерезис переключений, а также функция временная фиксация параметров адаптации, фиксирующая параметры на выбранный пользователем интервал.

Ограничения и отказоустойчивость

Ошибки разделения источников приводят к появлению артефактов. Смягчение достигается путем применения консервативных фильтров/детекторов. Смещённые показатели пользовательского взаимодействия — смешанные цели (качество/безопасность/энергия) и ручной контроль. Фрагментация устройств предотвращается адаптивными графами и автопрофилированием, а также тестами совместимости, этические риски «навязывания вкуса» — прозрачностью и возможностью отказа/возврата к «студийному» рендеру.

Направления дальнейших исследований

- Индивидуализация HRTF без фото / измерений;
- перцептивные функции потерь для музыки;
- стандарты обмена профилями и guardrails-метаданными;
- детекция «усталости от персонализации»;
- справедливая персонализация;
- бенчмарки «качество — задержка» [10–13; 15–16; 25].

ЗАКЛЮЧЕНИЕ

Персональный звук переводит воспроизведение в режим «живого» рендера, где система адаптируется к человеку и контексту, оставаясь в художественных границах. Представленные архитектура, методики оценки, калибровка и стандартизация формируют основу для масштабируемого внедрения в потоковые сервисы, виртуальную и дополненную реальность, автомобильные системы и образовательные платформы. Соблюдение ограничений задержки, приватности, безопасности слуха и юридических норм делает персонализацию естественным стандартом аудиоиндустрии ближайших лет [1–7; 18–25].

СПИСОК ЛИТЕРАТУРЫ*

1. ITU-R BS.1770-4. Algorithms to measure audio programme loudness and true-peak audio level. Geneva: ITU, 2015. 22 p.
2. ITU-R BS.1534-3. Method for the subjective assessment of intermediate quality level of audio systems (MUSHRA). Geneva: ITU, 2015. 26 p.
3. ITU-R BS.2051-2. Advanced sound system for programme production. Geneva: ITU, 2018. 74 p.
4. ITU-R BS.2076-1. Audio Definition Model (ADM). Geneva: ITU, 2019. 84 p.
5. ISO/IEC 23008-3:2020. Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 3: 3D audio. Geneva: ISO/IEC, 2020. 236 p.
6. ISO/IEC 23003-4:2015. MPEG-D Dynamic Range Control. Geneva: ISO/IEC, 2015. 98 p.
7. AES69-2015 (r2020). AES standard for file exchange of loudspeaker and microphone data using the SOFA format. New York: AES, 2020. 34 p.
8. Zwicker E., Fastl H. Psychoacoustics: Facts and Models. 3rd ed. Berlin; Heidelberg: Springer, 2013. 505 p.
9. Moore B. C. J., Glasberg B. R. A Revision of Zwicker's Loudness Model // Acta Acustica. 1997. Vol. 82, No. 2. P. 335–345.
10. Zölzer U. (ed.). DAFX — Digital Audio Effects. 3rd ed. Chichester: Wiley, 2022. 864 p.
11. Pulkki V., Karjalainen M. Communication Acoustics. Chichester: Wiley, 2015. 456 p.
12. Steinmetz C. J., et al. Neural Audio Effects: Learning Parametric Emulations // Proc. DAFx. 2020. P. 1–8.
13. Algazi V. R., Duda R. O., Thompson D. J., Avendano C. The CIPIC HRTF Database // Proc. IEEE WASPAA. 2001. P. 99–102.
14. Farina A. Simultaneous Measurement of Impulse Response and Distortion with a Swept-Sine Technique // 108th AES Convention, Preprint 5093. 2000. 18 p.
15. Maki A., Takanashi M. Personalized HRTF Estimation from Anthropometry Using Deep Regression // IEEE/ACM TASLP. 2019. Vol. 27, No. 3. P. 515–527.

* Список литературы составлен в авторской редакции.

16. Stitt P., Oldfield R., Wierstorf H. The SADIE II Database for Spatial Audio. York: University of York, 2016. URL: https://www.york.ac.uk/sadie-project (дата обращения: 21.10.2025).
17. Rafii Z., Liutkus A., et al. MUSDB18 — a corpus for music separation // Proc. ISMIR. 2017. P. 1–6.
18. ITU-T P.863. POLQA. Geneva: ITU, 2018. 66 p.
19. Regulation (EU) 2016/679 (GDPR). Official Journal of the EU. 2016. 88 p.
20. EU AI Act (proposal). Brussels: European Commission, 2021. URL: https://eur-lex.europa.eu (дата обращения: 21.10.2025).
21. European Data Protection Board. Guidelines on processing of personal data in connected devices. Brussels: EDPB, 2020. 35 p.
22. Dirac Research AB. Dirac Live / Room Correction — Technical Overview. Uppsala, 2022. URL: https://www.dirac.com (Дата обращения: 21.10.2025).
23. RCF S.p.A. FIRPHASE Technology White Paper. Reggio Emilia, 2022. URL: https://www.rcf.it (Дата обращения: 21.10.2025).
24. Dolby Laboratories. Dolby Atmos for Music — Technical Guidelines. San Francisco, 2021. URL: https://professional.dolby.com (Дата обращения: 21.10.2025).
25. Taal C. H., Hendriks R. C., Heusdens R., Jensen J. STOI Intelligibility Prediction // IEEE TASLP. 2011. Vol. 19, No. 7. P. 2125–2136.

Приложение А
Расчёт задержек и параметров STFT

Целевой бюджет суммарной задержки ≤ 35 мс. При 48 кГц и окне L=1024 (шаг H=L/4) задержка STFT ≈ 21,3 мс. Для конволюции — разбиение: первые 256 тапов — во времени (≈2,7 мс), хвост — в частоте (редкие крупные блоки). DRC/EQ — 3–5 мс. Кодек/буферы добавляют 5–10 мс; суммарно 28–35 мс в типичных наушниковых сценариях [1; 6; 23].

Приложение Б
Чек-листы внедрения

Технический: валидация задержки; стресс-тесты worst-case; контроль true-peak; ADM/MPEG-H; защита от переинверсии; деградация качества. Юридический: согласие на обработку профилей; локальное хранение; право на удаление; журнал вмешательств; экспорт профиля. UX: понятные пресеты; обратная связь; предупреждения о длительной экспозиции; режим «дети»; доступность интерфейса.

Приложение В
A/B и пилотные релизы малого охвата с автоматическим откатом при ухудшении качества

Метрики: MUSHRA/POLQA/STOI, удержание, жалобы, энергия. Рандомизация по пользователям/устройствам; длительность — ≥2 недели. Критерии остановки и автооткат при ухудшении. Прозрачные сообщения пользователю при существенных изменениях качества.

Приложение Д
Шаблоны SLA и guardrails

SLA: задержка <35 мс; true-peak < −1 дБFS; отсутствие щелчков/обрывов; стабильность панорамы; безопасность слуха (лимит дозы). Guardrails: диапазоны EQ/DRC, запрет на переворот панорамы / чрезмерную реверберацию, инварианты для вокала/соло, ограничения на скорость/амплитуду изменений.

Приложение Е
Словарь используемых терминов и сокращений

Амплитудно-частотная характеристика (АЧХ) — это зависимость амплитуды колебаний выходного сигнала некоторой системы от частоты её входного сигнала.

Аудиограмма — индивидуальный порог слышимости по частотам, используемый для персональной коррекции.

Кроссфейд — плавный переход между конфигурациями или сигналами, исключающий щелчки и скачки уровня. В литературе также встречается перевод «плавное перекрытие».

Персональный звук — режим воспроизведения, при котором параметры звучания подстраиваются под конкретного слушателя, устройство и акустическую обстановку.

Регрессор — модель регрессии, отображающая набор признаков (в т.ч. эмбеддинг) в непрерывные параметры обработки (например, настройки эквализации или компрессии).

Стем (stem) — термин в производстве аудио, который означает отдельные аудиофайлы, представляющие конкретные компоненты песни.

Транзиент — короткий участок сигнала с резкой атакой и высоким пиковым уровнем (например, удар барабана или щипок струны); важен для субъективной «ударности» и читаемости.

Эквализация — частотная коррекция тембра аудиосигнала с целью согласования с целевым спектром.

Эмбеддинг — компактное числовое (векторное) представление объекта; в аудиозадачах используется для описания трека или фрагмента по набору акустических и контекстных признаков.

ADM, Audio Definition Model — стандарт описания аудиообъектов и метаданных для совместимого обмена между студиями и сервисами.

BRIR, Binaural Room Impulse Response — импульсная характеристика помещения, записанная на два уха; используется для моделирования сцены и коррекции комнаты.

DI, Dependency Injection — это подход к проектированию в объектно-ориентированном программировании, при котором объект получает необходимые ему зависимости извне, а не создаёт их самостоятельно. Этот подход улучшает гибкость, тестируемость и поддерживаемость кода.

DRC, Dynamic Range Control — динамическое управление диапазоном громкости для повышения разборчивости и безопасности прослушивания.

DSP, Digital Signal Processing — цифровая обработка сигналов; также специализированный процессор (аудио DSP), выполняющий вычисления обработки звука в реальном времени.

ERB, Equivalent Rectangular Bandwidth — эквивалентная прямоугольная полоса пропускания — это мера, используемая в психоакустике, которая позволяет приблизительно определить ширину полосы пропускания фильтров в слуховом аппарате человека.

EQ, Equalizer — эквалайзер; настройка амплитудно частотной характеристики для коррекции тембра.

FIR, Finite Impulse Response — фильтр с конечной импульсной характеристикой; часто применяется для линейно фазной коррекции.

Guardrails — заранее заданные границы изменений параметров, сохраняющие художественный замысел.

Headroom — резерв по уровню сигнала до клиппинга и искажений; используется при мастеринге и последующей обработке для сохранения запаса амплитуды.

HRTF, Head-Related Transfer Function — набор частотно зависимых откликов, описывающих, как уши человека принимают звук с разных направлений.

IIR, Infinite Impulse Response — рекурсивный фильтр; используется для эффективной коррекции с малой задержкой.

ILD, Interaural Level Differences — межзвуковая разница уровней (также известна как межфоническая разница интенсивности). Это разница в уровне звукового давления, достигающего двух ушей.

ITD, Interaural Time Differences — межфоновая разница во времени. Согласно теории дуплекса, ITD вносят больший вклад в локализацию низкочастотных звуков (ниже 1 кГц), в то время как ILD используются для локализации высокочастотного звука.

LUFS, Loudness Units relative to Full Scale — единицы громкости относительно полного масштаба; метрика нормализации уровней по BS.1770.

LRA, Loudness Range — оценка разброса громкости в программе; применяется для настройки динамической обработки.

MPEG H — семейство стандартов кодирования и доставки объектного и трёхмерного звука.

MUSHRA, MUltiple Stimuli with Hidden Reference and Anchor — методика субъективной оценки качества звука с использованием эталонов и деградированных версий.

NPU, Neural Processing Unit — нейропроцессорный блок, предназначенный для ускорения вычислений моделей машинного обучения на устройстве.

POLQA, Perceptual Objective Listening Quality Assessment — объективная метрика качества речи по стандарту ITU T P.863.

Room correction — компенсация влияния акустики помещения на спектр и время отклика системы.

SOFA, Spatially Oriented Format for Acoustics — формат хранения акустических измерений (в т.ч. HRTF/BRIR) согласно AES69.

Spatializer — это технология или плагин, который создаёт иллюзию трёхмерного звука, имитируя, как звук ведёт себя в физическом пространстве.

STOI, Short-Time Objective Intelligibility — объективная метрика прогнозирования разборчивости речи.

STFT, Short-Time Fourier Transform — представление сигнала во временно частотной области для блочной обработки и анализа.

SoC, System on Chip — система на кристалле; интегрированная микросхема, объединяющая вычислительные блоки (CPU/GPU/DSP/NPU) и периферию.

SNR, Signal-to-Noise Ratio — отношение сигнал/шум; показатель условий прослушивания и качества входных измерений.

Source separation — выделение компонентов микса (вокал, ударные и т.п.) для адресной обработки.

SLA, Service Level Agreement — целевые пределы задержки и стабильности системы, соблюдение которых контролируется в реальном времени.

True-peak — «истинный пик»: пиковое значение сигнала с учётом интерполяции (междискретных пиков); применяется для предотвращения клиппинга при преобразованиях и кодировании.

Taste profiling — агрегация признаков предпочтений слушателя для настройки тембра и динамики в допустимых пределах.

UX, User Experience — совокупность характеристик пользовательского опыта (удобство, предсказуемость, контроль), определяющих взаимодействие человека с системой.

УДК: 004.056.53

Защита SIP-регистраций от атак методом динамической смены портов

Gurovskiy I.D., Makhnich G.V., Kruglov A.M., Saulin I.A.

Protection of SIP Registrations from Attacks by Dynamic Port Change Method

Abstract. *This article discusses a method for increasing the resilience of SIP devices to attacks on SIP registrations. The method is based on the dynamic change of ports for receiving registration requests. A prototype was implemented using Asterisk software platform and an experiment was conducted in a laboratory environment. It is shown that the proposed approach reduces the proportion of successful attacks with minimal impact on server performance.*

Keywords: *Session Initiation Protocol, IP telephony, security, dynamic port change, REGISTER attack.*

Гуровский И.Д.[1]
Махнич Г.В.[2]
Круглов А.М.[3]
Саулин И.А.[4]
[1]Студент, МИРЭА – Российский технологический университет.
E-mail: gurovskiy.i.d@edu.mirea.ru
[2]Студент, МИРЭА – Российский технологический университет.
E-mail: makhnich.g.v@edu.mirea.ru
[3]Преподаватель кафедры телекоммуникаций, Институт радиоэлектроники и информатики, МИРЭА – Российский технологический университет.
E-mail: kruglov@mirea.ru
[4]Студент, МИРЭА – Российский технологический университет.
E-mail: saulin.i.a@edu.mirea.ru

Аннотация. *В статье рассмотрен метод повышения устойчивости SIP-устройств к атакам, связанным с процессом SIP-регистрации. Метод основан на динамической смене портов приёма регистрационных запросов. Реализован прототип с использованием программной платформы Asterisk и проведён эксперимент в лабораторной среде. Показано, что предложенный подход снижает долю успешных атак при минимальном влиянии на производительность сервера.*

Ключевые слова: *протокол инициирования сеанса, IP-телефония, защита от несанкционированного доступа, динамическая смена портов, REGISTER-атака.*

ВВЕДЕНИЕ

За последние годы IP-телефония стала стандартом корпоративной связи. Одним из наиболее распространенных протоколов сигнализации остается протокол SIP, который предназначен для установления связи, модификации и завершения мультимедийных сеансов между клиентами. В архитектуре VoIP (от англ. “Voice over Internet Protocol” — «голос поверх интернет-протокола») он отвечает за передачу сообщений регистрации, адресацию абонентов, согласование параметров соединения и маршрутизацию вызовов. SIP работает поверх протоколов UDP, TCP или TLS[1] и обладает открытой текстовой структурой, что упрощает разработку, но в то же время часто делает его уязвимым к различным видам атак. [1, 2]

Наиболее распространённые атаки — массовый подбор паролей, схожий с «brute force» (полный перебор), и массовая отправка регистрационных запросов (например, «REGISTER flooding»). Эти атаки приводят к компрометации учётных записей, нарушению работоспособности сервера и к увеличению операционных расходов. Типовая конфигурация SIP-сервера имеет фиксированный порт приёма запросов — стандартный UDP порт 5060 (для SIP-сигнализации). Эта предсказуемость облегчает работу злоумышленников. [3, 4]

Существующие меры защиты включают аутентификацию, фильтрацию адресов, правила на уровне межсетевого экрана (firewall) и инструменты типа Fail2ban (средство автоматической блокировки источников по журналам событий). Эти меры по-прежнему остаются рабочими, однако их существенным недостатком остается то, что для полноценной защиты необходимо их совместное использование, чтобы нивелировать проблемы каждой из них. [5, 6]

Вместе с тем, в современных VoIP-инфраструктурах на практике применяются и более развитые механизмы противодействия: корреляция событий по журналам сигнализации и сетевым признакам, поведенческие фильтры и адаптивное ограничение частоты запросов (rate limiting) на уровне идентификаторов и источников трафика.

[1]UDP – User Datagram Protocol, протокол пользовательских датаграмм; TCP – Transmission Control Protocol, протокол управления передачей; TLS – Transport Layer Security, протокол защиты транспортного уровня.

Отдельный класс составляют пограничные устройства (Session Border Controller, SBC – пограничный контроллер сеансов) и специализированные VoIP-межсетевые экраны, выполняющие валидацию SIP-сигнализации, нормализацию сообщений, сокрытие топологии и ограничение аномальной активности, включая сценарии регистрации. Указанные средства повышают устойчивость к массовым воздействиям, однако требуют дополнительной инфраструктуры и зачастую решают задачу на уровне периметра, не устраняя предсказуемость точки входа при использовании стандартного порта регистрации. [7, 8]

В рамках статьи была поставлена задача рассмотреть существующие способы защиты SIP и оценить их эффективность, а также выполнить сравнение с предложенным методом периодической смены порта приёма регистрационных запросов. Эффективность сравнения фиксируется по следующим показателям: числу успешных регистраций нарушителя за заданный интервал времени, среднему времени перерегистрации легитимного клиента и изменению вычислительной нагрузки сервера при моделируемой интенсивности регистрационных запросов. [8, 9]

Практическим ограничением метода считается сохранение работоспособности регистрации для легитимных клиентов при среднем времени перерегистрации на уровне единиц секунд, а также отсутствие существенного роста средней загрузки CPU (Central Processing Unit, центральный процессор) (в пределах нескольких процентных пунктов) по сравнению с контрольным сценарием. [10]

Предлагаемый подход относится к классу проактивных мер снижения поверхности атаки (moving target defense) и рассматривается как дополнительный уровень защиты, не заменяющий криптографические механизмы защищённой сигнализации, аутентификацию и контроль доступа. [11, 12]

В работе предложена и экспериментально оценена реализация проактивного подхода класса «moving target defense» (port hopping) применительно к процедуре SIP-регистрации в стеке Asterisk/PJSIP (PJSIP – программный стек SIP, применяемый в Asterisk). Особенность подхода состоит в интеграции механизма смены порта с автоматизированным обновлением конфигурации клиентов и с сохранением непрерывности. [10, 11]

АКТУАЛЬНОСТЬ И НОВИЗНА

Практическая актуальность защиты SIP-регистраций определяется не только распространённостью IP-телефонии, но и измеримым масштабом злоупотреблений, ориентированных на учетные записи и доступность SIP-инфраструктуры. По данным крупномасштабных измерений на сетевом телескопе фиксируются сотни миллионов попыток подбора SIP-учетных данных: в исследовании Griffioen собрано более 822 млн попыток подбора учётных данных SIP методом полного перебора от 5 691 источника из 187 стран, что указывает на устойчивый «фон» автоматизированного поиска и компрометации VoIP-узлов в глобальной сети. [13]

Дополнительно открытые наблюдения по экспонированным сервисам показывают, что в публичном IPv4-пространстве (IPv4 – Internet Protocol version 4, интернет-протокол версии 4) остаются тысячи SIP-серверов, доступных извне по стандартным портам сигнализации, что облегчает автоматизированное сканирование и проведение атак на регистрацию. [13]

Отраслевые документы операторского уровня также подчёркивают, что атаки на VoIP-системы остаются одним из частых классов интернет-угроз, а отдельным объектом воздействия выступает именно SIP-регистрация: среди релевантных сценариев выделяются компрометация/утечка регистрационных данных, подбор (в т. ч. по передаваемым значениям) и повтор (replay) регистраций, а также атаки «человек посередине» и понижение уровня защиты. [3, 4, 14]

В качестве практических мер снижения риска указываются, в частности, ограничение источников сигнализации (access-lists/ACL – списки контроля доступа), отказ от SIP поверх UDP при внешнем доступе и переход к защищённой сигнализации на базе TCP/TLS, а также применение SBC-класса средств для фильтрации и сокрытия топологии (SBC – Session Border Controller, пограничный контроллер сеансов). [3, 15]

С нормативной точки зрения протокол SIP и его базовые требования определяются RFC 3261, а вопросы защищённого установления соединений и интерпретации защищённых идентификаторов/транспортов конкретизируются, в том числе, рекомендациями по использованию схемы SIPS и связанным с ней нормативным поведением. Дополнительные аспекты построения защищённых SIP-соединений (например, применение доменных сертификатов и особенности повторного использования TLS-соединений в SIP-инфраструктуре) формализованы в профильных RFC (аббр. от “Request for Comments” – серия технических документов Интернета), что позволяет опираться на стандартизованные свойства защищённой сигнализации при

проектировании мер противодействия атакам на регистрацию. [1, 2, 7, 16, 17]

Наряду с атаками на учетные данные, сохраняют актуальность и сценарии «flooding» на уровне SIP-сигнализации (включая регистрационные запросы), что подтверждается современными работами по обнаружению и классификации SIP-flooding/DDoS[2]. [18, 19]

При этом подход рассматривается как дополнительный уровень защиты, повышающий стоимость автоматизированного сканирования и массовых атак, и не заменяет криптографические механизмы (TLS/SIPS – защищённые механизмы передачи SIP-сигнализации)), аутентификацию и контроль доступа. [2]

На этом фоне новизна предлагаемого подхода может быть обоснована как развитие идей «moving target defense» применительно к SIP-регистрации: динамическое изменение порта приема регистраций усложняет автоматизированное сканирование и повышает сложность атаки, дополняя стандартные меры (аутентификацию, фильтрацию, TLS/SBC) без требования радикальной перестройки SIP-стека. [11]

ОБЗОР СУЩЕСТВУЮЩИХ ПОДХОДОВ К ЗАЩИТЕ SIP

Основные классы атак на SIP-регистрацию

Наиболее типовые угрозы включают подбор регистрационных данных, атаки отказа в обслуживании на уровне сигнализации (в том числе message flooding / REGISTER-flooding), а также подмену регистрации (registration hijacking), при которой нарушитель стремится изменить привязку «адрес записи — контакт» для перехвата входящих вызовов или нарушения доступности.

