Российская Академия Наук

Российский центр научной информации

Вестник Российского фонда фундаментальных исследований

ISSN 2587-6090 eISSN 2587-8956 № 1 (129) январь – март 2026 года

Основан в 1994 году

Зарегистрирован Комитетом РФ по печати, рег. № 012620 от 03.06.1994

Сетевая версия зарегистрирована Роскомнадзором, рег. № ФС77-61404 от 10.04.2015

Учредитель

Федеральное государственное бюджетное учреждение

«Российский центр научной информации»

Главный редактор В.Я. Панченко,

заместители главного редактора В.В. Квардаков, В.Н. Фридлянов

Редакционная коллегия:

В.П. Анаников, В.Б. Бетелин, К.Е. Дегтярёв, И.Л. Ерёменко,

П.К. Кашкаров, В.П. Матвеенко, А.С. Сигов,

В.А. Ткачук, Р.В. Петров, Д.Р. Хохлов

Редакция:

И.А. Мосичева, К.В. Клименко

Адрес редакции:

119991, г. Москва, Ленинский пр-т, д. 32а

Тел.: (499) 995-16-05

E-mail: pressa@rcsi.science

© Российский центр научной информации, 2026

Russian Academy of Sciences

Russian Centre for Science information

Russian Foundation for Basic Research Journal

ISSN 2587-6090 eISSN 2587-8956 No 1 (129) January – March 2026

Founded in 1994

Registered by the Committee of the Russian Federation for Printed Media, 012620 of 03.06.1994 (print)
Registered by the Roskomnadzor FS77-61404 of 10.04.2015 (online)

The Founder

Federal State Budgetary Institution

Russian Centre for Science information

Chief editor V.Ya. Panchenko,
Deputy chief editors V.V. Kvardakov, V.N. Fridlyanov

Editorial board:

V. Ananikov, V. Betelin, K. Degtyarev, I. Eremenko,
P. Kashkarov, V. Matveenko, A. Sigov,
V. Tkachuk, R. Petrov, D. Khokhlov

Editorial staff:

I. Mosicheva, K. Klimenko

Editorial office address:

32a, Leninskiy Ave., Moscow, 119991 , Russia
Tel.: (499) 995-16-05
E-mail: pressa@rcsi.science

© Russian Centre for Science information, 2026

СОДЕРЖАНИЕ

КОЛОНКА ТЕМАТИЧЕСКОГО РЕДАКТОРА

О редакторе тематического блока академике РАН, докторе технических наук, профессоре И.А. Шеремете 7

Аннотация к тематическому блоку 11

ТЕМАТИЧЕСКИЙ БЛОК: ЦИФРОВОЙ СУВЕРЕНИТЕТ: ТЕХНОЛОГИЧЕСКИЕ ОСНОВЫ И ВЫЗОВЫ

Массель Л.В., Массель А.Г.
Методология научного обоснования стратегических решений по цифровой трансформации энергетики на основе ситуационного управления и цифровых двойников 16

Карпук А.А., Кохно П.А.
Модели показателей и параметров качества услуг сотовой связи 25

Михайленко И.И., Мещеряков О.Д., Литвинов А.И.
Формирование обучающего датасета для оценки функциональных состояний КРС 43

Лобанов А.Г., Алиев М.В., Чефранов С.Г., Алиева М.Ф.
Структурированные данные как фактор производства в цифровой экономике 53

Белов В.А., Кобринский Б.А., Акимова А.А.
Экспертный подход к формированию признакового пространства факторов риска хронического тонзиллита у детей 64

Бубнов О.А.
Обеспечение информационной безопасности систем искусственного интеллекта в финансовом секторе 76

Лебедь С.В.
Киберугрозы и безопасность банковской инфраструктуры: анализ в контексте обеспечения цифрового суверенитета России 88

Игонин А.А.
Безопасный и дешёвый криптокошелёк на базе доверенной SIM-карты 103

Самоходкин Е.В., Самоходкина А.А.
Доверие к системам искусственного интеллекта как условие цифрового суверенитета в финансовом секторе 113