Для атак типа «flooding» в современных работах рассматриваются методы обнаружения и классификации DDoS/DoS на SIP-сигнализации, включая модели машинного обучения и гибридные схемы детектирования, что подтверждает актуальность угроз доступности для SIP-инфраструктуры. [18, 19]

Меры защиты SIP

• ***Дайджест-аутентификация SIP***. Механизм основан на хэшировании и отправке данных для проверки клиента. Он снижает риск перехвата паролей при пассивном прослушивании. Однако при активном подборе паролей аутентификация сама по себе не предотвращает атаку. [1, 7]

• ***Fail2ban и блокировка по логам***. Система отслеживает неудачные попытки и добавляет правило в межсетевой экран. Такой подход – эффективный, но медленный: требуется собрать статистику и сгенерировать правило. При распределённых атаках и при использовании большого пула адресов блокировки оказываются малоэффективны. [5, 6]

• ***Шифрование и защищённые транспортные протоколы*** защищают содержимое и сигнализацию от прослушивания и подделки. Однако они не защищают от перебора учётных данных, если атакующий пытается пройти аутентификацию напрямую через открытый порт. [2, 7]

• ***ACL[3] и геоблокировка***. Ограничение диапазонов IP-адресов повышает безопасность, но снижает гибкость. [3]

• ***Проактивные подходы сокрытия/изменения параметров доступа*** (moving target defense). В смежных областях сетевой безопасности применяется класс методов, основанных на динамическом изменении наблюдаемых параметров сервиса с целью усложнения разведки и автоматизированных атак. К таким решениям относятся port hopping (динамическая смена порта/отображения сервиса) и более общий подход «moving target defense». [11]

Отдельно выделяется «port knocking», где доступ к сервису предоставляется после корректной последовательности «стуков» по портам и, таким образом, реализуется скрытая аутентификация на сетевом уровне. Данный подход чаще рассматривается для административного доступа и управления устройствами, но концептуально относится к методам сокрытия точки входа. [11]

Следует отметить, что подобные методы не обеспечивают криптографической стойкости и не заменяют базовые меры безопасности. В инженерной практике они рассматриваются как дополнительный слой, уменьшающий экспонированность сервиса и повышающий трудоёмкость массовых автоматизированных атак; использование «скрытия» как единственного барьера относится к подходу «security through obscurity» (безопасность через сокрытие) и не должно рассматриваться как достаточная мера защиты. [11]

• ***IDS/IPS[4] и сигнатурный анализ SIP-сигнализации***. Для выявления атак на уровне SIP приме-

[2]Flooding – от англ. «лавинная отправка сообщений»; DDoS – Distributed Denial of Service, распределённый отказ в обслуживании.

[3]ACL – Access Control List, список контроля доступа.

[4]IDS – Intrusion Detection System, система обнаружения вторжений; IPS – Intrusion Prevention System, система предотвращения вторжений.

няются системы сетевого анализа с поддержкой прикладного разбора протокола и сопоставления с правилами/сигнатурами. В частности, в Snort реализован специализированный препроцессор SIP, упрощающий детектирование атак и уязвимостей, связанных с обработкой SIP. В Suricata предусмотрены SIP-ориентированные поля и “sticky buffers” (закреплённые буферы правил анализа), позволяющие строить правила по методам/заголовкам SIP, что применимо для выявления аномалий и попыток злоупотребления регистрацией. [20]

Отдельные исследования предлагают архитектуры SIP IDS/IPS и прототипы, расширяющие Snort для анализа SIP поверх UDP/TCP, что демонстрирует практическую применимость данного класса средств для защиты VoIP-сетей. [20]

• ***Session Border Controller (SBC)*** и операторские меры защиты. В корпоративной и операторской практике для защиты SIP-транкинга и пограничных узлов широко применяется класс устройств SBC, выполняющих функции контроля сигнализации, фильтрации, ограничения нежелательных запросов и противодействия DoS/DDoS, а также сокрытия топологии и принудительного применения защищённых транспортов. Типовые механизмы и сценарии противодействия SIP-атакам, включая меры против «flooding» и блок-листы, подробно описываются в руководствах по безопасности производителей SBC. [3, 4, 15]

Перечисленные меры снижают риск компрометации и повышают устойчивость, однако часть из них требует заранее ограничивать периметр (ACL/SBC), а часть реагирует уже после начала атаки (fail2ban/IDS). [3, 5, 15, 20]

РАЗРАБОТАННЫЙ ЛАБОРАТОРНЫЙ СТЕНД

Лабораторный стенд представлен на рисунке 1 и реализован в локальной сети с использованием следующих компонентов:

— сервер IP-телефонии: ОС AstraLinux 1.7, Asterisk 20 с PJSIP, Python 3.11;

— рабочие места: IP-телефон с поддержкой протокола SIP: Eltex VP-15P, компьютер с ОС AstraLinux 1.7, MicroSIP;

— коммутатор с поддержкой PoE: Eltex MES2324P;

— компьютер злоумышленника: ОС AstraLinux 1.7;

— инструменты для атаки: SIPVicious (SVMap, SVCrack), скрипты генерации REGISTER в Python.

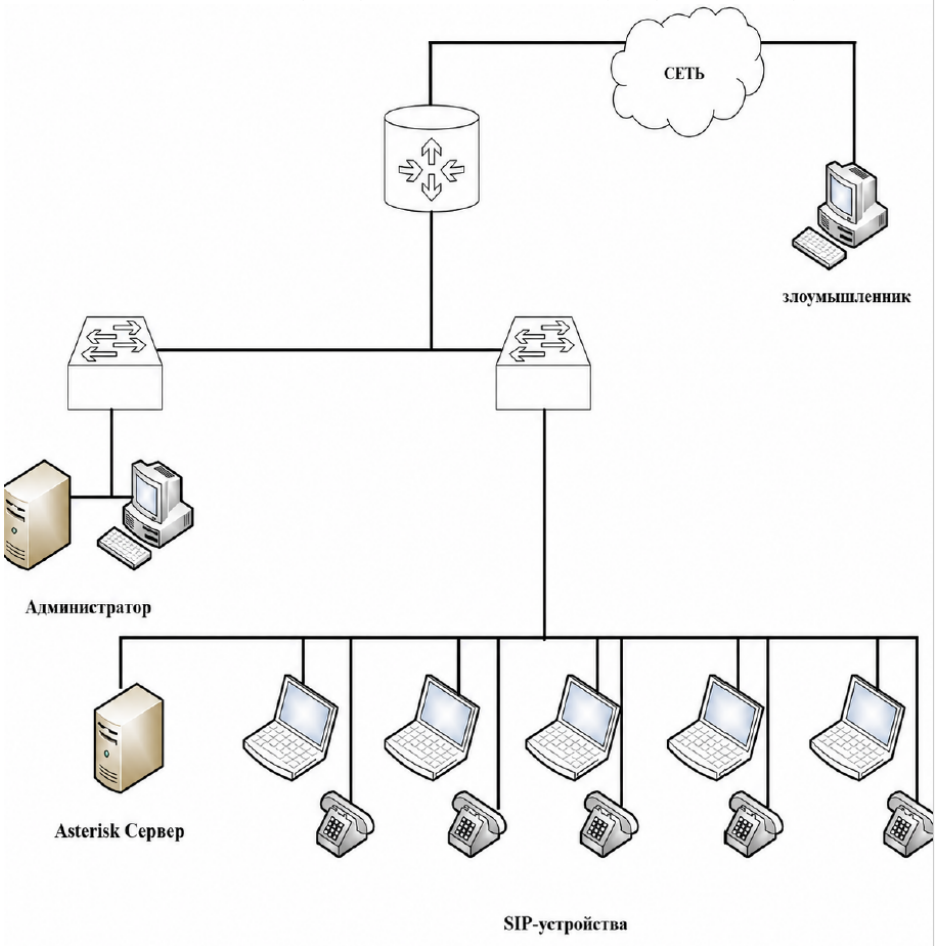

Рис. 1. Схема лабораторного стенда

Лабораторный стенд развернут в локальной Ethernet-сети со звездообразной топологией на базе коммутатора Eltex MES2324P (рис. 1). Все узлы стенда находятся в одной L2-широковещательной области и взаимодействуют по интернет-протоколу версии 4 (IPv4) в пределах одной подсети. Преобразование адресов (NAT, Network Address Translation) в лабораторном контуре не использовалось, что фиксирует модель доступности SIP-сервера для атакующего как для узла в той же локальной сети. Канальная скорость соединений составляет 1000 Мбит/с, при этом измеренная пропускная способность между узлами по TCP/UDP-тестам составляет около 930 Мбит/с (TCP) и порядка 900 Мбит/с (UDP).

Для исключения влияния внешней сети были оценены задержки доставки пакетов внутри контура: средняя односторонняя задержка между клиентами и сервером составила 0,2–0,5 мс, джиттер — менее 1 мс, потери пакетов — 0% при фоновой нагрузке отсутствовала либо была минимальной (служебный трафик).

В рамках эксперимента SIP-сигнализация передавалась по UDP, медиа-трафик (RTP – Real-time Transport Protocol, протокол передачи данных в реальном времени) — по RTP/UDP. Шифрование сигнализации (SIPS/TLS) и медиа (SRTP – Secure RTP, защищённый RTP) не использовалось, поскольку цель эксперимента заключалась в оценке влияния механизма смены порта на устойчивость к атакам на регистрацию и на эксплуатационные метрики.

УСТРОЙСТВО РАБОТЫ СХЕМЫ

Метод заключается в периодическом изменении UDP-порта, на котором SIP-сервер принимает запросы на регистрацию. Порт выбирается случайно в заранее определённом диапазоне. Период изменения настраивается. Смена порта не требует модификации SIP-протокола. Достаточно обновить конфигурацию модуля res_pjsip Asterisk (модуль Asterisk для работы со стеком PJSIP) и выполнить его перезагрузку. Архитектура прототипа включает три компонента:

1. SIP-сервер (Asterisk). Работает с PJSIP и поддерживает параметр «bind» (привязку сервиса к сетевому адресу и порту) для транспортного протокола UDP.

2. Порт-менеджер (Python-скрипт). Периодически выбирает новый порт и записывает его в конфигурацию. Выполняет «reload» (перезагрузку конфигурации без полной остановки сервиса) соответствующего модуля через Asterisk.

3. Синхронизатор с клиентами. Записывает конфигурационный файл для SIP-устройств на сервер, откуда они загружают обновленный конфигурационный файл.

Рассматриваемый метод предполагает наличие контура управления, обеспечивающего доведение актуального порта регистрации до легитимных клиентов (через конфигурационный сервер и программный интерфейс приложения – Application Programming Interface, API). Следует отметить, что компрометация конфигурационного сервера или интерфейса управления приводит к возможности навязывания клиентам неверных параметров регистрации, что может нивелировать эффект защиты. Поэтому защищённость управляющего канала является обязательным условием корректного применения подхода и должна обеспечиваться аутентификацией клиентов, защищённой передачей, сетевой изоляцией доступа к API и аудитом операций управления.

Схематическая работа алгоритма представлена на рисунке 2.

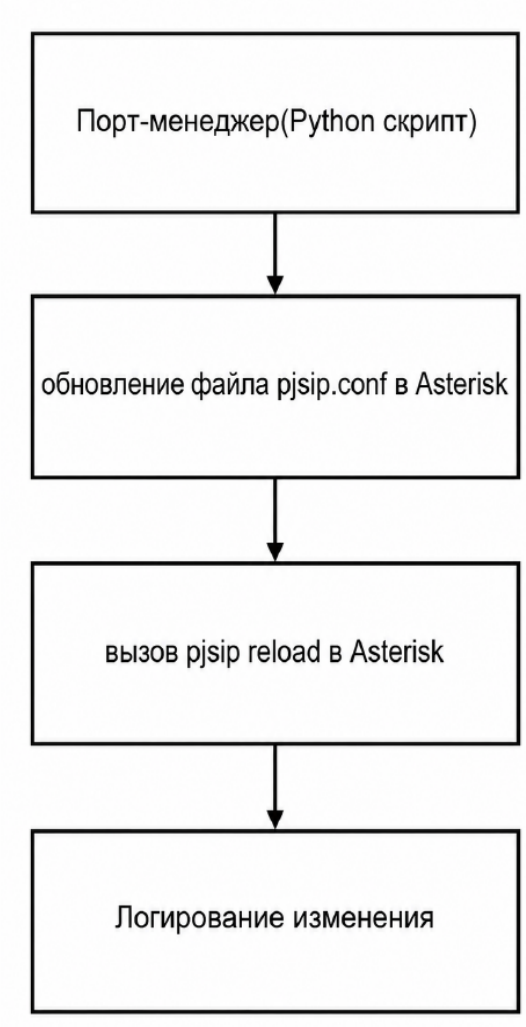

Рис. 2. Работа Python-скрипта

ОПИСАНИЕ РЕАЛИЗАЦИИ

Порт-менеджер — это автономный Python-скрипт. Он выполняет следующие шаги:

1) читает текущую конфигурацию pjsip.conf;

2) выбирает случайный порт из диапазона 40000–60000;

3) записывает новый порт в соответствующий блок транспорта;

4) выполняет команду 'asterisk -rx "pjsip reload"' для применения изменений;

5) логирует событие в файл '/var/log/port_change.log';

6) отправляет POST-запрос (POST – метод HTTP для отправки данных на сервер) на загрузку новой конфигурации на сервер.

Телефон проверяет конфигурацию на сервере раз в 60 секунд и загружает обновленный конфигурационный файл с измененным портом по указанному в нем URL-адресу на сервер до файла. Если файл изменен, телефон применяет обновленную конфигурацию, если нет — оставляет конфигурационный файл неизменным. Обеспечение непрерывности во время звонка осуществляется за счёт откладывания изменения SIP-параметров до завершения вызова. После успешной загрузки нового транспорта старый удаляется. Такой подход уменьшает вероятность потери текущих вызовов. Клиенты настроены на автоматическую перерегистрацию. Период регистрации составляет 300 секунд. Это позволяет клиенту в течение короткого времени получить новую конфигурацию через API и выполнить повторную регистрацию.

Для снижения вероятности отказа регистрации при задержках распространения конфигурации целесообразно использовать переходный интервал, в течение которого сервер принимает REGISTER как на новом, так и на предыдущем порту. При недоступности конфигурационного сервера или сбое обновления клиент должен сохранять последнюю валидную конфигурацию и повторять попытки получения обновления через заданные интервалы, не прерывая работу текущей регистрации. Дополнительно возможны резервирование конфигурационного сервера и механизм отката к предыдущему порту при массовых ошибках регистрации в период смены параметров.

Частая смена порта требует расширенного контроля событий, чтобы отделять штатные переходные процессы от атак и рассинхронизации. Для использования метода на практике необходимо фиксировать:

— событие смены порта;

— долю успешных/неуспешных регистраций в окнах до и после смены;

— количество попыток регистрации на “устаревшем” порту вне переходного интервала;

— последовательные попытки регистрации по множеству портов за короткое время;

— аномальный рост ошибок аутентификации и таймаутов.

ОЦЕНКА РЕЗУЛЬТАТОВ

Эксперимент направлен на сравнение эффективности трёх подходов защиты SIP-регистрации. Для сравнения используются показатели числа успешных регистраций нарушителя за фиксированный интервал времени, среднее время перерегистрации легитимного клиента, средняя загрузка центрального процессора Asterisk при заданной интенсивности атакующего трафика.

Под успешной регистрацией злоумышленника понимается завершение процедуры REGISTER с получением от сервера ответа 200 OK (успешный ответ SIP/HTTP-подобной сигнализации о выполнении запроса) и появлением активной регистрации в таблице контактов SIP-сервера (по данным Asterisk/PJSIP).

В рамках работы предполагается, что нарушитель имеет сетевую доступность SIP-узла и способен генерировать поток REGISTER-запросов с применением типовых инструментов (SIPVicious и скрипты генерации REGISTER). Нарушитель не имеет доступа к управляющему каналу распространения текущего порта регистрации и не получает сведения о новом порте из доверенного контура. Данная постановка оценивает устойчивость метода к массовым автоматизированным атакам, использующим предсказуемость стандартной точки входа SIP-сигнализации по UDP (порт 5060). Сценарии адаптивного поведения нарушителя (непрерывное сканирование диапазона портов, подстройка стратегии к интервалу смены порта, координация распределённых ботов) в настоящей серии не моделировались и рассматриваются как направление дальнейшего исследования.

Были проведены три сценария:

1) контрольный сценарий (без защиты): сервер принимает REGISTER на порту 5060, Fail2ban отключён;

2) fail2ban: стандартная конфигурация Fail2ban и iptables;

3) динамическая смена порта: интервал смены порта 600 секунд, Fail2ban отключён для оценки эффекта только смены порта.

Во всех сценариях использовался генератор атак, формирующий поток REGISTER-запросов интенсивностью до 1000 запросов в секунду.

Таблица 1

Результаты тестов

Параметр	Контрольный сценарий	Fail2ban	Смена портов
Успешные регистрации злоумышленника за 1 час	580	120	12
Средняя загрузка CPU Asterisk	23 %	27 %	25 %
Среднее время перерегистрации легитимного клиента (в секундах)	4	5	2

Интерпретация результатов

Сценарий динамической смены порта снизил число успешных регистраций злоумышленника с 580 до 12 за час, что соответствует уменьшению в 48,3 раза по сравнению с контролем. По сравнению со сценарием Fail2ban снижение составило 10 раз. Рост средней загрузки CPU относительно контроля составил 2%, а среднее время перерегистрации легитимного клиента составило 2 секунды в сценарии смены порта.

Поскольку для каждого сценария приведён одиночный часовой прогон, эмпирическая вариативность результатов по повторным измерениям в работе не оценивается. Для ориентировочной оценки неопределённости счётчика «успешные регистрации за час» использована пуассоновская модель для числа событий за фиксированный интервал времени. В этом приближении 95% доверительные интервалы для среднего числа событий.

Сравнение с Fail2ban демонстрирует преимущество метода динамической смены портов в сценарии массовой автоматизированной атаки, использующей предсказуемость стандартного порта. Вместе с тем, в практической защите SIP-регистрации применяются и другие классы мер, решающие задачу иными способами. Так, «rate limiting» (ограничение частоты запросов) позволяет сдерживать flooding-нагрузку и замедлять перебор паролей, не полагаясь на скрытие порта. SIP-aware firewalls[5]/VoIP-файрволы и SBC выполняют разбор и нормализацию SIP-сообщений, вводят протокольные ограничения и политики (включая контроль регистраций), а также обеспечивают периметровую фильтрацию и сокрытие топологии. Поведенческие IDS/IPS и корреляция событий по журналам позволяют выявлять аномалии и распределённые атаки, в том числе при изменяемых сетевых параметрах, за счёт анализа профилей трафика и последовательностей событий.

Метод динамической смены порта относится к классу «moving target defense» и не заменяет перечисленные подходы, а дополняет их, повышая сложность автоматизированного сканирования и массовых атак на регистрацию при условии, что нарушитель ориентируется на стандартный порт и не обладает доступом к управляющему контуру.

Эффект метода снижается или становится ограниченным в ряде сценариев. Во-первых, при адаптивном нарушителе, выполняющем непрерывное сканирование диапазона портов и подстраивающем стратегию к частоте смены порта, выигрыш может сокращаться до величины, определяемой шириной диапазона и параметрами сканирования. Во-вторых, метод мало полезен против атак, не зависящих от знания порта регистрации, включая компрометацию учётных данных вне SIP-канала (утечки, фишинг), а также против атак на доступность и ресурсы, реализуемых на других уровнях (например, истощение канала или нагрузка на инфраструктурные компоненты). В-третьих, при компрометации управляющего канала распространения параметров регистрации (API/конфигурационный сервер) нарушитель получает возможность нивелировать эффект защиты. Также при эксплуатации в сетях с NAT/провайдерскими ограничениями и жёстко заданными правилами портов на периметре использование динамических портов может быть затруднено и требовать дополнительных согласований.

Таким образом, метод следует рассматривать как дополнительный барьер, наиболее эффективный в управляемых корпоративных сегментах для снижения сторонней процедуры регистрации и уменьшения доли успешных атак, но требующий совместного применения с базовыми мерами (аутентификация, защищённые транспорты, контроль доступа, «rate limiting» и периметровая фильтрация).

[5]SIP-aware firewalls – межсетевые экраны с разбором SIP.

ОГРАНИЧЕНИЯ И ПРАКТИЧЕСКАЯ ПРИМЕНИМОСТЬ

Предлагаемый метод относится к классу проактивных мер снижения поверхности атаки и предполагает наличие контура управления, который доставляет легитимным клиентам актуальные параметры регистрации. В эксплуатационной среде это приводит к росту сложности администрирования по сравнению с фиксированным портом: требуется поддерживать актуальность конфигурации на клиентских устройствах, контролировать корректность применения параметров и обеспечивать отказоустойчивость механизма распространения конфигурации. При нарушении синхронизации (задержки обновления, временная недоступность конфигурационного сервера, рассогласование политик доступа) повышается риск деградации сервиса и нарушения показателей SLA (Service Level Agreement, соглашение об уровне обслуживания), поскольку клиент может потерять возможность регистрации до восстановления согласованного состояния.

Существенным практическим ограничением являются сценарии работы удалённых и мобильных клиентов. При регистрации через NAT и публичные сети часть провайдеров и корпоративных политик межсетевого экранирования ограничивает прохождение трафика на нестандартные UDP-порты. В таких условиях динамическая смена порта может приводить к неоднородному качеству регистрации для клиентов, подключённых из разных сегментов, особенно при использовании гостевых Wi-Fi и мобильных сетей. Следовательно, для удалённого доступа метод целесообразно применять совместно с контролируемым способом выхода в корпоративную сеть.

Практическая применимость в распределённых корпоративных сетях и у операторов определяется совместимостью с периметровой инфраструктурой. В ряде случаев порты SIP-сигнализации фиксируются в правилах межсетевых экранов, списках контроля доступа и пограничных устройствах, а внешние SIP-транки могут предполагать заранее согласованные параметры сигнализации. Это ограничивает возможность использования динамической смены порта на стыке с внешними сетями и делает более реалистичным применение метода на внутренних регистрационных интерфейсах (например, для корпоративных SIP-устройств в управляемой сети), где контроль политик доступа и обновления конфигурации находится в зоне ответственности администратора.

Для крупной операторской инфраструктуры с обязательным использованием SBC и регламентированных точек входа метод в первую очередь может рассматриваться как дополнительный механизм на отдельных сегментах, но не как замена стандартных мер периметровой защиты и криптографически защищённой сигнализации.

Отдельного внимания требует влияние динамической смены порта на средства наблюдаемости. Изменение точки входа усложняет настройку систем мониторинга и детектирования атак, использующих статические правила по портам (сетевые датчики, IDS/IPS, пассивные SIP-пробы. В практической реализации необходима интеграция механизма смены порта с системами мониторинга и учёта событий: фиксация смены параметров регистрации, контроль ошибок регистрации в окнах смены, а также поддержание актуальных политик фильтрации на периметре. При отсутствии такой интеграции возрастает риск ложных срабатываний и усложняется расследование инцидентов.

Таким образом, метод наиболее применим в сценариях, где клиентские устройства управляемы и поддерживают централизованное обновление конфигурации, доступность портов контролируется администратором, контур управления защищён и отказоустойчив, мониторинг учитывает факт динамической смены параметров. В средах с жёстко фиксированными правилами портов на стыке с внешними сетями и при наличии существенных ограничений провайдеров на нестандартные порты применение метода требует дополнительных согласований или может быть ограничено внутренними сегментами.

ЗАКЛЮЧЕНИЕ

Результаты исследования показали работоспособность превентивного метода защиты SIP-регистраций методом динамической смены портов, который снижает долю успешных атак при невысокой стоимости внедрения. Метод полезен в сочетании с традиционными мерами безопасности и совместим с большинством современных SIP-клиентов.

Ключевое требование — наличие защищённого канала для передачи информации о текущем порте. В корпоративной среде это обычно достигается через VPN или централизованное управление конфигурацией устройств. Для динамически оповещаемых клиентов потребуется механизм обновления конфигурации.

Из ограничений можно отметить необходимость синхронизации. Если клиент не получил новое значение порта, он не сможет зарегистрироваться. Это ограничивает применение в сетях с ненадёжными каналами управления.

Дополнительно следует учитывать риски, связанные с контуром управления: компрометация конфигурационного сервера или интерфейса распространения параметров регистрации может привести к навязыванию клиентам неверных значений и снижению эффективности защиты, поэтому требуется защита канала управления (аутентификация, TLS, ограничение доступа и аудит). В связи с частой сменой порта также предъявляются требования к мониторингу: необходимо контролировать ошибки регистрации в момент смены параметров и выявлять аномалии, характерные для сканирования и попыток обхода механизма.

СПИСОК ЛИТЕРАТУРЫ

1. Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schooler E. SIP: Session Initiation Protocol. RFC 3261. 2002. P. 57-63.

2. Audet F., Jennings C. The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP). RFC 5630. 2009. P. 10-15.

3. National Institute of Standards and Technology. Security Considerations for Voice Over IP Systems. NIST Special Publication 800-58. 2005. P. 43-45.

4. VoIP Security Alliance. VoIP Security and Privacy Threat Taxonomy. Technical Report. 2005. P. 27-28.

5. Porter T. Practical VoIP Security. Syngress, 2006. P. 145-181.

6. Морозов А. М. Анализ уязвимостей сети SIP к угрозам фрода // Электросвязь. 2013. С. 10-13.

7. Peterson J., Jennings C. Security Mechanism Agreement for the Session Initiation Protocol (SIP). RFC 3329. 2003. P. 6-10.

8. Hilt V., Sparks R., Johnston A. Session Initiation Protocol (SIP) Overload Control. RFC 7339. 2014. P. 13-19.

9. Hilt V., Noel E., Shen C., Abdelal A. Design Considerations for Session Initiation Protocol (SIP) Overload Control. RFC 6357. 2011. P. 14-21.

10. Van Meggelen J., Smith J., Madsen L. Asterisk: The Future of Telephony. O'Reilly Media, 2020. P. 1-24.

11. de Graaf S., de Laat R., van der Stok P. Improved Port Knocking with Strong Authentication // ACSAC. 2005. P. 451-454.

12. Sisalem D., Floroiu J., Kuthan J., Abend U., Schulzrinne H. SIP Security. John Wiley & Sons, 2009. P. 225-278.

13. Griffioen H., Hu H., Doerr C. SIP Bruteforcing in the Wild: An Assessment of Adversaries, Techniques and Tools. IFIP Networking Conference. 2021. P. 1-2.

14. Androulidakis I. I. VoIP and PBX Security and Forensics: A Practical Approach. Springer Briefs in Electrical and Computer Engineering. 2016. P. 55-73.

15. ETSI. Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN; Threat, Vulnerability and Risk Analysis (TVRA). ETSI TR 187 002. 2008. P. 17-36.

16. Peterson J. Domain Certificates in the Session Initiation Protocol (SIP). RFC 5922. 2010. P. 7-12.

17. Peterson J. Connection Reuse in the Session Initiation Protocol (SIP). RFC 5923. 2010. P. 10-15.

18. Ormazabal G., Nagpal S., Yardeni E., Schulzrinne H. SIP Security: A Denial-of-Service Perspective // IEEE Communications Surveys & Tutorials. 2009. P. 107-132.

19. Hussain S., Djahel S., Zhang Z., Naït-Abdesselam F. A comprehensive study of flooding attack consequences and countermeasures in SIP // Security and Communication Networks. 2015. P. 4438-4450.

20. Израилов К. Е., Макарова А. К., Шестаков А. В. Обобщенная модель защиты от кибератак на VoIP // Вопросы кибербезопасности. 2023. С. 109-118.

УДК: 003.26, 091

Взаимосвязи криптографии и лингвистики в историческом аспекте

E.S. Goncharenko, I.A. Kirillov

The Interrelations Between Cryptography and Linguistics in Historical Perspective

Abstract. *This article presents historical facts about the interrelations between linguistic and cryptographic research. It considers examples of the use of steganography by the ancient Greek poet Epicharmus, which were related to the emergence and spread of acrostic poems in the 5th century BC. The article also discusses statistical studies in 9th-century Arabic linguistics, which led to the development of frequency-based cryptanalysis. It analyzes fragments of Al-Kindi's treatise on deciphering cryptographic messages. The contribution of Leon Battista Alberti (the 15th century) to linguistics and cryptography is considered. The cipher he created – the Alberti disk, as well as his treatise on ciphers, are discussed.*

Keywords: *linguistics, language studies, cryptography, cryptanalysis, steganography, acrostic, Alberti Disc.*

Е.С. Гончаренко[1]
И.А. Кириллов[2]
[1]Кандидат филологических наук, доцент, Московский государственный лингвистический университет.
E-mail: elisea@rambler.ru
[2]Кандидат технических наук, доцент, Московский государственный лингвистический университет.
E-mail: I.A.Kirillov@gmail.com

Аннотация. *. В статье приводятся исторические факты взаимосвязей лингвистических и криптографических исследований. Рассматриваются примеры применения стеганографии древнегреческим поэтом Эпихармом, связанные с возникновением и распространением акростихов в V в. до н.э. Обсуждаются статистические исследования в арабском языкознании IX века, приведшие к созданию частотного криптоанализа. Анализируются фрагменты трактата Аль-Кинди о дешифровании криптографических сообщений. Описывается вклад Леона Батисты Альберти (XV век) в лингвистику и криптографию, в частности, созданный им шифр «диск Альберти», а также его трактат о шифрах.*

Ключевые слова: *лингвистика, языкознание, криптография, криптоанализ, стеганография, акростих, диск Альберти.*

ВВЕДЕНИЕ. СТЕГАНОГРАФИЯ В АНТИЧНОЙ ЛИТЕРАТУРЕ

Криптография и лингвистика тесно связаны как в научном, так и в прикладном смысле. Их многовековые связи послужили взаимному обогащению и развитию.

Стеганография — это практика сокрытия информации в другом сообщении или физическом объекте таким образом, чтобы её наличие не было очевидным для неподготовленного человека. Как правило, скрытые сообщения выглядят как что-то другое или являются частью чего-то другого[1]. Термин происходит от греческих слов στεγανός — скрытый + γράφω — пишу («тайнопись»).

Современная стеганографическая терминология оформилась лишь к концу двадцатого века [1, с.26] и оперирует со следующими основными понятиями:

– ***стеганографическая система*** — совокупность средств и методов для обеспечения скрытого хранения или передачи информации;

– ***сообщение*** — передаваемая (либо хранимая) скрытая информации;

– ***контейнер*** — любая информация, используемая для сокрытия тайного сообщения [1, с.27].

Логика возможных использований стеганографических методов позволяет применить эти методы не только для сокрытия текстовой информации. Так, в подходящий стеганографический контейнер может быть встроено специальное сообщение-маркер, не для сокрытия этого сообщения, а для обеспечения неброской маркировки самого контейнера. Таким способом, если контейнером, например, является некоторое авторское произведение искусства, то метка-сообщение, встроенное в такой контейнер, сможет в прямом смысле обеспечить защиту авторских прав на такое произведение-контейнер и его содержимого.

Именно для целей обеспечения авторского права и были использованы стеганографические акростихи, первое упоминание о которых относится к V веку до н. э. Это упоминание было связано с именем греческого поэта и философа Эпихарма [2, с.332].

[1] Steganography. URL: https://en.wikipedia.org/wiki/Steganography?ysclid=mfkqjpxl58457287077 (Дата обращения: 01.10.2025)

ЭПИХАРМ И ЕГО АКРОСТИХИ

Эпихарм родился в VI веке до н. э. в Древней Греции. Современники Эпихарма отмечали влияние на его мировоззрение пифагорейской философии, а некоторые даже утверждали, что он был учеником Пифагора [2]. Однако значение Эпихарма в истории поэзии несопоставимо важнее, чем его место в истории философии.

Деятельность этого поэта протекала в Сиракузах в конце VI и первой половине V в. до н.э. По сохранившимся античным каталогам Аристотель в своем сочинении «Поэтика» приписывает ему большую роль в истории развития комедии, из чего можно заключить, что Эпихарм первым стал создавать комические пьесы с целостным и законченным действием[2].

Для своих комедий Эпихарм использовал сюжеты не только из древних мифов, но и из повседневной жизни простых людей своего времени. Всего ему приписывается порядка пятидесяти комедий. Однако, ни одна из них не сохранилась полностью [3, с.342]. Во II веке до н. э. усилиями Аполлодора Афинского[3] творческое наследие Эпихарма было собрано воедино. Исходя из восстановленных сборников удалось установить, что они были записаны на древнем дорическом диалекте ямбическими триметрами.

По-видимому, комедии Эпихарма пользовались успехом у современников, содержали большое количество глубоких замечаний и мудрых высказываний. Как можно судить по сохранившимся литературным источникам, от Эпихарма до наших дней дошло значительное количество замечательных афористических изречений, достигших широкого распространения. Среди них: «Ум и видит, ум и слышит, неразумный глух и слеп», «Никто в состоянии гнева ничего не решает, как следует», «Мёртвым быть — ничуть не страшно, умирать — куда страшней», «Рука руку моет».

Весьма возможно, что именно необходимость бороться с плагиатом привела Эпихарма к изобретению акростиха [3, с.347]. При этом само произведение у Эпихарма (обычно – его комедия) в современных стеганографических терминах являлось «контейнером», а «встраиваемой информацией» было имя автора стихотворного произведения, читаемое по первым буквам некоторых стихотворных строк.

К концу жизни Эпихарм, как автор комедий, достиг заслуженной славы и занимал почетное место при дворе Сиракузского тирана Гиерона II. В его честь была воздвигнута бронзовая статуя со следующей надписью: «Насколько великий свет солнца отличается от света звезд и насколько сила моря больше силы рек; настолько превосходил всех мудростью Эпихарм, которого увенчала родина сиракузян» [3, с.347].

ДАЛЬНЕЙШАЯ ИСТОРИЯ РАСПРОСТРАНЕНИЯ АКРОСТИХА

Начиная с III века до н. э. мода на акростихи получает распространение не только в Греции, но и в Риме. Арат[4], греческий поэт III века до н. э., благодаря своим акростихам получил широкую известность среди римских писателей и поэтов. Им восхищались и ему подражали Цицерон и Овидий. Как установили последующие исследования, сам Вергилий часто использовал акростихи в своей знаменитой Энеиде[5]. Не редко читаемый по первым буквам акростиха текст в концентрированном виде выражал смысл всего, либо части поэтического произведения.

В российской поэтике акростихи-посвящения получают употребление, по-видимому, с XVIII века. Текст, читаемый в таких стихах по первым буквам стихотворных строк, обычно заключал в себе имя его адресата. При этом адресат может быть указан и в самом тексте либо в эпиграфе стихотворения.

Иногда других указаний не было и тогда акростих-посвящение становился в полном смысле стеганографическим сообщением. Вот пример такого посвящения первого профессионального русского литератора Александра Петровича Сумарокова (1717 – 1777) «Изъ 110 псалма. Исповемся тебе Господи всемъ сердцемъ моимъ»:

[2] «Поэ́тика» (335 до н. э.) – трактат Аристотеля. Согласно античным каталогам, состоял из двух частей, из которых до нас дошла лишь первая. Вторая часть предположительно была посвящена разбору комедии и лично Эпихарму.