Егоров А.А., Егорова М.А.
Модель распространения информации в обществе: учёт влияния современных масс-медиа 127

Шеремет И.А.
Большие языковые модели и их влияние на интеллектуальный потенциал человечества 136

CONTENTS

THEMED ISSUE EDITOR'S COLUMN

About the Editor of the Thematic Section, Full Member of the Russian Academy of Sciences Igor Anatolyevich Sheremet 9

Sheremet I.A. Abstract of the Themed Section 13

THEMATIC SECTION: DIGITAL SOVEREIGNTY: TECHNOLOGICAL FOUNDATIONS AND CHALLENGES

Massel L.V., Massel A.G.
Methodology for the Scientific Substantiation of Strategic Decisions on the Digital Transformation of the Energy Sector Based on Situational Management and Digital Twins 16

Karpuk A.A., Kokhno P.A.
Models of Indicators and Parameters of Quality of Cellular Services 25

Mikhailenko I.I., Meshcheryakov O.D., Litvinov A.I.
Creating a Training Dataset for Assessing the Functional States of Cattle 43

Lobanov A.G., Aliev M.V., Chefranov S.G., Aliyeva M.F.
Structured Data as a Factor of Production in the Digital Economy 53

Belov V.A., Kobrinsky B.A., Akimova A.A.
Expert Approach to Forming the Signal Space of Chronic Tonsillitis Risk Factors in Children 64

Bubnov O.A.
On Ensuring Information Security of Artificial Intelligence Systems in the Financial Sector 76

Lebed S.V.
Cyberthreats and Banking Infrastructure Security: an Analysis in the Context of Ensuring Russia's Digital Sovereignty 88

Igonin A.A.
Secure and Cheap Crypto Wallet Based on a Trusted SIM Card 103

Samokhodkin E.V., Samokhodkina A.A.
Trust in Artificial Intelligence Systems as a Condition for Digital Sovereignty in the Financial Sector 113

Egorov A.A., Egorova M.A.
A Model of Information Spreading in Society: Taking into Account the Influence of Modern Mass Media 127

Sheremet I.A.
Large Language Models and Their Impact on the Intellectual Potential of Humanity 136

О редакторе тематического блока академике РАН Игоре Анатольевиче Шеремете

- Председатель Научного совета РАН «Информационная безопасность»
- Член президиума Высшей аттестационной комиссии при Минобрнауки России
- Член президиума научно-технического совета Минцифры России
- Генерал-майор в отставке
- Действительный государственный советник Российской Федерации 3 класса
- Заместитель председателя Комитета РАН по системному анализу
- Заместитель председателя Научного совета по робототехнике и мехатронике РАН
- Член научного совета РАН «Квантовые технологии»
- Почётный член (Fellow) Китайской компьютерной федерации (China Computer Federation, CCF)

Игорь Анатольевич Шеремет родился в городе Молодечно (ныне Республика Беларусь) в 1956 году. В 1972 году закончил с золотой медалью среднюю школу и поступил в Военную академию имени Ф.Э. Дзержинского (сейчас Военная академия Ракетных войск стратегического назначения имени Петра Великого), которую закончил с отличием в 1977 году. В 1984 году защитил кандидатскую диссертацию, а в 1993 — докторскую. В 2016 году был избран членом-корреспондентом РАН по отделению нанотехнологий и информационных технологий, в 2022 — академиком РАН по этому же отделению.

И.А. Шеремет с 2009 по 2012 год являлся заместителем начальника Генерального штаба Вооружённых Сил Российской Федерации, возглавлял Военно-научный комитет Вооружённых Сил. С 2012 по 2015 год — член Военно-промышленной комиссии при Правительстве Российской Федерации и коллегии ВПК России, председатель Совета ВПК по АСУ, связи, разведке, радиоэлектронной борьбе и информационному противоборству, курировал радиоэлектронную промышленность России. С 2015 по 2022 год — заместитель директора по науке Российского фонда фундаментальных исследований, курировал междисципли-

нарные исследования, проводившиеся на гранты РФФИ в интересах федеральных органов власти и крупнейших корпораций Российской Федерации («Ростех», «Росатом», «Роскосмос», «Российские железные дороги» и др.), а также региональную и международную деятельность РФФИ. В течение ряда лет И.А. Шеремет работал профессором на кафедре «Информационная безопасность» МГТУ им. Н.Э. Баумана, возглавлял кафедру «Информационная безопасность» Финансового университета при Правительстве Российской Федерации.