[3] Аполлодор Афинский. URL: https://ru.wikipedia.org/wiki/Аполлодор_Афинский (Дата обращения: 01.10.2025)

[4] Аратус. URL: https://en.wikipedia.org/wiki/Aratus. (Дата обращения: 01.10.2025)

[5] Acrostic. URL: https://en.wikipedia.org/wiki/Acrostic (Дата обращения: 01.10.2025)

«Есть ли Божій страхъ въ сердцѣ обитаетъ,
Къ вышнему умомъ кто всегда взлетаетъ,
Адаманта сей чище много разъ,
Твердь какъ камень той въ честности всякъ часъ.
Ежели не зримъ Божья мы величья,
Разна чудеси многова отличья,
И порядка въ нихъ пышна естества;
Не узримъ во вѣкъ мы и божества.
Ахъ! когда бъ ево мы не забывали,
Въ добродѣтели бъ тверды пребывали:
Ей въ насъ мѣсто есть, только корень слабъ:
Лютости страстей рѣдкой въ насъ не рабъ.
Истинна одна насъ путемъ да водитъ!
Къ трону въ небеси ложь и не подходитъ.
Ангели Царя держатъ тамо тронъ:
Я погибъ, когда мной погибъ законъ[6].
1774 год»

Адресатом приведенного акростиха является Екатерина Великая.

В форме акростихов составлялись и загадки, в которых, отгадка заключалась в первых буквах стихотворных строк.

Русский поэт, публицист и лингвист Константин Сергеевич Аксаков (1817 –1860) посвятил акростих своему любимому городу:

«Мои мечты и силы молодые
Одной тебе я отдал, посвятя;
Судьбой своей чудесной в дни былые
Как сильно ты тревожила дитя!
Всю жизнь свою останусь я с тобою,
А ты сияй бессмертной красотою.
Около 1840»[7]

Из приведенного выше акростиха следует, что любимым городом Аксакова была Москва.

Следует отметить, что один из авторов данной статьи имеет и личный опыт создания акростихов [3].

ЛИНГВИСТИКА КОРАНА

К VIII веку, за первую сотню лет своего существования, Арабский халифат стал крупнейшим и развитым государством своего времени. Пока Европа забывала античные знания, арабский мир становился научным авангардом. Здесь развивалась математика, астрономия, медицина и даже криптография. Практическое использование получило искусство шифрования, называемое «Ильм-ат-таамия» — «наука сокрытия».

Шифрование применялось как для военных целей, так и в повседневной бюрократии. Например, в трактате «Адаб аль-Куттаб» («Руководство для секретарей») имелся целый раздел, посвящённый методам криптографической защиты налоговых записей.

Принято считать, что начиная с 830 года ведущую роль в научной и культурной жизни арабского халифата играл Дом мудрости, являвшийся главным интеллектуальным центром эпохи при дворе халифа в Багдаде. Руководил в те поры Домом мудрости фаворит халифа, выдающийся ученый и философ арабского мира – Аль-Кинди[8].

Большое значение в рассматриваемый период начали приобретать лингвистические исследования, связанные со священной книгой мусульман – Кораном. Теологи Дома мудрости проводили скрупулезный лингвистический анализ текстов Корана. Значительное внимание уделялось использованию рифмованной и ритмизованной прозы, характерной для ряда сур (глав) Корана.

Отдельное направление составляли исследования, связанные с анализом появления слов в различных сурах и аятах[9] («стихах») путём подсчёта частот встречаемости отдельных слов в каждом откровении. Таким образом, можно считать, что этими эмпирическими исследованиями был заложен фундамент лингвистической статистики. Однако, до установления строгой количественной закономерности распределения частотности слов естественных языков пришлось ждать ещё более тысячи лет, пока в 1949 году американским лингвистом Джорджем Ципфом не был установлен соответствующий закон, получивший название «Закон Ципфа»[10].

Приведенные примеры лингвистических трудов арабских филологов дают представление о состоянии лингвистической науки рассматриваемого периода. Лингвисты Дома мудрости, не останавливаясь на словарном частотном анализе текста Корана, продолжили его и на уровне отдельных букв этого текста.

СОЧИНЕНИЕ АЛЬ-КИНДИ «ТРАКТАТ О ДЕШИФРОВАНИИ КРИПТОГРАФИЧЕСКИХ СООБЩЕНИЙ»

Неизвестно, кто первый изобрёл частотный криптоанализ, но первое известное описание этого метода, приведенное в «Трактате о дешифро-

[6] Сумароков Александр. URL: https://sumarokov.lit-info.ru (Дата обращения: 01.10.2025)

[7] К. Аксаков. Акростих. URL: https://www.culture.ru/poems/31433/akrostikh?ysclid=mggjy5pxn0553672022 (Дата обращения: 01.10.2025)

[8] Абу Ю́суф Яку́б ибн Исха́к аль-Ки́нди (801—873) был автором более чем 250 книг по медицине, астрономии, математике, лингвистике и криптографии. Среди творений, приписываемых перу аль-Кинди, был и «Трактат о дешифровании криптографических сообщений».

[9] Аят. URL: https://ru.wikipedia.org/wiki/Аят (Дата обращения: 01.10.2025)

[10] Закон_Ципфа. URL: https://ru.wikipedia.org/wiki/Закон_Ципфа (Дата обращения: 01.10.2025)

вании криптографических сообщений» принадлежит выдающемуся арабскому философу и учёному Аль-Кинди, который в годы правления халифа аль-Мутаваккиля (847–861) подвергался гонениям, унижениям и даже избиениям. Большое количество его книг и сочинений было утрачено, в том числе и подлинник его «Трактата о дешифровании криптографических сообщений».

Список этого самого знаменитого трактата аль-Ки́нди был обретен заново лишь в 1987 году в оттоманском архиве Сулайманийа в Стамбуле [4]. В нем наряду с проблемами криптографии содержится подробный анализ статистики, фонетики и синтаксиса арабского языка. Описанная в трактате революционная система криптоанализа аль-Кинди может быть кратко сформулирована следующим образом.

«Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, — это взять другой незашифрованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву «первой», букву, которая по частоте появления стоит на втором месте, назовем «второй», букву, которая по частоте появления стоит на третьем месте, назовем «третьей» и так далее, пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдем наиболее часто встречающийся символ и заменим его «первой» буквой незашифрованного текста, второй по частоте появления символ заменим «второй» буквой, третий по частоте появления символ заменим «третьей» буквой и так далее, пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать» [4,с.22].

Однако не следует безоговорочно применять правила аль-Кинди для криптоанализа, поскольку частоты появления букв конкретного текста являются только усредненными значениями. Они не будут в точности совпадать с частотами появления этих же букв в любом другом тексте. К примеру, краткое сообщение, в котором обсуждается дифференцирование функций (и очень часто встречается буква «ф») не поддалось бы непосредственному применению частотного анализа аль-Кинди.

Частота появления букв в коротком, да еще и специфичном тексте, может значительно отклоняться от «стандартной», и если в сообщении меньше ста букв, то его дешифрование окажется весьма затруднительным. В то же время в более длинных (репрезентативных) текстах частоты появления букв в большинстве случаев (в соответствии с «законом больших чисел») будут приближаться к «стандартным» значениям.

КНИГА ТАЙНОГО ЯЗЫКА

К сожалению, не только криптографический трактат аль-Кинди, но и другие достижения арабской криптографической науки и практики должным образом сохранены не были. В косвенных свидетельствах встречаются сведения о «Китаб аль-Маумма» («Книга тайного языка») – трактате, написанном в VIII веке первым широко известным арабским филологом Абу аль-Ахмади Халилем ибн Ахмадом аль-Фарахиди[11] (717–786) на основе его уникальных криптографических методов. Хотя оригинал книги не сохранился и о «Китаб аль-Маумма» известно только по упоминаниям в работах других учёных, считается, что автор трактата первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования шифрованных сообщений.

В частности, этот метод заключается в том, что если криптоаналитик правильно предположил слово в одном из двух одноключевых (одномаркантных) текстах, то он может «протянуть» этот фрагмент открытого текста слева и справа от угаданного слова. Правильность догадки тут же подтверждается читаемостью второго (из двух одномаркантных) текста.

В отечественном криптоанализе этот метод называется «протяжкой вероятного слова» и основывается на частотных закономерностях «разностей» открытых текстов. В описании этого метода аль-Фарахиди будто бы сообщал, что для дешифрования криптограмм, посланных ему византийским императором, по исламской традиции первыми словами должны быть: «Во имя Аллаха». Это предположение оказалось истинным, что и позволило ему прочитать оставшиеся части зашифрованных посланий [5]. Повторно метод поиска одномаркантных сообщений, носящий название «метода Фридмана[12]» был установлен лишь в 1920 году[13].

[11] Китаб аль-Маумма. URL: https://ru.wikipedia.org/wiki/Книга_тайного_языка. (Дата обращения: 01.10.2025)

[12] Фридман Уильям Фредерик. URL: https://ru.wikipedia.org/wiki/Фридман,_Уильям_Фредерик. (Дата обращения: 01.10.2025)

[13] Индекс_совпадений. URL: https://ru.wikipedia.org/wiki/Индекс_совпадений (Дата обращения: 01.10.2025)

КРИПТОЛОГИЯ АЛЬБЕРТИ

В 1466 году Леон Баттиста Альберти[14] написал удивительную книгу (на тот момент без фиксированного названия), сохранившуюся в пятнадцати латинских рукописных вариантах. Сегодня её общепринятое название – «De Componendis Cyfris» («Трактат о шифрах») [8]. Интересно, что этот потрясающий по глубине проникновения в криптографию и лингвистику трактат за почти пятивековую историю существования остался без внимания как научной, так и культурной европейской общественности.

Текст этого сочинения оставался неизвестным исследователям шифров вплоть до двадцатого века и вообще сохранился, наверное, только из уважения к имени его автора. Содержание же самого De Componendis Cyfris вне узкого круга специалистов криптографов было недоступно на протяжении сотен лет, так как те, по-видимому, не могли представить, что гений криптологии и гений раннего возрождения могут сочетаться в одном человеке.

Когда же специалисты наконец обратили внимание на содержание этого произведения, их прежде всего заинтересовал так называемый диск Альберти – полиалфавитный шифр замены. При этом практически были упущены из виду первая часть трактата (связанная с криптоанализом и свойствами, и закономерностями языка открытого текста), последняя часть трактата (связанная с использованием номенклатора с перешифровкой) и сверх того – случайные моменты переходов от одного шифровального диска к другому.

Обстоятельства, сподвигшие Альберти к написанию этого трактата, приводятся им на первой странице его сочинения [8]. Его старый приятель Дата Леонардо, апостольский секретарь Папы Павла II, предложил ему изучить вопросы криптологии, а именно, что могло бы быть полезным для лучшей защиты зашифрованной папской переписки, и разработать методы взлома шифров папских недоброжелателей.

Не прошло и года, как Альберти вник в самую суть криптографических проблем, проанализировал недостатки существовавших в его время шифров замены и выявил наиболее важные криптографические уязвимости, до которых последующие криптографы в лице Клода Шеннона дошли только к середине двадцатого века [9].

Изучавшие криптографический трактат Альберти указывали на то, что, начав с частотных характеристик открытых латинских текстовых сообщений, в дальнейшем Леон Баттиста предложил некоторые упрощения латинской орфографии и использование в шифртексте «пустышек» — ничего не обозначающих символов. Его криптографические исследования были направлены на такие лингвистические объекты, как повторяемость букв, пар букв, чередование гласных и согласных. На этом этапе, зная практические частоты встречаемости букв в открытых текстах, можно было бы осуществить идентификацию замененных символов.

В связи с этим особого упоминания заслуживает метод частотного анализа аль-Кинди (IX век), формулировки которого во многом повторяются у Альберти. Тем не менее, трактат аль-Кинди после его утраты в IX веке был повторно обнаружен в оттоманском архиве в Стамбуле лишь в 1987 году [4] и, по-видимому, не мог быть доступен исследователям в XV веке. Поэтому о заимствовании метода частотного анализа говорить не приходится.

Анализируя закономерности открытого текста, которые могли бы послужить отправным моментом для взлома любого шифра замены, Альберти приходит к выводу об усложняющей роли омофонов, то есть, использования более одного символа для шифрования одной буквы открытого текста. При этом Альберти делает гениальное заключение о том, что и омофоны не помогут при использовании их по фиксированным правилам (так как это в конце концов и случилось с шифром Виженера).

На основе вышесказанного Леон Баттиста описывает свой метод – «Шифр Альберти», как полиалфавитную замену со случайными моментами переходов от одного алфавита замены к тайно выбираемому другому алфавиту, да и обеспечивающего еще удобный способ кодирования с перешифровкой. Для практической реализации этого метода Альберти предлагал использовать разработанное им специальное устройство – диск Альберти.

Внимательное прочтение тракта о шифрах еще раз убеждает в том, что его автор был криптографическим гением не только своего времени, но и на многие сотни лет вперед. В частности, открытие Леоном Баттистой Альберти нового класса шифров – шифров полиалфавитной замены со случайными переходами между алфавитами – могло иметь важнейшее значение для совершенствования криптографических методов. Однако, ни его современни-

[14] Леон Баттиста Альберти (1404–1472) – философ, писатель, поэт, лингвист, основоположник современного итальянского языка, архитектор, скульптор, художник, медальер, математик, криптограф [6, 7] – одним из первых выступил за использование итальянского (не только латинского) языка в литературном творчестве. Его элегии и эклоги — первые образцы этих жанров на итальянском языке. Некоторые другие работы Альберти: «Четыре книги о семье», «Десять книг о зодчестве», «Три книги о живописи», собрание басен и аллегорий «Застольные беседы». По архитектурным проектам Альберти были построены великолепные сооружения, определившие основное направление в итальянской архитектуре пятнадцатого века.

ки, ни последующие криптографы вплоть до XX века не смогли до конца ни понять, ни оценить его идей.

ЗАКЛЮЧЕНИЕ

Криптография и лингвистика тесно связаны как в научном, так и в прикладном смысле. Эти многовековые связи послужили их взаимному обогащению и развитию.

Открытые в V веке до н. э. стеганографические свойства акростиха, базирующиеся на дополнительной избыточности поэтической речи, были оформлены в теоретико-лингвистическом виде только Андреем Николаевичем Колмогоровым в шестидесятые годы XX века.

Введенное им понятие «остаточной энтропии поэтических текстов», по идее Колмогорова, характеризует «гибкость» языка стихотворения, позволяя его создателю выбирать между различными стилистическими, грамматическими и фонетическими односмысловыми текстовыми вариантами.

Изучению лингво-статистических закономерностей текстов арабскими лингвистами VIII - IX веков криптология обязана зарождением частотного криптоанализа. Это открытие на многие годы изменило представление о криптографической стойкости и дало мощный стимул к совершенствованию классических шифров.

Наконец идеи лингвиста, филолога, гения раннего возрождения Леона Батисты Альберти явились отправной точкой к созданию абсолютно стойкого шифра полиалфавитной замены со случайными переходами между алфавитами. Однако, ни его современники, ни последующие криптографы вплоть до XX века не смогли до конца ни понять, ни оценить его идей, приведших в конце концов к теореме Клода Шеннона о теоретической стойкости шифра. Эта теорема, бесспорно, имеет крайне важное значение для криптографии. Шеннон ввёл понятие абсолютно стойкого шифра и доказал свою теорему спустя более четырех с половиной столетий после написания трактата Леона Батисты Альберти «De Componendis Cyfris».

СПИСОК ЛИТЕРАТУРЫ

1. Аграновский А.В., Балакин А.В. [и др.] Стеганография, цифровые водяные знаки и стеганоанализ. Москва: Вузовская книга, 2009. 220 с.
2. Досократики. Доэлеатовский и элеатовский периоды. Пер. с древнегреческого А. Маковельского. Серия: Классическая философская мысль. Минск: Харвест, 1999. 784 с.
3. Гончаренко Е.С. Спасибо за надежду... Стихи. Москва: Русь, 1999. 36 с.
4. Кириллов И.А. Криптографическая защита информации. – М.: ИПК МГЛУ Рема, 2010. 100 с.
5. Шанкин Г. Тысяча и одна ночь криптографии. URL: http://cccp.narod.ru/work/book/kgb/shankin_01.html (Дата обращения: 18.11.2025)
6. Альберти Леон Баттиста. URL: https://ru.ruwiki.ru/wiki/Альберти,_ Леон_Баттиста (Дата обращения: 18.11.2025)
7. Леон Баттиста Альберти (1404–1472). https://artchive.ru/artists/ 87114~Leon_Battista_Al'berti. (Дата обращения: 18.11.2025)
8. Kim Williams, Lionel March, Stephen R. Wassell. Leon Battista Alberti, De Componendis Cyfris. In book: The Mathematical Works of Leon Battista Alberti. P.169-200. DOI:10.1007/978-3-0346-0474-1_4
9. Богданова А. В., Кириллов И. А. Криптология Леона Баттисты Альберти, гения раннего возрождения // Журнал высоких гуманитарных технологий. 2025. № 1 (8). С. 6-23.

УДК: 004.8

Использование искусственного интеллекта в правоохранительных органах КНР: опыт внедрения и перспективы

E.A. Vorobeva, A.A. Vorobeva, S.Y. Melnikov

AI in Law Enforcement in the PRC: Implementation, Experience and Prospects

Abstract. *The People's Republic of China is currently transitioning from the experimental implementation of artificial intelligence (AI) technologies in law enforcement to their systematic scaling. This process is accompanied by emerging institutional challenges related to algorithmic transparency, evidentiary verification, and the distribution of responsibility among participants. This paper outlines the key areas of AI application in Chinese law enforcement, based on official documents and practices from 2026, as well as the technological and legal risks that arise from the large-scale deployment of such systems. It analyzes data on actual technology adoption during the first half of 2026, including specialized large language models (LegalOne-R1) and autonomous robotic systems. The study identifies critical risks such as algorithmic bias, the "black box" problem in legal decision-making, information redundancy, and the need to institutionalize new expert competencies. Particular attention is devoted to analyzing the risks of integrating AI into the law enforcement activities based on the most recent Chinese sources, which have not previously been introduced into academic discourse in the Russian-language literature.*

Keywords: *artificial intelligence, law enforcement agencies, large language models, algorithmic bias, explainable artificial intelligence, robotic systems, evidence verification.*

Е.А. Воробьева[1]
А.А. Воробьева[2]
С.Ю. Мельников[3]
[1]Студентка, Московский государственный лингвистический университет,
E-mail: evgeniavorobeva.chinese@mail.ru
[2]Студентка, Московский государственный лингвистический университет.
E-mail: china_aleksandravorobeva@mail.ru
[3]Доктор физико-математических наук, профессор кафедры теории вероятностей и кибербезопасности института компьютерных наук и телекоммуникаций факультета физико-математических и естественных наук Российского университета дружбы народов имени Патриса Лумумбы.
ORCID : 0000-0002-9023-9896.
E-mail: melnikov-syu@rudn.ru

Аннотация. *В настоящее время Китайская Народная Республика переходит от экспериментального внедрения технологий искусственного интеллекта (ИИ) в правоохранительную сферу к их системному масштабированию, что сопровождается формированием новых институциональных вызовов, связанных с прозрачностью алгоритмов, верификацией доказательств и распределением ответственности участников. В статье указаны направления применения ИИ в правоохранительных органах КНР на основе официальных документов и практик 2026 года, а также технологические и правовые риски, возникающие при масштабировании таких систем. Анализируются данные о реальном внедрении технологий в первом полугодии 2026 года, в том числе специализированных больших языковых моделей (LegalOne-R1) и автономных роботизированных комплексов. Указаны ключевые риски, такие как алгоритмическая предвзятость, проблема „черного ящика" в правоприменении, информационная избыточность и необходимость институционализации новых экспертных компетенций. Особое внимание уделено анализу рисков внедрения ИИ в правоохранительную деятельность на основе самых свежих китайских источников, ранее не вводившихся в научный оборот в русскоязычной литературе.*

Ключевые слова: *искусственный интеллект, правоохранительная деятельность, большие языковые модели, алгоритмическая предвзятость, объяснимый искусственный интеллект, робототехнические комплексы, верификация доказательств.*

ВВЕДЕНИЕ

С момента принятия в 2017 году государственного «Плана развития искусственного интеллекта нового поколения» правоохранительная сфера Китая рассматривается как одна из приоритетных для внедрения технологий ИИ наряду с такими отраслями, как умное производство, интеллектуальная логистика, финансовый сектор и сфера общественной безопасности.

В соответствии с национальным стандартом КНР GB/T 41867–2022, искусственный интеллект определяется как «совокупность технологий и систем, которые путём имитации, расширения и дополнения человеческого интеллекта обеспечивают восприятие, познание, принятие решений и их реализацию» [1]. Высокий приоритет развития ИИ подтверждается ростом государственного финансирования. В 2025 году расходы на науку в КНР составили 398 млрд юаней [2], а в 2026 году – уже 426 млрд юаней [3]. В апреле 2025 года запущен наци-

ональный фонд развития ИИ (60 млрд юаней) [4]. К 2026 году в области общественной безопасности, прокуратуры и судов Китай завершил этап пилотных проектов и перешел к системному масштабированию ИИ-решений.

Вместе с тем, по мере того как системы ИИ всё активнее внедряются в правоохранительную деятельность, на первый план выходят новые проблемы [5]. Среди них — проблема верификации корректности работы таких систем, вопрос о том, кто несёт ответственность в случае ошибки (сотрудник, разработчик или владелец), а также риск закрепления и воспроизведения существующих диспропорций через данные, используемые для обучения.

СОВРЕМЕННЫЕ НОРМАТИВНО-ПРАВОВЫЕ АКТЫ

В феврале 2026 года Верховный суд провинции Гуандун принял документ «Мнения о содействии технологическим инновациям и развитию индустрии искусственного интеллекта посредством качественного рассмотрения дел об интеллектуальной собственности» [6]. Этот документ стал первым в Китае комплексным актом на уровне провинции, регулирующим правовые аспекты использования ИИ. Он охватывает такие вопросы, как защита данных, правовой режим сгенерированного контента и условия функционирования открытых экосистем.

С точки зрения правоохранительной деятельности, создание предсказуемой правовой среды является необходимым условием для масштабирования ИИ-решений. Судебные споры об ИИ приводят к появлению прецедентов, которые определяют, можно ли использовать результаты машинных вычислений в качестве доказательств в уголовном процессе.

На уровне исполнительной власти отметим «План работы органов общественной безопасности на 2026 год», опубликованный Управлением общественной безопасности города Шэньчжэнь [7]. В КНР органы общественной безопасности — это полицейская структура, подчиняющаяся Министерству общественной безопасности и выполняющая функции охраны правопорядка, расследования преступлений, управления дорожным движением, отвечающая за паспортно-визовую систему и регистрацию населения.

В указанном плане прямо говорится: «Углубленно продвигать проект повышения боеспособности новых видов вооруженных сил органов общественной безопасности. Усилить концентрированное строительство информационных систем и создание системы защиты данных, ускорить создание интеллектуальной платформы больших данных органов общественной безопасности, глубоко развернуть инновационное применение "Искусственный интеллект+", повысить уровень применения беспилотников и интеллектуального видеонаблюдения, углубить практическое применение новых технологий и оборудования, таких как роботы и AI-очки».

«Искусственный интеллект+» (AI+) – это государственная стратегическая инициатива КНР, закреплённая в докладе о работе правительства в 2024 году, направленной на повсеместную интеграцию технологий ИИ во всех отраслях экономики и сферах общественной жизни, включая правоохранительную деятельность.

В августе 2025 года Госсовет КНР принял развёрнутые руководящие указания по реализации AI+, определив трёхэтапный план: к 2027 году — достичь широкого внедрения ИИ в шести ключевых секторах, к 2030 году — обеспечить охват более 90% сфер деятельности, к 2035 году — полностью сформировать интеллектуальную экономику и общество [8]. Можно отметить, что упоминание AI+ в полицейском плане Шэньчжэня является прямым следствием государственной стратегии.

Таким образом, в 2026 году в повседневную работу полиции Шэньчжэня (одного из крупнейших городов Китая с населением 17 млн человек) уже внедряются технологии ИИ. Важно, что акцент здесь делается не на абстрактные концепции, а на конкретный перечень устройств и систем, которые предстоит внедрить.

СПЕЦИАЛИЗИРОВАННЫЕ ЯЗЫКОВЫЕ МОДЕЛИ

В январе 2026 года в Шанхае прошла Конференция по искусственному интеллекту в правосудии Китая — крупнейшее отраслевое мероприятие по применению ИИ в судебной и правоохранительной областях [9]. Ее организатором было Китайское общество искусственного интеллекта. В работе конференции участвовали представители Верховного народного суда КНР, а также ведущих университетов страны.

На конференции была представлена большая языковая модель LegalOne-R1, разработанная факультетом компьютерных наук Университета Цинхуа и Институтом интернет-правосудия Университета Цинхуа [10]. Модель выпущена в трёх версиях с разным числом параметров — 1,7 млрд (LegalOne-R1-1.7B), 4 млрд (LegalOne-R1-4B) и 8 млрд (LegalOne-R1-8B). Три версии нужны для выбора между производительностью и вычислительными затратами при

развёртывании этой модели в правоохранительных органах. Согласно докладу профессора Лю Ицюня, директора Института интернет-правосудия, модель прошла три этапа обучения: средний этап обучения — внедрение масштабных юридических знаний; этап инструктивной тонкой настройки — моделирование профессиональных рабочих процессов; этап обучения с подкреплением — формирование «юридического мышления» и создание сквозного цикла рассуждений для реальных задач [10].

Наибольшая из моделей, LegalOne-R1-8B, на публичных оценочных наборах LexEval, LawBench и JecQA продемонстрировала результаты, сопоставимые с моделями значительно большего объёма (DeepSeek-R1, GPT-5), а в задачах понимания правовых концепций, использования законодательных норм и многоэтапных рассуждений достигла лидирующих позиций среди моделей с открытым исходным кодом [10].

Модель LegalOne-R1 предназначена для выполнения юридических задач и ориентирована на анализ судебных решений и нормативных документов, подготовку проектов процессуальных документов, выявление правовых коллизий и поддержку принятия решений в правоприменительной практике.

Основные характеристики использованных оценочных наборов приведены в таблице 1.

Академик Чжан Бо, почетный директор Института искусственного интеллекта Университета Цинхуа, в докладе «Эпоха искусственного интеллекта и правосудие» отметил необходимость сочетания технической эффективности с этическими ограничениями и обратил внимание на проблему «черного ящика» в ИИ-системах, используемых в правоприменении [9]. Интерпретируемость решений ИИ является необходимым условием их использования в судебной практике.

Ректор Юго-Западного университета политологии и права Линь Вэй отметил, что развитие LegalOne-R1 и подобных моделей требует пересмотра подходов к юридическому образованию и подготовки кадров, способных работать в условиях «человеко-машинного взаимодействия». По его словам, ключ к решению этих проблем — именно в этом взаимодействии, причем право принятия решений должно оставаться за судьёй [9].

КЕЙСЫ ПРИМЕНЕНИЯ РОБОТИЗИРОВАННЫХ СИСТЕМ

Роботы-полицейские в Шэньчжэне

18 марта 2026 года на портале правоохранительных органов провинции Гуандун была опубликована официальная информация о начале использования роботов-полицейских в районе Баньтянь города Шэньчжэнь [11]. Можно выделить следующие основные характеристики роботов:

- интегрированность в систему управления дорожным движением и синхронизация с работой светофоров;
- оснащенность системами компьютерного зрения для распознавания нарушений (непристегнутые мотоциклисты, выезд за стоп-линию, неправильная парковка);

Таблица 1

Назначение и ключевые особенности оценочных наборов LexEval, LawBench и JecQA

Название	Разработчик	Основной фокус и задачи	Ключевая особенность
LexEval	Университет Цинхуа и др.	Комплексная оценка юридических когнитивных способностей: от запоминания норм до применения права.	Предлагает новую таксономию юридических когнитивных способностей LLM, включает проверку на этичность.
LawBench	OpenCompass и др.	Оценка знаний и способностей LLM на 20 разнообразных задачах (классификация, извлечение, генерация).	Структурирован по трём когнитивным уровням: запоминание, понимание и применение правовых знаний.
JecQA	Университет Цинхуа	Датасет типа «вопрос-ответ» на основе материалов национального юридического экзамена Китая.	Крупнейший QA-датасет в юриспруденции (~26 тыс. вопросов), требует многоэтапных рассуждений.

• способность в автоматическом режиме выдавать предупреждения нарушителям;

В планы развития входит расширение функционала для проверки водителей на состояние опьянения, фиксации дорожно-транспортных происшествий и автоматического сбора доказательств [10].

Внешний вид роботов-полицейских на улицах города представлен на рисунке 1.

Рис. 1. Робот-полицейский с функцией регулировщика (г. Шэньчжэнь)

В реальных условиях городской среды использование средств компьютерного зрения сталкивается с рядом трудностей. Точность систем распознавания лиц и объектов заметно зависит от условий освещения, погодных факторов и угла обзора, что приводит к ошибочной фиксации нарушений [12]. Однако механизмы выявления и обжалования таких ошибок гражданами в настоящее время отсутствуют.

Применение AI-роботов в Ханчжоу

22 марта 2026 года во время полумарафона на Западном озере в Ханчжоу впервые в Китае было организовано массовое применение AI-роботов для регулирования дорожного движения в условиях крупного публичного мероприятия (рисунок 2) [13]. На официальном сайте полиции Ханчжоу сообщается:

• роботы были развернуты на ключевых участках маршрута (мост Бэйшань, мост Чанцяо, перекресток Хуанлун);

• работа роботов координировалась с беспилотными летательными аппаратами;

• применялась технология «пузырькового пропуска»[1] пешеходов, позволяющая минимизировать задержки движения [13].

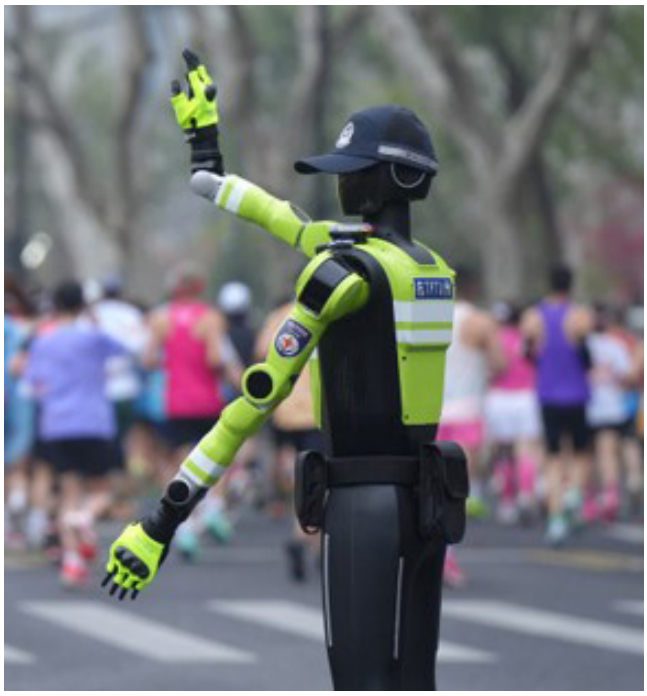

Рис. 2. Применение AI-робота во время полумарафона на Западном озере в Ханчжоу

Пример использования AI-роботов показывает, что ИИ может работать в меняющихся условиях (большое скопление людей, временные изменения маршрутов). Однако появляется вопрос: кто ответит за сбой или ошибочное решение системы, если это приведёт к негативным последствиям? Ответственность предстоит распределить между разработчиком ИИ, его оператором и полицейским, который осуществляет общий контроль. Этот вопрос, как отмечается в материалах конференции CJAI2026 (Китайская конференция по искусственному интеллекту в правосудии, Шанхай, 23–24 января 2026 г.) [4], не имеет на сегодняшний день нормативного разрешения [13].

22 января 2026 года в Ханчжоу было развернуто комплексное патрулирование с использованием человекоподобных роботов, роботов-собак и беспилотных патрульных машин [10]. Как сообщает газета «China Youth Daily», этот «полицейский отряд высоких технологий» осуществлял совместное па-

[1] «Пузырьковый пропуск» — это технология организации пешеходного движения во время массовых беговых мероприятий на временно перекрытых для транспорта маршрутах. В паузах между группами бегунов на трассе динамически открывается короткое „окно“ (обычно 5–7 секунд), через которое пешеходы пересекают дорогу компактной группой — „пузырьком“. Как только приближается следующая группа бегунов, переход закрывается. Такой подход позволяет жителям пересекать трассу, не дожидаясь полного окончания забега, и минимизирует неудобства граждан от перекрытия дорог.

трулирование и обеспечение безопасности в районе Биньцзян [14]. Этот пример показывает, что различные роботизированные системы постепенно интегрируются в единую экосистему интеллектуального правоприменения.

КЛЮЧЕВЫЕ РИСКИ И ПРОБЛЕМЫ ПРИМЕНЕНИЯ ИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Алгоритмическая предвзятость и перенос диспропорций

Модели, обученные на имеющихся данных о правонарушениях, в своих решениях могут воспроизводить сложившиеся региональные и социальные диспропорции. Если в прошлом в отдельных районах осуществлялся более плотный контроль, база данных содержит больше зафиксированных правонарушений в данных районах, что влечёт за собой ещё более интенсивный контроль. Это явление т.н. «алгоритмической предвзятости» изучалось в ряде работ, однако нормативные механизмы его ограничения в правоохранительной сфере пока не разработаны.

В контексте уголовного судопроизводства это может привести к тому, что системы ИИ, используемые для оценки рисков или рекомендации мер пресечения, будут систематически выдавать более строгие рекомендации для представителей определенных социальных или региональных групп, не имея для этого объективных оснований, но воспроизводя статистические корреляции, присутствовавшие в обучающих данных.

Проблема «черного ящика» и прозрачности алгоритмических решений

В научной литературе широко обсуждается проблема «чёрного ящика», которая заключается в невозможности для человека-оператора (например, судьи) понять, на основании каких именно признаков модель ИИ (собственно, она здесь и называется «черным ящиком») пришла к тому или иному выводу. Эта неспособность объяснить логику работы системы создаёт серьёзные препятствия для её использования в правосудии, так как подрывает принципы прозрачности и подотчётности судебных решений. При возникновении сомнений судья лишён возможности проверить логику ИИ. Следствием становятся два риска: необоснованное доверие к алгоритмам и отсутствие инструментов для их критической оценки.

В «Голубой книге по судебной информатизации» — ежегодном докладе «О развитии информатизации судов Китая», выпускаемом Институтом права Китайской академии общественных наук, подчёркивается: «с широким применением информационных технологий народным судам следует обратить внимание на необходимость и возможность включения открытости алгоритмов в судебную практику» [15]. Авторы доклада также указывают на необходимость «усиления контроля, проверки и надзора за алгоритмическими правилами, регулярной оценки справедливости и надежности алгоритмов, а также их масштабного влияния на судебную справедливость и социальное управление». Отметим, что «Голубая книга» отражает позицию ведущего академического института КНР в области права и влияет на формирование государственной политики в области цифровизации правосудия, фиксируя переход от технологического оптимизма к осознанию рисков алгоритмической непрозрачности.

В качестве одного из перспективных подходов к решению этой проблемы на конференции CJAI2026 отмечалась необходимость использования «объяснимого ИИ» в правоприменительной деятельности [9]. Основная идея заключается в том, что решения, принимаемые ИИ-системами, должны быть интерпретируемы для человека, что позволяет выявлять ошибки систем, обеспечивать возможность обжалования решений и проводить аудит корректности работы системы. Хотя само направление «объяснимого ИИ» развивается уже около десяти лет [16], именно в судебной области, как было отмечено на конференции, его применение приобретает особую значимость и перспективность.

Информационная избыточность и изменение характера нагрузки на сотрудников

Особенности использования ИИ-моделей в работе полиции изучались в [17] с использованием наблюдения и глубинных интервью с сотрудниками полицейских органов. Авторы приходят к выводу, что внедрение систем искусственного интеллекта в полицейские органы порождает эффект «информационного переизбытка»: модели генерируют значительные объёмы данных, требующих проверки и обработки. Внедрение моделей ИИ в деятельность полиции сопряжено с двойственным эффектом. С одной стороны, они расширяют профессиональные возможности сотрудников. С другой — замещают их рутинные знания и навыки, что создает риск профессиональной деградации. Кроме того, возникающий «информационный переизбыток» на практике

существенно перераспределяет рабочую нагрузку: значительную часть времени сотрудники тратят на проверку и обработку информации, генерируемой системами ИИ.

Данные эффекты не в полной мере учитывались при планировании внедрения технологий. Таким образом, информатизация полицейских органов с применением ИИ несёт не только позитивные изменения (повышение эффективности борьбы с преступлениями), но и непредвиденные сложные последствия, требующие дальнейшего осмысления и корректировки как технологических, так и организационных подходов.

Верификация доказательств, сформированных ИИ-системами

Вопрос о статусе и допустимости доказательств, полученных с использованием систем искусственного интеллекта, активно обсуждается в современной китайской юриспруденции. В реальной судебной практике всё чаще фигурируют такие виды доказательств, как доказательства на основе распознавания лиц, доказательства на основе интеллектуального анализа траекторий передвижения подозреваемых или транспортных средств, а также алгоритмические доказательства (результаты, полученные с помощью машинных вычислений и моделей ИИ) [18].

Исследователи обращают внимание на проблему верификации таких доказательств. Алгоритмы обработки данных, используемые в правоохранительных целях, часто являются либо коммерческой тайной разработчиков, либо сведениями ограниченного доступа. В результате сторона защиты лишена возможности оспорить корректность работы системы, что вступает в противоречие с принципом состязательности в судопроизводстве и правом на эффективную защиту.

В качестве возможных решений предлагается повышение прозрачности механизмов генерации доказательств, введение института экспертов-специалистов для оказания помощи суду и сторонам в оценке доказательств, полученных с помощью ИИ, а также проведение практической проверки систем на основе исторических данных.

МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ И ЛЕГИТИМНОСТИ ИИ-СИСТЕМ

Технические методы повышения надежности

К числу подходов к обеспечению надёжности ИИ-систем в правоохранительной сфере относятся:

• обучение на репрезентативных выборках — включение в обучающие данные примеров, отражающих разнообразие условий эксплуатации (различное освещение, погодные условия, углы обзора), что снижает вероятность ошибок в нестандартных ситуациях;

• верификация выходных данных — создание механизмов проверки результатов работы ИИ независимыми методами (например, перекрёстная проверка данными из разных источников);

• многоуровневая система контроля — комбинирование автоматической фиксации с последующей выборочной проверкой сотрудником, что позволяет сохранить человеческий контроль над критически важными решениями.

Формирование новых профессиональных компетенций

Внедрение ИИ в правоохранительную деятельность объективно требует появления специалистов, обладающих междисциплинарными знаниями на стыке права и информационных технологий. В их функции могут входить: анализ архитектуры ИИ-систем и принципов их работы; выявление и оценка рисков, связанных с использованием конкретных систем в правоприменительной практике; проведение аудита корректности работы ИИ; выполнение роли посредников между разработчиками алгоритмов и правоприменителями (следователями, судьями). В перспективе возможно введение соответствующих должностей в управлениях общественной безопасности и судах.