И.А. Шеремет — известный учёный, автор и соавтор более 300 научных трудов, в том числе 26 книг и двух патентов. Подготовил пять докторов и тринадцать кандидатов технических наук.

В первой половине 1980-х годов, в период повсеместного развития различных модификаций реляционной модели данных и ассоциированных с ней моделей представления знаний, И.А. Шеремет предложил принципиально иной подход к формализации и аксиоматизации баз данных и знаний. В основу этого подхода положено представление базы данных (БД) в виде множества символьных строк («фактов»), а базы знаний (БЗ) — в виде специальным образом модифицированной («расширенной») системы Поста (РСП), определяющей логику формирования новых фактов из ранее сформированных и/или имеющихся в БД. При этом система логического вывода РСП непосредственно реализует мультиагентную технологию смысловой обработки и накопления поступающих фактов, в том числе естественно-языковых текстов, в связи с чем РСП уже в 1980-е годы могли использоваться для реализации не только простейших LLM/LMM, но и существенно более адекватных моделей разговорного искусственного интеллекта. Подход был впервые успешно реализован во второй половине 1980-х годов на мейнфреймах серии ЕС. Ядром его программной реализации была созданная в 1986 г. оригинальная система управления так называемыми страничными базами данных, оперировавшая динамическими гипертекстами и представлявшая собой прообраз современных веб-серверов. Одновременно был создан прототип веб-клиента для персональных компьютеров.

И.А. Шеремет с 2000-х годов разрабатывает теорию рекурсивных мультимножеств и методы её применения для решения задач системного анализа, исследования операций и цифровой экономики. В рамках этого направления им предложен математический инструментарий, сочетающий в себе достоинства классического математического программирования и современной инженерии знаний, и получены фундаментальные результаты, обеспечивающие эффективное применение методов искусственного интеллекта для решения задач программно-целевого планирования и управления в больших социотехнических системах. Наряду с этим разработаны методы анализа и обеспечения устойчивости критических инфраструктур и использующих их социотехнических систем к деструктивным воздействиям (стихийным бедствиям, техногенным катастрофам, террористическим актам, кибератакам, экономическим санкциям).

About the Editor of the Thematic Section, Full Member of the Russian Academy of Sciences Igor Anatolyevich Sheremet

- Chairman of the Scientific Council of the Russian Academy of Sciences on Information Security
- Member of the Presidium of the Higher Attestation Commission under the Ministry of Science and Higher Education of the Russian Federation
- Member of the Presidium of the Scientific and Technical Council of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation
- Major General, retired
- Full State Councillor of the Russian Federation, 3rd Class
- Deputy Chairman of the RAS Committee on Systems Analysis
- Deputy Chairman of the RAS Scientific Council on Robotics and Mechatronics
- Member of the Scientific Council of the Russian Academy of Sciences on Quantum Technologies
- Honorary Fellow of the China Computer Federation (CCF)

Igor Anatolyevich Sheremet was born in the city of Molodechno, now in the Republic of Belarus, in 1956. In 1972, he graduated from secondary school with a gold medal and entered the F.E. Dzerzhinsky Military Academy, now the Peter the Great Military Academy of the Strategic Missile Forces, from which he graduated with honors in 1977. In 1984, he defended his Candidate of Sciences dissertation, and in 1993 his Doctor of Sciences dissertation. In 2016, he was elected a Corresponding Member of the Russian Academy of Sciences in the Division of Nanotechnologies and Information Technologies, and in 2022 a Full Member of the Russian Academy of Sciences in the same division.

From 2009 to 2012, I.A. Sheremet served as Deputy Chief of the General Staff of the Armed Forces of the Russian Federation and headed the Military Scientific Committee of the Armed Forces. From 2012 to 2015, he was a member of the Military-Industrial Commission under the Government of the Russian Federation and of the Board of the Military-Industrial Commission of Russia; he chaired the Commission's Council on automated control systems, communications, intelligence, electronic warfare, and information confrontation, and oversaw Russia's radio-electronic industry. From 2015 to 2022, he served as Deputy Director for Science at the Russian Foundation for Basic Research, where he supervised interdisciplinary research conducted with RFBR grants in the interests of federal authorities and major Russian corporations, including Rostec, Rosatom, Roscosmos, Russian Railways, and others, as well as the Foundation's regional and international activities. For a number of years, I.A. Sheremet worked as a professor at the Department of Information Security of Bauman Moscow State Technical University and headed the Department of Information Security at the Financial University under the Government of the Russian Federation.

I.A. Sheremet is a renowned scholar and the author and co-author of more than 300 scientific works, including 26 books and two patents. He has supervised five Doctors of Technical Sciences and thirteen Candidates of Technical Sciences.

In the first half of the 1980s, during the widespread development of various modifications of the relational data model and the associated models of knowledge representation, I.A. Sheremet proposed a fundamentally different approach to the formalization and axiomatization of databases and knowledge bases. This approach is based on representing a database (DB) as a set of character strings ("facts") and a knowledge base (KB) as a specially modified ("extended") Post system (EPS), which defines the logic for generating new facts from previously generated facts and/or facts available in the DB. At the same time, the logical inference system of the EPS directly implements a multi-agent technology for semantic processing and accumulation of incoming facts, including nat-

ural-language texts. For this reason, as early as the 1980s, EPSs could be used to implement not only the simplest LLMs/LMMs, but also substantially more adequate models of conversational artificial intelligence. This approach was first successfully implemented in the second half of the 1980s on ES-series mainframes. The core of its software implementation was an original management system for so-called page databases, created in 1986, which operated with dynamic hypertexts and constituted a prototype of modern web servers. At the same time, a prototype web client for personal computers was developed.

Since the 2000s, I.A. Sheremet has been developing the theory of recursive multisets and methods for applying it to problems of systems analysis, operations research, and the digital economy. Within this line of research, he proposed a mathematical toolkit that combines the advantages of classical mathematical programming and modern knowledge engineering, and obtained fundamental results that enable the effective application of artificial intelligence methods to program-target planning and management in large sociotechnical systems. In addition, methods have been developed for analyzing and ensuring the resilience of critical infrastructures and of the sociotechnical systems that use them against destructive impacts, including natural disasters, technological accidents, terrorist acts, cyberattacks, and economic sanctions.

И.А. Шеремет, академик РАН,
доктор технических наук, профессор

АННОТАЦИЯ К ТЕМАТИЧЕСКОМУ БЛОКУ

Любая социотехническая система (СТС) представляет собой совокупность трёх компонентов: социума; технологической базы, которая включает устройства и комплексы, обеспечивающие жизнедеятельность социума; и ресурсной базы, содержащей ресурсы, необходимые социуму и технологической базе для функционирования. В этом контексте целесообразно различать ресурсно-технологическую устойчивость, ресурсно-технологическую независимость и интеллектуальную независимость СТС.

Ресурсно-технологическая устойчивость СТС — её способность обеспечить себя ресурсами в ассортименте и объёмах, необходимых для существования и развития социума, в условиях деструктивных внешних воздействий со стороны враждебных систем и/или окружающей среды.

Ресурсно-технологическая независимость СТС — её способность создавать и эксплуатировать объекты техносферы, необходимые для обеспечения её ресурсно-технологической устойчивости, в условиях её частичной либо полной изоляции от содействия дружественных внешних систем.

Интеллектуальная независимость СТС — её способность самостоятельно определять и решать задачи, критически важные для обеспечения её ресурсно-технологической независимости.