Стандартизация экспертизы систем на отраслевом уровне

В качестве перспективного направления развития предлагается введение института судебной технической экспертизы систем ИИ. Такая экспертиза должна проводиться независимыми специалистами и включать:

• проверку корректности работы на тестовых наборах данных;

• анализ обучающей выборки на предмет наличия систематических искажений;

• оценку устойчивости к изменениям входных данных;

• подготовку заключения о допустимости использования результатов работы системы в качестве доказательства.

В [18] отмечается, что сейчас соответствующие нормативные акты отсутствуют, однако накопление судебной практики создает предпосылки для их появления в ближайшие годы.

ЗАКЛЮЧЕНИЕ

К 2026 году Китай перешел от этапа экспериментального внедрения ИИ в правоохранительную сферу к системному масштабированию, что подтверждается принятием нормативных актов (документ Верховного суда провинции Гуандун, февраль 2026 г.), развитием специализированных технологических решений (LegalOne-R1, январь 2026 г.) и массовым внедрением роботизированных комплексов в городской среде (Шэньчжэнь, март 2026 г.; Ханчжоу, январь–март 2026 г.).

Параллельно с расширением применения ИИ формируется новая область институциональных вызовов. Основные риски: алгоритмическая предвзятость (перенос существующих диспропорций через обучающие данные), проблема «черного ящика» (невозможность проверки логики принятия решений), информационная избыточность (изменение структуры нагрузки на сотрудников), отсутствие механизмов верификации доказательств, сформированных ИИ-системами.

Перспективные направления: внедрение «объяснимого ИИ» в правоприменительную практику, разработка технических методов повышения надежности (обучение на репрезентативных выборках, верификация выходных данных, многоуровневый контроль), формирование новых профессиональных компетенций, связанных с обработкой данных и аудитом систем ИИ в правоохранительных органах, внедрение судебной технической экспертизы систем ИИ.

Опыт КНР может оказаться полезным для нашей страны. Он показывает не только возможности масштабирования ИИ-решений, но и необходимость комплексного подхода к их надёжности, прозрачности и легитимности. Китай одновременно формирует нормативную базу, разрабатывает модели и осмысливает риски. Этот подход можно учесть при разработке российской стратегии внедрения ИИ в правоохранительную сферу.

СПИСОК ЛИТЕРАТУРЫ[2]

1. Information Technology — Artificial Intelligence — Terminology. GB/T 41867–2022. 2022. URL: https://www.chinesestandard.net/PDF/English.aspx/GBT41867-2022 .(Дата обращения: 19.05.2026)

2. 中华人民共和国财政部. (2025). 2025年中央一般公共预算支出预算表. URL: http://yss.mof.gov.cn/2025zyczys/202503/t20250324_3960482.htm.(Дата обращения: 19.05.2026)

3. 中华人民共和国财政部. (2026). 2026年中央一般公共预算支出预算表. URL: http://yss.mof.gov.cn/2026zyczys/202603/t20260324_3986019.htm. (Дата обращения: 19.05.2026)

4. 吴少龙. (2025). 600亿国家人工智能基金将开展投资布局 围绕全产业链覆盖算力等各环节. 证券时报. URL: https://stcn.com/article/detail/1653447.html. (Дата обращения: 19.05.2026)

5. 中国犯罪学学会. 算法与正义：新十年的挑战 [C]. 中国犯罪学学会2025年年会论文集, 北京, 2025年3月. 312 с.

6. 广东省高级人民法院. 关于以高质量知识产权审判工作促进人工智能科技创新和产业发展的意见 [EB/OL]. 广州市增城区人民法院, 2026-02-14. URL: http://www.zcfy.gov.cn/sfgg/dt/2026/02/14104817359.html. (Дата обращения: 19.05.2026)

7. 深圳市公安局. 2026年公安工作计划 [EB/OL]. 深圳市公安局, 2026-02-11. URL: https://ga.sz.gov.cn/szsgajgkml/szsgajgkml/ghjh/fzgh/content/post_12644402.html. (Дата обращения: 19.05.2026)

8. http://www.gov.cn/zhengce/202508/content_60218473.htm. (Дата обращения: 19.05.2026)

9. 中国人工智能学会. 2026中国司法人工智能大会（CJAI2026）在沪举办 [EB/OL]. 中国人工智能学会, 2026-01-24. URL: https://www.caai.cn/site/content/5468.html. (Дата обращения: 19.05.2026)

10. 清华大学计算机科学与技术系. 清华大学Legal0ne-R1法律大模型正式发布 [EB/OL]. 清华大学计算机科学与技术系, 2026-01-29. URL: https://www.cs.tsinghua.edu.cn/info/1088/7036.htm. (Дата обращения: 19.05.2026)

[2] Список литературы составлен в авторской редакции.

11. 广东政法网. “机器人交警”，现身深圳街头 [EB/OL]. 广东政法网，2026-03-18. URL: https://www.gdzf.org.cn/xbsy/znzf/content/mpost_195079.html. (Дата обращения: 19.05.2026)

12. 警察技术. 2026年第01期 [J]. 中国知网，2026. URL: https://wap.cnki.net/touch/web/Journal/List/JCJS202601.html.

13. 杭州市公安局. 全国首次！西湖半马迎来“AI机器人交警”，还有无人机配合“气泡式”过街 [EB/OL]. 杭州市公安局, 2026-03-23. URL: https://police.hangzhou.gov.cn/col/col1228937564/art/2026/art_84e32468b81b4f9592cb31d5c987cae9.html. (Дата обращения: 19.05.2026)

14. 中国青年报. Hangzhou's "black technology police force": Robots, robotic dogs and unmanned patrol vehicles team up for security patrols [EB/OL]. 2026-01-28. URL: http://m.cyol.com/gb/articles/2026-01/28/content_dqRKoWt0Jd.html. (Дата обращения: 19.05.2026)

15. 最高人民法院. 中国法院信息化发展报告No. 9 (2025) [R]. 北京：人民法院出版社，2025. 187 c.

16. URL: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (Дата обращения: 19.05.2026)

17. 宋锴业，徐雅倩. 人工智能算法何以重构社会治理？——基于中国警务部门算法运作的实证研究 [J]. 社会学研究，2026(1).

18. 石魏，陈渝欣. 刑事诉讼中人工智能证据的不可解释性困境及其化解路径［N/OL］. 人民法院报，2025-12-08. URL: http://mdjtl.hljcourt.gov.cn/public/detail.php?id=7844. (Дата обращения: 19.05.2026)

О применениях искусственного интеллекта: от правоохранительной сферы к системе социального рейтинга. Мнение редакции

Предисловие

Развитие искусственного интеллекта в правоохранительной сфере стало одним из наиболее заметных направлений цифровой трансформации государственного управления. Алгоритмические системы сегодня, как мы видим в предыдущей статье, применяются для анализа больших массивов данных, распознавания лиц, выявления аномалий в поведении, прогнозирования рисков и повышения эффективности контроля за общественным порядком. В этой логике ИИ выступает не только как технический инструмент поддержки полиции или административных органов, но и как элемент более широкой модели управления, основанной на сборе, сопоставлении и интерпретации данных о действиях людей и организаций.

Именно на этом фоне становится понятным переход от обсуждения искусственного интеллекта в правоохранительной деятельности к анализу социального рейтинга. Если в правоохранительной сфере алгоритмы первоначально используются для выявления правонарушений, идентификации подозреваемых и оценки угроз, то в системе социального кредита аналогичная логика распространяется уже на гораздо более широкий круг социальных и экономических отношений. Речь идет о смещении акцента от реагирования на конкретное нарушение к постоянному мониторингу благонадежности, дисциплины и соблюдения установленных правил различными субъектами.

Китайский опыт особенно показателен в этом отношении, поскольку система социального кредита рассматривается многими исследователями как часть более общей модели управления, основанного на данных. В рамках такой модели сведения, первоначально значимые для правоприменения и надзора, начинают использоваться не только для расследования или санкционирования уже совершенных нарушений, но и для построения долговременных профилей доверия, которые влияют на административные решения, рыночные возможности и доступ к отдельным социальным благам.

При этом важно подчеркнуть, что переход от ИИ в правоохранительной сфере к социальному рейтингу не означает простого расширения полицейских функций. Скорее речь идет о качественном изменении самой управленческой логики: контроль становится менее эпизодическим и более встроенным в повседневные экономические, административные и социальные практики. В этом смысле социальный рейтинг можно рассматривать как одну из форм алгоритмического управления, в которой инструменты наблюдения, анализа и прогнозирования соединяются с механизмами поощрения и ограничения.

В связи с этим обращение к теме социального рейтинга в Китае является закономерным продолжением разговора о применении искусственного интеллекта в сфере правопорядка. Оно позволяет увидеть, как цифровые технологии, изначально внедряемые ради обеспечения безопасности и повышения эффективности правоохранительной деятельности, могут становиться частью более масштабной инфраструктуры социального регулирования. Именно этот переход — от точечного использования ИИ для борьбы с правонарушениями к системной оценке надежности и управляемости поведения — и составляет предмет дальнейшего рассмотрения.

Под «социальным рейтингом» в Китае обычно понимают не единый универсальный балл для каждого гражданина, а более широкую систему социального кредита: совокупность государственных реестров, черных и красных списков, а также механизмов поощрения и ограничений за «добросовестное» и «недобросовестное» поведение. [1]

Общая характеристика системы

Система социального кредита формировалась как государственный механизм повышения «доверия» в экономике, государственном управлении и общественной жизни. [2] В реальной практике ее ядро составляют межведомственный обмен данными, учет соблюдения нормативных требований, а также применение последствий через черные и красные списки.

Важной особенностью китайской модели является ее фрагментированный характер. Корректнее говорить не о едином рейтинге, а о совокупности взаимосвязанных режимов учета благонадежно-

сти: существуют судебные списки, корпоративные кредитные досье, отраслевые системы надзора и местные пилотные проекты для граждан.

Основные направления применения

Применение системы можно разделить на несколько направлений.

Во-первых, это исполнение судебных решений. Один из наиболее известных механизмов касается лиц, которые не исполняют вступившие в силу судебные решения. Для таких лиц могут устанавливаться ограничения, включая меры против так называемого «высокого потребления».

Во-вторых, система активно используется в государственном регулировании бизнеса. Компании получают кредитные файлы, в которых отражаются сведения о налоговой дисциплине, лицензиях, административных штрафах, экологических нарушениях и иных аспектах комплаенса. Эти данные используются для надзора, допуска к государственным закупкам, субсидиям и другим мерам поддержки. [3]

В-третьих, социально-кредитные механизмы применяются в отраслевом надзоре. Отдельные черные и красные списки существуют в таких сферах, как продовольственная безопасность, экология, рынок услуг и иные регулируемые области.

В-четвертых, в ряде городов действовали или продолжают действовать локальные пилотные программы для граждан. Однако данные источников показывают, что представление о единой общенациональной системе индивидуальных баллов для всех жителей Китая является сильным упрощением.

Механизм действия

Логика системы строится поэтапно. Государственные органы собирают сведения о соблюдении правил и о нарушениях из административных, судебных и иных официальных источников. Далее профильный регулятор может включить субъект в черный список при наличии установленных нарушений либо в красный список при наличии признаков добросовестности. После этого информация может использоваться другими ведомствами, которые применяют согласованные меры поощрения или ограничения.

В корпоративной сфере это означает, что одно существенное нарушение способно повлечь последствия и за пределами исходного правонарушения: например, усиление проверок, ограничение доступа к субсидиям, усложнение административных процедур и снижение шансов на участие в отдельных государственных программах.

В отношении граждан наиболее разработан судебно-исполнительный механизм, связанный с лицами, уклоняющимися от исполнения судебных решений.

Формы поощрения и ограничения

Для субъектов, включенных в красные списки, могут предусматриваться различные меры содействия: ускоренное рассмотрение административных процедур, снижение частоты проверок, более благоприятное отношение при доступе к финансированию или государственным программам.

Для субъектов, включенных в черные списки, характерны усиленный надзор, репутационные потери, ограничения в доступе к отдельным административным услугам и иные меры воздействия. В случае судебных должников ограничения могут затрагивать транспортные и потребительские возможности.

Таким образом, система выполняет не только карательную, но и дисциплинирующую функцию: она призвана побуждать к исполнению обязательств, устранению нарушений и восстановлению правового статуса.

Особенности применения к гражданам и компаниям

К гражданам система применяется прежде всего через судебные механизмы, а также через отдельные местные инициативы. Вопреки распространенному мифу, доступные аналитические материалы не подтверждают существование полностью унифицированного общенационального «балла поведения» для каждого гражданина.

К компаниям система применяется более институционализированно. Формируются корпоративные профили, данные собираются множеством органов, а последствия могут затрагивать лицензирование, кредитование, участие в государственных закупках, экологический надзор и другие аспекты хозяйственной деятельности. Это касается и иностранных компаний, работающих в Китае.

Проблемы и критика

Основные претензии к системе связаны с непрозрачностью отдельных критериев [4], рисками ошибок в данных, межведомственным переносом санкционных последствий и ограниченными возможностями эффективного обжалования.

Критики подчеркивают, что система усиливает административный контроль государства: нарушение, зафиксированное одним органом, может повлечь последствия в иных сферах. [5] Вместе с тем исследования показывают, что популярный образ

тотальной автоматической оценки каждого шага гражданина не вполне соответствует фактической архитектуре китайской модели.

Вывод

Социальный рейтинг в Китае представляет собой не единый универсальный счет для всех граждан, а сложную систему учета благонадежности, основанную на черных и красных списках, обмене данными между ведомствами и механизмах поощрения и ограничения. Наиболее развито его применение в судебном исполнении и в государственном регулировании компаний. Поэтому при анализе китайской модели важно отличать реальные институты правоприменения и надзора от медийных упрощений.

СПИСОК ЛИТЕРАТУРЫ

1. China Law Translate. The redlists are coming! The blacklists are coming! URL: https://www.chinalawtranslate.com/en/the-redlists-are-coming-the-blacklists-are-coming/ (Дата обращения: 9.06.2026)

2. U.S.-China Economic and Security Review Commission. China's Corporate Social Credit System. URL: https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf (Дата обращения: 9.06.2026)

3. CNBC. China social credit system will affect businesses, not just citizens. URL: https://www.cnbc.com/2019/09/04/china-plans-for-corporate-social-credit-system-eu-sinolytics-report.html (Дата обращения: 9.06.2026)

4. Nature Humanities and Social Sciences Communications. On the transparency of the credit reporting system in China. URL: https://www.nature.com/articles/s41599-023-02081-3 (Дата обращения: 9.06.2026)

5. Supreme People's Court provisions on judgment defaulters list. URL: https://www.chinalawtranslate.com/en/court-blacklist/ (Дата обращения: 9.06.2026)

УДК: 14, 612.82

Лемма Пошебякина и крах трансгуманизма

A.Yu. Shcherbakov

The Poshebyakin Lemma and the Collapse of Transhumanism

Abstract. *This article explores and interprets the so-called Poshebyakin Lemma — the idea that human consciousness is fundamentally finite and, consequently, that there is a limit to radically extending human life. The lemma's essence is related to modern concepts of transhumanism, brain neurophysiology, and the age-related dynamics of synaptic connections. Data on the number of neurons and synapses are summarized, and changes in synaptic density in the human brain over the course of life are analyzed. Several mathematical approximation models are presented, and it is concluded that, with linear extrapolation, the critical limit of degradation of the "human" structure of consciousness lies approximately in the range of 210–230 years. Consequently, the "Poshebyakin Limit" can be viewed not as a strict biological law, but as a philosophical and ontological hypothesis about the finiteness of human mentality and the limitations of any scenarios for technological immortality.*

Keywords: *Poshebyakin's lemma, finiteness of consciousness, neurophysiology of the brain, synaptic pruning, neuroplasticity.*

А.Ю. Щербаков
Доктор технических наук, профессор,
научный руководитель Центра передовых фундаментальных исследований АРКЦФА,
ведущий научный сотрудник
Государственного университета управления.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена изучению и интерпретации так называемой леммы Пошебякина — идеи о принципиальной конечности человеческого сознания и, следовательно, о существовании предела радикального продления жизни человека. Суть леммы соотносится с современными представлениями о трансгуманизме, нейрофизиологии мозга и возрастной динамике синаптических связей. Обобщаются данные о числе нейронов и синапсов, проводится анализ изменений синаптической плотности человеческого мозга на протяжении жизни. Представлены некоторые математические модели аппроксимации и сделан вывод о том, что при линейной экстраполяции критическая граница деградации «человеческой» структуры сознания располагается примерно в интервале 210–230 лет, следовательно, «предел Пошебякина» может рассматриваться не как строгий биологический закон, а как философско-онтологическая гипотеза о конечности человеческой ментальности и ограниченности любых сценариев технологического бессмертия.*

Ключевые слова: *лемма Пошебякина, финитность сознания, нейрофизиология мозга, синаптический прунинг, нейропластичность.*

ВМЕСТО ПРЕДИСЛОВИЯ

У социализма и капитализма в 1980-х годах XX века, когда автор этого текста еще только учился в ВУЗе, были вполне заметные расхождения во взглядах на мир. Например, социализм обещал и надеялся, что советские люди будут жить при коммунизме, но ни словом не обмолвился, что они будут жить при коммунизме вечно. Или социализм никогда не запускал космические аппараты к внешним планетам, понимая, в отличии от капитализма, замкнутость местного Домена и полную бесперспективность этого процесса.

Можно констатировать, что взгляды социализма были более реалистичны, несмотря на лозунг «Пока империализм в бессильной злобе делает компьютеры, мы воспитываем нового человека». Однако, если кто-то и вспомнит, что воспитанный новый человек не смог спасти свою страну в эпоху перестройки, заметим, что со страной не случилось по большому счету ничего плохого, например, в то время не произошло масштабного гражданского противостояния и массовых батальных сцен на территории бывшего Советского Союза, за что глубокая благодарность и низкий поклон тому самому «советскому человеку».

Следует заметить, что в воспитании «нового человека» немаловажную роль играла небезынтересная даже на сегодняшний день марксистко-ленинская философия с ее неизменными тремя законами диалектики, а также тремя источниками и тремя составными частями марксизма.

Слушая в своё время лекции по указанной философии, автор вдруг в потоке вербальных лекционных смыслов вычленил тезис, немного необычный для советской риторики: человеческое сознание финитно, то есть конечно во времени, поэтому партия и правительство не занимаются бессмысленным бессмертием и враждебные посылы трансгуманистов к вечной жизни по меньшей мере неконструктивны. Продлевать бесконечно человеческую жизнь не имеет смысла, поскольку, с точки зрения ментальной, вечное существо с некоторого момента времени не будет иметь ничего общего с человеком.

Трансгуманизм представляет собой философское и интеллектуальное движение, направленное на преодоление биологических ограничений человека с помощью науки и технологий. Основные его направления фокусируются на улучшении физических, когнитивных и социальных возможностей человека[1].

Идеи трансгуманизма уходят корнями в 1950–1970-е гг. Джулиан Хаксли ввёл этот термин в 1957 году, Роберт Эттингер развил идеи крионики в 1962-м году.