Цифровой суверенитет СТС можно рассматривать как сегмент её ресурсно-технологической независимости, охватывающий её информационную инфраструктуру (технические и программные средства, обеспечивающие получение, обработку, накопление, передачу и отображение информации) и информационные ресурсы. При этом в условиях повсеместной цифровизации информационная инфраструктура естественным образом стала ядром техносферы и основой функционирования всех остальных критических инфраструктур — энергетической, транспортной, производственной, банковско-финансовой, агропромышленной и других. Поэтому цифровой суверенитет в настоящее время — это основа ресурсно-технологической независимости государства в целом. С другой стороны, распространение во всех перечисленных сферах моделей, технологий и средств искусственного интеллекта (ИИ), во многих случаях зарубежного происхождения, сделало крайне актуальными исследования, направленные на оценку степени доверия к результатам его применения. Подобные исследования подтверждают то обстоятельство, что для обеспечения реального цифрового суверенитета социотехническая система должна обладать интеллектуальной независимостью, то есть, в конечном итоге, интеллектуальным потенциалом, достаточным для определения и решения важнейших задач обеспечения её ресурсно-технологической независимости.

Настоящий номер журнала посвящён рассмотрению различных аспектов цифрового суверенитета нашей страны в условиях массового применения искусственного интеллекта в банковско-финансовой, агропромышленной и медицинской сферах, а также на объектах телекоммуникационной и энергетической инфраструктур.

В статье Л.В. Массель и А.Г. Массель предлагается методология научного обо-

снования стратегических решений по цифровой трансформации энергетики на основе ситуационного управления и цифровых двойников. Разработанная авторами архитектура мульти-агентной интеллектуальной среды обеспечивает взаимодействие цифровых двойников объектов энергетики на уровне конкретных систем и энергетической инфраструктуры в целом.

Статья А.А. Карпука и П.А. Кохно посвящена вопросам оценки качества телекоммуникационной инфраструктуры в части сотовой связи. При этом показатели качества разделены по зонам ответственности между оператором и пользователем услуг связи, что позволяет достичь компромисса между обеспечением качества услуг связи и затратами на это обеспечение.

В статье И.И. Михайленко, О.Д. Мещерякова и А.И. Литвинова рассматриваются принципы построения основанных на машинном обучении по видеоданным бесконтактных систем наблюдения за поведением животных. Авторы развивают биометрию животных путём применения нейронных сетей для решения задач регистрации, уникальной идентификации и верификации крупного рогатого скота.

В статье А.Г. Лобанова, М.В. Алиева, С.Г. Чефранова и М.Ф. Алиевой рассматриваются вопросы цифровой трансформации в растениеводстве и создания информационной инфраструктуры для комплексной обработки потоков цифровых данных с полей. Это, в свою очередь, обеспечивает переход к «сквозным» моделям селекционно-семеноводческих процессов и к интегрированному геномно-экологическому прогнозированию посредством применения методов искусственного интеллекта.

Статья В.А. Белова, Б.А. Кобринского и А.А. Акимовой содержит описание подхода и основных результатов применения методов искусственного интеллекта для оценки контролируемых факторов риска развития хронического тонзиллита и их объективной характеристики с учётом возможной неопределённости. Авторами сформировано поле знаний риск-факторов этого заболевания, что необходимо для создания базы знаний интеллектуальной рекомендательной системы в этой области здравоохранения.

В статье О.А. Бубнова исследуется влияние уязвимостей систем искусственного интеллекта на обеспечение цифрового суверенитета Российской Федерации при их эксплуатации на объектах критической информационной инфраструктуры и в финансовом секторе. Показано, что неконтролируемое использование зарубежных моделей и средств ИИ, отсутствие стандартизированных процедур валидации моделей и недостаточная проработка вопросов кибербезопасности на всех этапах жизненного цикла ИИ создают прямые угрозы национальной безопасности в целом.

В статье С.В. Лебедя подробно анализируются различные аспекты кибербезопасности банковской инфраструктуры России в условиях роста интенсивности и расширения спектра кибератак на неё со стороны организованных сообществ киберпреступников и спецслужб враждебных и недружественных стран.

Статья А.А. Игонина посвящена детальному рассмотрению современного состояния архитектуры распределённых реестров (блокчейн), которая может использоваться в целом ряде приложений в рамках обеспечения цифрового суверенитета, и описанию предлагаемого нового подхода к реализации функций криптографического обеспечения указанной архитектуры на основе доверенных SIM-карт.

Статья Е.В. Самоходкина и А.А. Самоходкиной посвящена исследованию доверия к системам искусственного интеллекта в финансовом секторе как необходимого условия цифрового суверенитета. Показано, что доверие не сводится ни к пользовательской лояльности, ни к технической эффективности алгоритма; оно возникает на пересечении объяснимости, подотчётности, управления модельным риском, контроля над данными и инфраструктурной автономии. Обосновано, что в условиях повсеместного использования моделей

и средств ИИ зарубежного происхождения, характеризующихся непрозрачностью, доверие к ним приобретает суррогатный характер и не способствует укреплению цифрового суверенитета.

В статье А.А. Егорова и М.А. Егоровой предложена и исследована динамическая модель распространения информации в социуме. Представлены результаты теоретического анализа и компьютерного моделирования, демонстрирующие особенности поведения социума при вариации управляющих параметров. Анализ полученных результатов позволил установить области изменения параметров, при которых происходит переход от стационарного к периодическому и затем к хаотическому поведению, а впоследствии — обратный переход от хаотического к стационарному или периодическому поведению. Обращено внимание на возросшую роль Интернета как глобальной инфраструктуры для реализации управляющих информационно-психологических воздействий на индивидуальное, групповое и массовое сознание.

Статья И.А. Шеремета посвящена анализу больших языковых моделей (LLM) и их влияния на интеллектуальный потенциал человечества, а значит, нашей страны. Показывается, что повсеместное распространение LLM-чат-ботов и их систематическое использование, в особенности в образовательном цикле, влекут за собой риски массовой интеллектуальной деградации и утраты когнитивных способностей.

Статьи, вошедшие в номер, раскрывают различные направления и проблемы обеспечения цифрового суверенитета и могут служить основой для развёртывания и углубления дальнейших исследований по обозначенным направлениям.

I.A. Sheremet, Academician of the Russian Academy of Sciences, Doctor of Technical Sciences, Professor

ABSTRACT OF THE THEMED SECTION

Any sociotechnical system (STS) consists of three components: society; a technological base, which includes devices and complexes that support the functioning of society; and a resource base, which contains the resources required by society and the technological base for their operation. In this context, it is appropriate to distinguish between the resource-technological resilience, resource-technological independence, and intellectual independence of an STS.

The resource-technological resilience of an STS is its ability to provide itself with resources in the range and volumes necessary for the existence and development of society under destructive external impacts from hostile systems and/or the environment.

The resource-technological independence of an STS is its ability to create and operate technosphere facilities necessary to ensure its resource-technological resilience under conditions of partial or complete isolation from assistance by friendly external systems.

The intellectual independence of an STS is its ability to independently identify and solve tasks that are critically important for ensuring its resource-technological independence.

The digital sovereignty of an STS may be regarded as a segment of its resource-technological independence that covers its information infrastructure, including the hardware and software that provide for the acquisition, processing, accumulation, transmission, and display of information, as well as its informa-

tion resources. Under conditions of pervasive digitalization, information infrastructure has naturally become the core of the technosphere and the basis for the functioning of all other critical infrastructures, including energy, transport, manufacturing, banking and finance, agriculture and industry, and others. Therefore, digital sovereignty today is the foundation of the resource-technological independence of the state as a whole. On the other hand, the spread of artificial intelligence (AI) models, technologies, and tools, in many cases of foreign origin, across all the above areas has made research aimed at assessing the degree of trust in the results of their application extremely important. Such studies confirm that, in order to ensure genuine digital sovereignty, a sociotechnical system must possess intellectual independence; that is, ultimately, it must have intellectual potential sufficient to identify and solve the most important tasks involved in ensuring its resource-technological independence.

This issue of the journal is devoted to various aspects of our country's digital sovereignty under conditions of the large-scale application of artificial intelligence in the banking and financial, agricultural and industrial, and medical sectors, as well as at facilities of telecommunications and energy infrastructure.