Одним из основоположников трансгуманизма был Ферейдун М. Эсфендиари (сменил своё имя на FM-2030, выражая надежду на то, что в 2030 году ему удастся отпраздновать свой сотый день рождения). С 1966 г. Эсфендиари активно продвигал идеи трансгуманизма, а в 1980-х – читал лекции в Университете Калифорнии в Лос-Анджелесе (UCLA), где и проходили первые официальные встречи трансгуманистов.

В 1980 году Наташа Вита-Мор (урождённая Нэнси Кларк) — американская трансгуманистка – представила экспериментальный фильм "Breaking Away" на площадке EZTV в Лос-Анджелесе, иллюстрирующий преодоление биологических ограничений, предвосхищая темы загрузки сознания и морфологической свободы.

В 1982–1983 гг. Наташа Вита-Мор написала "Трансгуманистический манифест", который позже был отправлен на борту космической миссии Cassini–Huygens к Сатурну. В 1993 году она основала течение «Transhumanist Arts and Culture», а в 2002–2006 – возглавила Институт экстропии. Известен её проект прототипа "Primo Posthuman" — концепция сверхчеловеческого тела с использованием биотехнологий, нанотехнологий и ИИ.

На перемене автор подошел к преподавательскому столу в надежде задать вопрос о численном значении того возраста, когда вечный человек превратится в непредсказуемое чудовище, и вдруг увидел в конспекте лектора заинтересовавшее его утверждение о финитности сознания с названием «Лемма д. Паши Бякина». И число «200». Он сразу понял, что это то самое критическое значение в годах.

Существенно позже ему довелось столкнуться в интернет-дискурсах с «Леммой Пошебякина», в которой он с удивлением и радостью узнал утверждение, так сильно поразившее его в годы юности.

В поисках Бякина и Пошебякина

Итак, автор занялся поисками советского ученого Павла Бякина, и первой его внимание привлекала Валентина Петровна Бякина (1936–2019 гг.) — российский ученый-историк медицины, доктор исторических наук, профессор Первого Санкт-Петербургского государственного медицинского университета им. И.П.Павлова (ПСПбГМУ). Валентина Петровна окончила исторический факультет Ленинградского государственного университета и с 1968-го г. работала в ПСПбГМУ (в то время – Первый Ленинградский медицинский институт).

Ее основные работы – по истории петербургской физиологической школы И.П.Павлова и его учеников, она также является автором работ об академике И.П.Павлове («Академик И. П. Павлов: штрихи к биографии») [1-2]. Кроме того, она многие годы была главным редактором научных изданий университета, соавтором публикаций по истории женского медицинского образования в России и охране здоровья в СССР (1940–1950-е гг.). Занималась она и геронтологией, что сконцентрировало внимание автора этой статьи на ее предках.

Валентина Петровна также оставила записки о своей семье – отце Петре, его брате-близнеце Павле («дяде Паше») и старшем брате Владимире. Она с теплотой писала и о своем деде – отце братьев Бякиных – Иване Митрофановиче Бякине, который направил своих детей на стезю науки и образования.

«Старший брат, дядя Володя был прирожденным педагогом и знатоком геометрии, вместе в дядей Пашей они все время спорили о математике и рисовали какие-то фигуры. К сожалению, меня

[1] **Ключевые направления трансгуманизма**

Экстропианство: подчеркивает вечный прогресс, самосовершенствование и отказ от ограничений, включая смерть, через технологии, например, нанотехнологий и ИИ.

Сингулярианство: ориентировано на технологическую сингулярность — момент, когда ИИ превзойдет человеческий интеллект, приведя к экспоненциальному развитию, в том числе даруя человеку вечную или продолжительную жизнь.

Либертарианский трансгуманизм: сочетает трансгуманистические идеи с либертарианством, акцентируя свободу индивида в использовании технологий без государственного вмешательства.

Демократический трансгуманизм: стремится к равному доступу к технологиям улучшения для всех, призывая избегать неравенства возможностей.

Религиозный трансгуманизм: интегрирует трансгуманизм с теологией, обозначая технологии как путь к божественному совершенству.

Движение против старения: фокусируется на биотехнологиях для продления жизни и борьбы со старением, включая генную инженерию и крионику.

Техногайянизм: объединяет экологию и технологии для гармоничного сосуществования человека с природой через чистые инновации.

Постгендеризм: использует биотехнологии для добровольного устранения гендерных различий.

больше влекли общественные науки и особенно история, в чем меня неизменно поддерживал мой отец» – отмечала Валентина Петровна.

Владимир Иванович Бякин работал учителем математики в средней школе. Его публикация 1955 г. — "Задачи на повторение курса планиметрии в IX классе" — вошла в сборник опыта преподавания именно в VIII–X классах средней школы (М.: Учпедгиз, 1955).

ЛЕММА И ЕЕ СОДЕРЖАНИЕ

Итак, напомним читателю, что лемма – вспомогательное утверждение, помогающее доказать или понять более глобальную математическую или мировоззренчески-философскую проблему.

Передадим смысл леммы по источнику [3]: Лемма Пошебякина в романе «Факап» Михаила Харитонова[2] — самый известный научный результат Карла Людвиговича Пошебякина.

Суть леммы Пошибякина излагается в главе романа с номером «120»:

В классическом виде лемма Пошибякина формулируется так: «Человеческое сознание является финитным процессом с конечным внутренним временем». Доказательство я видел: это пятьдесят страниц зубодробительных формул и такого же качества текста. Так что приходится доверять компьютерам, которые эту галиматью проверяли. А проверяли её очень тщательно.

Практические вычисления по принятой сейчас классической модели человеческого сознания Лефевра-Шихтмана показали, что для человека временной лимит — около двухсот лет максимум. Это по внутреннему времени...

Проблема-то на самом деле сложнее. Общественность понимает дело так, что после истечения конечного внутреннего времени сознание прекращается. Ну то есть умирает. И ничего с этим не поделаешь. Двести лет — точно каюк, а скорее раньше. И ничего с этим не поделаешь: доказано наукой. В науку общественность верит. Нужно же ей во что-то верить.

На самом деле всё не так однозначно. Процесс может продолжаться и после достижения лимита. Просто сознание перестаёт быть человеческим сознанием – или даже сознанием вообще. При этом «человеческое сознание» принимается в смысле модели Лефевра-Шихтмана. Если отойти от классической модели или вообще убрать условие «человечности», то ситуация выглядит не столь однозначной.[3]

Лемма доказывает, что человек не может жить дольше двухсот лет несмотря ни на какие биологические или технологические меры по продлению жизни. Это ограничение связано с самой сутью человеческого сознания, которое является ограниченным по времени процессом.

Таким образом, смысл леммы Пошебякина заключается в "обобщающем утверждении" о пределах человеческой жизни. Согласно этой лемме, как бы мы ни продлевали человеческую жизнь (биологически или технологически), человек в своем первозданном виде не сможет жить дольше примерно двухсот лет.

Иными словами, лемма обозначает предельный бытийный (онтологический) горизонт человеческого существования, понимаемый скорее как культурно-философская, чем как научно-биологическая граница.

Лемма смысловым образом окрепла в онлайн-дискуссиях о продлении жизни и технологическом бессмертии, вероятно, в 2020-х годах на платформах типа LiveJournal VK, Telegram или специализированных форумах (типа haritonov.wiki), где её и оформили в околонаучный стиль.

ОБОСНОВАНИЕ ЛЕММЫ

С точки зрения науки середины XX века лемма П.Бякина («Пошебякина») является своего рода озарением, поскольку она естественным образом опирается на сложность нейронной сети человеческого мозга и учитывает процессы ее возрастной деградации. Вопрос заключается в том, что количество нейронов в мозге и динамика формирования связей – это скорее результаты конца 20-го –

[2] Михаил Харитонов – псевдоним Константина Анатольевича Крылова. Крылов К.А. (1967-2020 гг.) — русский публицист, журналист, общественный деятель. Закончил факультет кибернетики МИФИ и философский факультет МГУ. С 2003 года — главный редактор газеты «Спецназ России». С 2005 года по 2007 — президент Русского общественного движения; после 2007 года — президент РОД-Россия. С осени 2006 года — член ЦК Конгресса русских общин. С 2007 года — главный редактор газеты «Русский марш». С сентября 2007 года — главный редактор Агентства политических новостей. Автор большого числа работ, в основном посвящённых вопросам социологии, политологии, философии и политической жизни. Рассказы М.Харитонова были рекомендованы издательству АСТ писателем Сергеем Лукьяненко, обнаружившим их в Интернете. В этот период времени авторство псевдонима было тщательно законспирировано, и о том, кто реально за ним скрывается, С.Лукьяненко сообщили в издательстве несколько позже, чем первый сборник был подписан в печать. Публично объявленный труд — совместный с Юрием Нестеренко роман в жанре альтернативной истории «Юбер аллес».

[3] Когда М.Харитонов говорит в тексте романа о модели Лефевра-Шихтмана, он, очевидно, имеет ввиду следующую монографию: Лефевр В. Космический субъект // Владимир Лефевр. Рефлексия. Составитель В. Е. Лепский. М.: Когито-Центр, 2003. С. 139–302.

начала 21-го века, и Павел Бякин о них мог только догадываться.

Опираясь на современные данные нейрофизиологии, попробуем проиллюстрировать содержание леммы, сделать оценку математического характера и обосновать «предел Пошебякина» – тех самых сакраментальных двухсот лет, которые максимально отводятся на жизнь человека.

Человеческий мозг содержит около 86 миллиардов нейронов, соединённых триллионами синапсов — специализированных структур для передачи сигналов между нервными клетками [4, 5]. Понимание количества и динамики синаптических связей критично для нейронауки, поскольку они лежат в основе когнитивных способностей, обучения и памяти [6].

Оценки числа синапсов в человеческом мозге варьируются от 10^{14} до 10^{15} [7, 8]. Для коры головного мозга стереологические исследования дают около $1.5x10^{14}$ синапсов, при средней плотности 7000 синаптических контактов на нейрон [8, 9].

Точное число зависит от методики подсчёта, возраста, области мозга и индивидуальных различий. Порядок величины является общепринятым в литературе [7, 8].

Изменения числа синапсов с возрастом

Количество синапсов изменяется на протяжении жизни нелинейно [10, 11] и отражено в таблице 1. Для более корректных подсчетов целесообразно оперировать не абсолютным количеством, а плотностью синапсов на кубический миллиметр.

Таблица 1

Изменение плотности синапсов в лобной коре (слой 3) по данным Huttenlocher (1979)

Возрастная группа	Плотность синапсов, на 10^8	Относительно взрослого
Новорождённые	~11	100%
1–2 года (пик)	~16,6	150%
2–16 лет (обрезка)	16,6 → 11,05	150% → 100%
16–72 года (стабильность)	11,05 ± 0,41	100%
74–90 лет (старение)	9,56 ± 0,28	~86%

В раннем детстве происходит быстрое увеличение числа синапсов (синаптогенез), достигая пика к 1–2 годам — примерно на 50% выше взрослого уровня [10, 11]. Затем следует период синаптической обрезки (pruning), продолжающийся до позднего подросткового возраста (~20–25 лет), особенно в префронтальной коре [12]. В пожилом возрасте (после 70 лет) наблюдается снижение количества синапсов на 10–30%, в зависимости от области мозга [13, 14].

Синаптическая обрезка — процесс элиминации (уничтожения) избыточных и слабых синапсов для оптимизации нейронных сетей [15, 16, 22, 23].

Этот процесс регулируется активностью нейронов и информацией извне, как описано ниже.

• **Зависимость от опыта:** активно используемые синапсы (с высокой частотой совпадающих импульсов) укрепляются и сохраняются, получая нейротрофины (нейротрофический фактор мозга, англ. brain-derived neurotrophic factor, BDNF). Слабые синапсы маркируются для удаления микроглией через систему комплемента (C1q, C3) [17-19].

• **Правило Хебба:** «взаимодействующие клетки объединяются» — корреляция активности определяет, какие связи сохранятся [20].

• **Последовательность созревания областей мозга:** первичные сенсорные зоны созревают раньше, чем ассоциативные области (префронтальная кора) [19, 21].

Плотность синапсов (число синапсов на единицу объёма, обычно мм³) напрямую определяет общее количество нейронных связей:

N = DxV,

где N — общее число синапсов, D — средняя плотность (~$1–2×10^9$ синапсов/мм³ в коре), V — объём коры (~600 000 мм³) [24, 25].

При $D=1,5x10^9$/мм³ и V ~600 см³ получаем $9x10^{14}$~ синапсов, что соответствует верхним оценкам.

Различия по областям мозга

Плотность синапсов и динамика созревания различаются по областям мозга [29, 30] и приведены в таблице 2.

Таблица 2

Гетерохрония созревания по данным Huttenlocher (1997)

Область мозга	Пик синаптогенеза	Завершение обрезки
Слуховая кора	~3 месяца	~12 лет
Средняя лобная извилина	>15 месяцев	Середина подросткового возраста

В старшем возрасте потеря синапсов также различается по областям: максимальна на нижней и медиальной стороне затылочной доли коры головного мозга (3,4–3,6% за декаду), меньше в префронтальной коре (1,8%), несмотря на значительную атрофию объёма последней [31, 32].

Плотность синапсов вполне коррелируется с психическими и неврологическими заболеваниями [33, 34] и отражена в таблице 3.

Таблица 3

Изменения синаптической плотности при патологиях

Патология	Изменение	Области и корреляция
Шизофрения	Снижение (10–20%)	Префронтальная кора, ACC; когнитивный дефицит.
Депрессия/ПТСР	Снижение	Дорсолатеральная префронтальная кора, гиппокамп.
Аутизм	Повышение	Сенсорные и ассоциативные области коры; социальные дефициты.
Болезнь Альцгеймера	Снижение (до 50%)	Гиппокамп, теменная доля; деменция.

Снижение плотности синапсов коррелирует с тяжестью симптомов и может быть визуализировано in vivo через PET-сканирование с радиолигандами SV2A (UCB-J)[4] [35, 36].

Посмотрим, как обстоят дела с синапсами для животных.

Количество синапсов сильно варьируется между видами [37, 38] и приведено в таблице 4.

Таблица 4

Нейроны и синапсы у различных животных

Животное	Нейроны (млн)	Синапсы (оценка)
Дрозофила	140–150	~50–55 млн
Мышь	71	10^{12}
Крыса	200	~4.5 x 10^{11}
Кошка	760	~10^{13}
Человек	86 000	10^{14}

Соотношение количества синапсов и нейронов (S/N) растёт от ~25 у червя C. elegans до 7000–10 000 у человека [39, 40]. У приматов S/N увеличивается с размером мозга за счёт снижения плотности нейронов при стабильной плотности синапсов [41].

Высокое соотношение S/N способствует когнитивным способностям, но интеллект определяется еще целым комплексом факторов [42, 43]:

- **Число кортикальных нейронов:** ~16 млрд у человека — ключевой предиктор интеллекта.
- **Морфология нейронов:** разветвлённые дендриты обеспечивают больше интеграции входящих импульсов; крупные пирамидальные нейроны коррелируют с IQ (r=0.46–0.51) [44, 45].
- **Скорость обработки:** миелинизация и диаметр аксонов определяют скорость проведения (до 100 м/с), коррелируя с IQ [43, 46, 47].
- **Синаптическая пластичность:** эффективность долговременной потенциации (LTP) и депрессии (LTD).
- **Генетика:** 50–80% наследуемости интеллекта (g-фактор) [48].

Нейроны и синапсы для техники

Ниже приведем биологические принципы, которые моделируются искусственными нейронными сетями (ANN) [49, 50].

- **Классические ANN:** перцептрон, в котором каждый искусственный нейрон вычисляет взвешенную сумму входных сигналов, где определенный набор коэффициентов — аналог синаптических весов [51].
- **Спайковые нейросети (SNN):** модели накопления и выброса (распространенный тип – «нейроны с утечкой», англ. Leaky Integrate-and-Fire, LIF). Включают пластичность (Spike-Timing-Dependent Plasticity, STDP) [52, 53].
- **Био-вдохновлённые техники:** разнородность синапсов, ремоделинг весов ускоряют обучение нейросети на 10–20% [51].

SNN энергоэффективны (0,3 спайка/нейрон) и используются в нейроморфных чипах. Полная симуляция мозга мыши (26 млрд. синапсов) выполняется на суперкомпьютерах [55].

[4] PET-сканирование (позитронно-эмиссионная томография) — метод диагностики, который позволяет оценить метаболическую активность тканей. Пациенту вводят радиоактивное вещество, которое накапливается в патологически изменённых тканях, например, в опухолевых клетках. Это позволяет визуализировать участки с высокой энергетической активностью, когда анатомические изменения не видны на обычной КТ или МРТ.

Верхние и нижние оценки

Для сохранения «человеческой» структуры мозга (86 млрд нейронов, архитектура коры) оценки числа синапсов ограничены [56, 57]:

• **Нижняя граница:** ~ (100 триллионов). Рассчитано как 86 млрд × 1000–3000 синапсов/нейрон.

• **Верхняя граница:** ~ (1 квадриллион). Рассчитано как 86 млрд × 10 000–17 500 синапсов/нейрон.

Изменение числа синапсов на один десятичный порядок величины привело бы к критической потере связности и функциональности, выходящей за пределы нормы человеческого мозга [58].

Таким образом, человеческий мозг содержит порядка 100–150 триллионов синапсов, динамически изменяющихся на протяжении жизни. Синаптическая плотность критична для когнитивных способностей и чувствительна к опыту и патологиям. Снижение на один десятичный порядок приводит к появлению ментально нечеловеческого существа, сущность которого нейрофизиологи политкорректно характеризуют «критической потерей связности и функциональности, выходящей за пределы нормы человеческого мозга».

Аппроксимации и шаги по шкале времени

Итак, проанализируем данные из предыдущего раздела по плотности синапсов и будем считать изменение по шкале времени критическим, если число связей упадет на один десятичный порядок, т.е. станет примерно равно $1.6x10^8$ (по сравнению с $16x10^8$ в детском возрасте).

Аргументы по оси абсцисс (годы): x = [0.1, 2, 16, 74]

Значения функции (плотность синапсов, без умножающего коэффициента): y = [11, 16.6, 11.05, 9.56]

Применяемые методы аппроксимации

1. Кубический полином (степень 3)

$P(x)=0.002915x^3-0.2631x^2+3.488x+10.65$

Характеристики:

- RSS = 0.00 (идеальная интерполяция)
- $R^2 = 1.00$
- AIC =-183.86
- Проходит точно через все четыре точки

RSS (residual sum of squares) — сумма квадратов остатков в регрессионном анализе. Это мера, которая оценивает разницу между прогнозируемыми и фактическими значениями зависимой переменной. RSS представляет собой различия в данных, которые не объясняются регрессионной моделью

AIC (Akaike information criterion) – информационный критерий Акаике критерий, который используется для сравнения нескольких статистических моделей на одной и той же обучающей выборке. Он основан на понятиях теории информации и информационной энтропии.

Критерий разработан японским математиком Хироцугу Акаике в 1971-м году и предложен им в статье 1974 года.

Принцип работы: AIC оценивает относительный объём информации, теряемой моделью. Поскольку предсказания реальной модели всегда не точные, по сравнению с идеальной моделью, которая не делает ошибок, реальная допускает потерю информации. AIC оценивает эту потерю: чем меньше значение критерия, тем меньше потеря информации, связанная с моделью, и тем лучше модель соответствует данным.

Особенность критерия — введение штрафа за число параметров модели. Параметры статистической модели, например, коэффициенты регрессии, оцениваются на основе обучающих данных, и включение в модель новых параметров увеличивает количество информации, привлекаемой для построения модели, но при этом улучшает подгонку модели именно к обучающим данным, что ведёт к переобучению. Введение штрафов на значение информационного критерия за число параметров модели позволяет решить эту проблему.

Считается, что лучшей будет модель с наименьшим значением критерия AIC.

Формула расчета

AIC = 2k — 2ln(L), где:

k — количество параметров модели;

L — максимальное значение функции правдоподобия.

Альтернативно, для моделей с нормально распределёнными ошибками AIC можно записать как AIC = 2k + 2ln(RSS/n), где:

RSS — сумма квадратов остатков;

n — размер выборки.

Логика формулы: первый член 2k представляет собой штраф за сложность модели, а второй член -2ln(L) отражает качество подгонки. Коэффициент 2 в штрафном члене выбран не случайно — он обеспечивает асимптотически оптимальные свойства критерия.

Важно отметить, что AIC не является абсолютной мерой качества модели — он предназначен для сравнения альтернативных моделей на одних и тех же данных. Разность значений AIC между моделями (ΔAIC) несёт больше информации, чем абсолютные значения.

Ограничения

1. Штрафование числа параметров ограничивает значительный рост сложности модели.

2. Проверка критерия является трудоёмкой операцией.

3. AIC может сравнивать модели только с выборками равного размера.

Когда размер выборки невелик, существует вероятность, что AIC выберет модели со слишком большим количеством параметров — в связи с этим разработан AICc (Corrected Akaike Information Criterion) — AIC с поправкой на небольшие размеры выборки.

2. Линейная регрессия (аппроксимация полиномом первой степени)

$$P(x)=-0.05297x+13.27$$

Характеристики:

- RSS = 18.86
- R^2 = 0.35
- AIC = 21.55
- Монотонное убывание

3. Квадратичная регрессия (полином второй степени)

$$P(x)=0.001413x^2-0.1613x+13.74$$

Характеристики:

- RSS = 17.73
- R^2 = 0.39
- AIC = 23.31
- Минимум ≈ 9.14 при x ≈ 57

Монотонно возрастает при x > 57, что не соответствует аппроксимируемому процессу.

Исследуем квадратичную функцию

$f(x) = 0.0014\ x^2 – 0.16\ x + 13.74$

Вид параболы:

– коэффициент a = 0.0014 > 0;

– ветви параболы направлены вверх, вершина — точка минимума.

Вершина параболы:

x ≈ 57

y ≈ 9.17

Дискриминант:

$D = b^2 – 4ac ≈ – 0.051344$

D < 0 → действительных корней нет, график не пересекает ось абсцисс.

4. Экспоненциальная модель

$$P(x)=4.55e^{-0.0345x}+9.11$$

Характеристики:

- RSS = 17.98;
- асимптота: y = 9.11 при x →∞;
- хорошо описывает спад после пика;
- значения всегда > 2.

5. Гауссова функция

$$P(x) = 62.97\exp\left(-\frac{(x-8.07)^2}{2\cdot 2.90^2}\right)+9.56$$

Характеристики:

RSS ≈ 0 (идеальное совпадение)

пик при x = 8.07;

асимптота: y = 9.56 при x →±∞;

отлично для симметричного спада от максимума;

значения всегда ≥ 9.56.

6. Логарифмическая модель

$$P(x)=-0.323\ln x+12.49$$

Характеристики:

- RSS = 26.44;
- монотонное убывание к-∞ при x →∞;
- медленный спад;
- P(x) < 2 при $x > 1.23\times10^{14}$.

В таблицах 5 и 6 приведены оценки, обосновывающие различные свойства аппроксимаций и выбор линейной модели.

Таблица 5

Сравнение качества моделей на обучающих данных

Модель	RSS	R^2	AIC
Кубическая	0.00	1.00	-183.86
Квадратичная	17.73	0.39	23.31
Линейная	18.86	0.35	21.55
Экспоненциальная	17.98	-	-
Гауссова			-
Логарифмическая	26.44	-	-

Таблица 6

Интерполяция значений функций

Модель	x=10	x=50	x=74	x=80
Кубическая	22.14	-108.22	9.56	98.71
Линейная	-	-	9.35	9.03
Квадратичная	-	10.92	9.54	11.74
Экспоненциальная	-	9.93	9.47	9.40
Гауссова	-		9.56	
Логарифмическая	-	11.23	11.10	11.08

Для интерполяции (внутри диапазона [0.1, 74])

1. Кубический полином дает идеальную точность.

2. Гауссова функция хорошо описывает пик и симметричный спад.

3. Кубические сплайны дают гладкую интерполяцию.

Указанные функции могут использоваться для прогнозирования плотности коры мозга при различном возрасте, приблизительно до 75 лет. Экстраполяция для иллюстрации леммы возможна только для линейной функции.

Для экстраполяции AIC минимален для линейной модели. Линейная регрессия показывает максимальную стабильность и гладкость.

Квадратичная аппроксимация создает некий компромисс между точностью и стабильностью, но как было доказано выше, не соответствует снижению плотности синапсов с возрастом.

Для прогнозирования за пределами наблюдаемого диапазона оптимальна линейная регрессия благодаря минимальной изменчивости поведения.

Итак, выделим для дальнейшего анализа линейную функцию (аргумент x – годы).

$P(x) = -0.05297x + 13.27$

Условия:

$P(x) < y$

Число синапсов падает до $2x10^8$ (фаза «Внимание!»)

$Y = 2$: $x > 212.76$ – около 213 лет.

Число синапсов падает на порядок (фаза «Новое нечеловеческое существо»)

$Y = 1.6$: $x > 220.31$ – около 220 лет.

Падение ниже 1.1 (фаза «Финал»)

$Y = 1.1$: $x > 229.31$ – около 230 лет.

Итак «предел Пошебякина» проходит по области от 210 до 230 лет, когда структура мозга кардинально меняется.

ЗАКЛЮЧЕНИЕ

Мы не будем завершать наше исследование на пессимистической ноте и вспомним, что о «пределе Пошебякина» наверняка знали и мудрые советские мастера искусств. Не случайно на эту тему звездным дуэтом Алексея Рыбникова и Булата Окуджавы написан «Романс черепахи Тортиллы» – самой древней жительницы пруда:

Был беспечным и наивным
Черепахи юной взгляд.
Все вокруг казалось дивным
Триста лет тому назад...
Юный друг, всегда будь юным,
Ты взрослеть не торопись,
Будь веселым, дерзким, шумным,
Драться надо – так дерись!
Никогда не знай покоя,
Плачь и смейся невпопад!
Я сама была такою
Триста лет тому назад...

В этом же романсе содержится ответ на вопрос, как снизить последствия уменьшения ментальных способностей с возрастом.

Добавим еще два соображения. Первое: ряд зарубежных исследователей говорят о том, что человеческому сознанию свойственна определенная ограниченная пластичность, которая не позволяет ему бесследно переживать исторические эпохи, когда происходит «слом парадигмы» и радикальные смены общественных и человеческих отношений. Сознание выдерживает без патологических изменений 3-4 таких «революции». Поскольку в новое время периодичность таких сломов – около 50 лет, получаем ту же численную оценку, что и лемма Пошебякина.

Второе: мы уже говорили о том, что лемма – это вспомогательное утверждение и есть свидетельства о том, что Павел Бякин сформулировал «Теорему Бякина», в которой говорил об ограниченном периоде существования как разумных живых систем (оценивая сроки жизни мыслящих животных), так и вычислительных машин определенной сложности.

СПИСОК ЛИТЕРАТУРЫ [5]

1. Бякина В.П. (2012). Вклад петербургской физиологической школы И.П. Павлова и его учеников первой волны эмиграции в создание геронтологии как науки. Cyberleninka. URL: https://cyberleninka.ru/article/n/vklad-peterburgskoy-fiziologicheskoy-shkoly-i-p-pavlova-i-ego-uchenikov-pervoy-volny-emigratsii-v-sozdanie-gerontologii-kak-nauki

2. Учёные записки. Первый Санкт-Петербургский государственный медицинский университет им. акад. И.П. Павлова. (2012). URL: https://www.1spbgmu.ru/images/home/universitet/izdatelstvo/uchenie_zapiski/4_12.pdf

3. Haritonov Wiki. Лемма Пошибякина. URL: https://haritonov.wiki/Лемма_Пошибякина

4. Dana Foundation. (2025). Neurotransmission: The Synapse. URL: https://dana.org/resources/neurotransmission-the-synapse/

5. BioNumbers. (2003). Number of synapses in cerebral cortex. Harvard Medical School. URL: https://bionumbers.hms.harvard.edu/bionumber.aspx?s=n&v=2&id=112056

6. Harvard Medical School. (2024). A New Field of Neuroscience Aims to Map Connections in the Brain. URL: https://hms.harvard.edu/news/new-field-neuroscience-aims-map-connections-brain

7. Seven and a Half Lessons About the Brain. (2015). URL: 500 trillion connections. https://sevenandahalflessons.com/notes/500_trillion_connections

8. AI Impacts. (2020). Scale of the Human Brain. URL: https://aiimpacts.org/scale-of-the-human-brain/

9. Tang Y., et al. (2001). Total regional and global number of synapses in the human brain neocortex. Synapse, 41(3), 258-273.

10. Healthline. (2018). Synaptic Pruning: Definition, Early Childhood, and More. URL: https://www.healthline.com/health/synaptic-pruning

11. Huttenlocher P. R. (1979). Synaptic density in human frontal cortex. Brain Research, 163(2), 195-205.

12. Wikipedia. (2007). Synaptic pruning. URL: https://en.wikipedia.org/wiki/Synaptic_pruning

13. PMC. (2007). Changes in the structural complexity of the aged brain. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC2441530/

14. ScienceDirect. (2014). The impact of ageing on synapse structure. URL: https://www.sciencedirect.com/science/article/abs/pii/S156816371400004X

15. Wikipedia. (2008). Синаптический прунинг. URL: https://ru.wikipedia.org/wiki/Синаптический_прунинг

16. RBC Trends. (2025). Почему подростки такие рассеянные. URL: https://trends.rbc.ru/trends/education/6853a1c99a7947909d0f609c

17. PMC. (2021). Mechanisms governing activity-dependent synaptic pruning. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8541743/

18. Nature. (2021). Mechanisms governing activity-dependent synaptic pruning in the developing mammalian CNS. URL: https://www.nature.com/articles/s41583-021-00507-y

19. Indicator.ru. (2019). Ученые выяснили, как мозг «отбирает» синапсы. URL: https://indicator.ru/biology/kak-mozg-otbiraet-sinapsy-06-08-2019.htm

20. JOVE. (2025). Experience-dependent remodeling of synaptic connectivity. URL: https://www.jove.com/ru/t/66629/experience-dependent-remodeling-juvenile-brain-olfactory-sensory

21. Frontiers. (2025). Neuron-to-glia signaling directs critical period synaptic pruning. URL: https://www.frontiersin.org/journals/cell-and-developmental-biology/articles/10.3389/fcell.2025.1540052/full

22. Nature. (2017). Monocular deprivation induces dendritic spine elimination. URL: https://www.nature.com/articles/s41598-017-05337-6

23. PMC. (2013). Accelerated experience-dependent pruning of cortical synapses. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC3792401/

24. Nature. (2025). Large-scale synaptic dynamics drive binocular circuit reconstruction. URL: https://www.nature.com/articles/s41467-025-60825-y

25. PNAS. (2011). Rapid experience-dependent plasticity of synapse function. URL: https://www.pnas.org/doi/10.1073/pnas.1108270109

26. PMC. (2020). Monocular deprivation affects visual cortex plaswww.jove.com/ru/t/56153/evaluation-of-synapse-density-in-hippocampal-rodent-brain-slices

[5] Составлен в авторской редакции. Период обращения к источникам: 21.02.2026-21.03.2026.

27. JOVE. (2025). Evaluation of synapse density in hippocampal rodent brain slices. URL: https://www.jove.com/ru/t/56153/evaluation-of-synapse-density-in-hippocampal-rodent-brain-slices
28. BioNumbers. (2004). Number of synapses in cortex - Human. URL: https://bionumbers.hms.harvard.edu/bionumber.aspx?id=106138
29. PubMed. (1997). Regional differences in synaptogenesis in human cerebral cortex. URL: https://pubmed.ncbi.nlm.nih.gov/9336221/
30. PMC. (2023). The regional pattern of age-related synaptic loss. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12701775/
31. PubMed. (2024). The regional pattern of age-related synaptic loss in the human brain. URL: https://pubmed.ncbi.nlm.nih.gov/37955791/
32. Mediasphera. (2017). Старение головного мозга человека. URL: https://www.mediasphera.ru/issues/zhurnal-nevrologii-i-psikhiatrii-im-s-s-korsakova-2/2017/1-2/1199772982017012003
33. PMC. (2023). Uncovering the link between synaptic density and mental illness. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC10139056/
34. Nature. (2024). Synaptic changes in psychiatric and neurological disorders. URL: https://www.nature.com/articles/s41386-024-01943-x
35. PMC. (2021). First in vivo evaluations of synaptic density alterations. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8617161/
36. PET Centre Turku. (2024). PET imaging of synaptic density. URL: http://www.turkupetcentre.net/petanalysis/target_synaptic_density.html
37. Wikipedia. (2006). List of animals by number of neurons. URL: https://en.wikipedia.org/wiki/List_of_animals_by_number_of_neurons
38. Nature. (2024). Network statistics of whole-brain connectome in fruit fly. URL: https://www.nature.com/articles/s41586-024-07968-y
39. PMC. (2019). Neuronal morphology and synapse count in C. elegans. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6817514/
40. Reddit. (2019). Each neuron has 10000 connections. URL: https://www.reddit.com/r/artificial/comments/181aeyg/each_neuron_has_10000_connections_too_other/
41. Academic OUP. (2020). Invariant synapse density and neuronal connectivity scaling. URL: https://academic.oup.com/cercor/article/30/10/5604/5850230
42. PMC. (2016). Neuronal factors determining high intelligence. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC4685590/
43. Wikipedia. (2004). Neuroscience and intelligence. URL: https://en.wikipedia.org/wiki/Neuroscience_and_intelligence
44. PMC. (2018). Large and fast human pyramidal neurons associate with intelligence. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6363383/
45. eLife. (2019). Human Intelligence: What single neurons can tell us. URL: https://elifesciences.org/articles/44560
46. PMC. (2024). Functional myelin in cognition and neurodevelopmental disorders. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11016012/
47. Academic OUP. (2024). Cerebral white matter myelination is associated with intelligence. URL: https://academic.oup.com/braincomms/article/6/6/fcae412/7902046
48. PMC. (2019). Genes, cells and brain areas of intelligence. https://pmc.ncbi.nlm.nih.gov/articles/PMC6384251/
49. Wikipedia. (2001). Neural network (machine learning). https://en.wikipedia.org/wiki/Neural_network_(machine_learning)
50. Habr. (2025). Спайковые нейросети на Swift. https://habr.com/ru/articles/933566/
51. Wikipedia. (2001). Artificial neural networks. https://en.wikipedia.org/?title=Artificial_neural_networks
52. Journals RCSI. (2024). Artificial neural network with dynamic synapse model. https://journals.rcsi.science/0869-6632/article/view/260944
53. Nature. (2024). High-performance deep spiking neural networks. https://www.nature.com/articles/s41467-024-51110-5
54. Nature. (2025). Concept transfer of synaptic diversity from biological to artificial neural networks. https://www.nature.com/articles/s41467-025-60078-9
55. Science Mail.ru. (2025). Суперкомпьютер создал виртуальную модель мозга мыши. https://science.mail.ru/news/40962-model-mozga-myshi-video/

56. USF Digital Commons. Total number of synapses in the adult human neocortex. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=4812&context=ujmm
57. Habr. (2014). В человеческом мозге столько же «транзисторов». https://habr.com/ru/articles/108483/
58. PMC. (2015). Nanoconnectomic upper bound on the variability of synaptic plasticity. https://pmc.ncbi.nlm.nih.gov/articles/PMC4737657/

Приглашаем авторов к участию в журнале «Вестник современных цифровых технологий»

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Редакция принимает материалы статей, соответствующие тематике журнала, содержащие новые научные результаты, не опубликованные ранее и не предназначенные к публикации в других печатных или электронных изданиях. Проводится независимое внутреннее рецензирование. Статьи в журнале публикуются бесплатно (объем – до 15 тыс. знаков), после получения одобрения Редакционного совета.

Для опубликования статьи в редакцию журнала необходимо направить по адресу *a.shcherbakov@c3da.org, a.ryazanova@c3da.org* **следующие материалы в электронном виде:**

- рукопись статьи в DOC- и PDF-форматах;
- иллюстрации, предоставленные также и отдельными файлами в формате JPG или PNG с разрешением 300 dpi;
- сведения об авторах, содержащие фамилию, имя, отчество, ученые степень и звание, должность, место работы, контактные телефоны или E-mail;
- англоязычную информацию, содержащую название статьи, ФИО авторов, аннотацию и ключевые слова;
- редакция может запросить экспертное заключение о возможности публикации статьи в открытой печати.

ПОСЛЕДОВАТЕЛЬНОСТЬ МАТЕРИАЛОВ ДЛЯ ПУБЛИКАЦИИ:

1. шифр УДК (см. Справочник УДК) в левом верхнем углу;
2. название статьи (полужирным шрифтом по центру) не более 12 слов;
3. инициалы и фамилия автора (полужирным шрифтом по центру), к каждому автору- сноска, содержащая ученое звание, должность, название организации (без сокращений), e-mail;
4. Аннотация, излагающая суть работы и полученные результаты (5-7 строк);
5. ключевые слова (8-10 слов);
6. англоязычная информация по статье (по пп.2-5)
7. текст статьи с учетом указанных далее требований к его оформлению;
8. список литературы, оформленный по ГОСТ Р 7.0.5-2008.

Статья должна быть структурирована, т.е. должна включать разделы с названиями, кратко и точно отражающими их содержание, в том числе:

- введение, содержащее обоснование актуальности и краткий обзор проблематики;
- четкую постановку задачи исследования;
- описание метода решения задачи исследования;
- прикладную интерпретацию и иллюстрацию полученных результатов исследования;
- заключение, включающее обобщение и указание области применения полученных результатов, не повторяющее аннотацию и не ограничивающееся простым перечислением того, что сделано в работе.

С детальными требованиями к рисункам, таблицам, формулам, списку литературы, а также с примерами оформления статьи можно ознакомиться на странице Вестника http://c3da.org/journal.html.

Приглашается к сотрудничеству редактор для работы в редакции журнала по совместительству. Просьба направлять резюме по электронному адресу *accda@c3da.org, info@c3da.org*

ТРЕБОВАНИЯ К РЕДАКТОРУ:

• отличное знание русского языка;
• свободное владение ПК, в том числе специальными текстовыми и графическими программами;
• опыт работы в издательстве.

Высшее техническое образование и знание английского языка являются существенными преимуществами.

ОБЯЗАННОСТИ

Редактор:

• редактирует рукописи, принятые к изданию;
• оказывает авторам необходимую помощь по улучшению структуры рукописей, выбору терминов, оформлению иллюстраций;
• проверяет, насколько учтены авторами замечания по доработке, предъявленные к рукописям;
• подписывает отредактированные рукописи в печать.