The article by L.V. Massel and A.G. Massel proposes a methodology for the scientific substantiation of strategic decisions on the digital transformation of the energy sector based on situational management and digital twins. The multi-agent intelligent environment architecture developed by the authors ensures the interaction of digital twins of energy facilities both at the level of specific systems and at the level of the energy infrastructure as a whole.

The article by A.A. Karpuk and P.A. Kokhno addresses the assessment of the quality of telecommunications infrastructure with respect to cellular communications. In this context, quality indicators are divided between the areas of responsibility of the communications service operator and the user, which makes it possible to achieve a compromise between ensuring the quality of communications services and the costs required to provide it.

The article by I.I. Mikhaylenko, O.D. Meshcheryakova, and A.I. Litvinov examines the principles of designing contactless systems for observing animal behavior based on machine learning from video data. The authors develop animal biometrics by applying neural networks to the tasks of registration, unique identification, and verification of cattle.

The article by A.G. Lobanov, M.V. Alieva, S.G. Chefranov, and M.F. Alieva considers issues of digital transformation in crop production and the creation of information infrastructure for the integrated processing of digital data flows from fields. This, in turn, enables a transition to end-to-end models of breeding and seed-production processes and to integrated genomic-environmental forecasting through the use of artificial intelligence methods.

The article by V.A. Belov, B.A. Kobrinsky, and A.A. Akimova describes an approach to, and the main results of, applying artificial intelligence methods to assess controllable risk factors for chronic tonsillitis and to provide their objective characterization while taking possible uncertainty into account. The authors form a knowledge field of risk factors for this disease, which is necessary for creating the knowledge base of an intelligent recommender system in this area of healthcare.

The article by O.A. Bubnov examines the influence of vulnerabilities in artificial intelligence systems on ensuring the digital sovereignty of the Russian Federation when such systems are operated at critical information infrastructure facilities and in the financial sector. It is shown that the uncontrolled use of foreign AI models and tools, the absence of standardized model validation procedures, and insufficient elaboration of cybersecurity issues at all stages of the AI life cycle create direct threats to national security as a whole.

The article by S.V. Lebed provides a detailed analysis of various aspects of cybersecurity in Russia's banking infrastructure amid increasing intensity and a broadening spectrum of cyberattacks carried out against

it by organized cybercriminal communities and the special services of hostile and unfriendly countries.

The article by A.A. Igonin is devoted to a detailed consideration of the current state of distributed ledger architecture (blockchain), which can be used in a wide range of applications related to ensuring digital sovereignty, and to a description of a proposed new approach to implementing cryptographic support functions for this architecture on the basis of trusted SIM cards.

The article by E.V. Samokhodkin and A.A. Samokhodkina is devoted to the study of trust in artificial intelligence systems in the financial sector as a necessary condition for digital sovereignty. It is shown that trust is reducible neither to user loyalty nor to the technical efficiency of an algorithm; rather, it emerges at the intersection of explainability, accountability, model risk management, control over data, and infrastructural autonomy. It is substantiated that, under conditions of the pervasive use of AI models and tools of foreign origin characterized by opacity, trust in them becomes surrogate in nature and does not contribute to strengthening digital sovereignty.

The article by A.A. Egorov and M.A. Egorova proposes and studies a dynamic model of information dissemination in society. The results of theoretical analysis and computer simulation are presented, demonstrating the features of societal behavior as control parameters vary. Analysis of the results obtained made it possible to identify parameter ranges in which a transition occurs from stationary behavior to periodic and then chaotic behavior, followed subsequently by a reverse transition from chaotic behavior to stationary or periodic behavior. Attention is drawn to the growing role of the Internet as a global infrastructure for implementing controlling informational and psychological influences on individual, group, and mass consciousness.

The article by I.A. Sheremet is devoted to an analysis of large language models (LLMs) and their influence on the intellectual potential of humanity and, consequently, of our country. It is shown that the widespread dissemination of LLM chatbots and their systematic use, especially in the educational cycle, entail risks of mass intellectual degradation and loss of cognitive abilities.

The articles included in this issue reveal various directions and problems in ensuring digital sovereignty and may serve as a basis for expanding and deepening further research in the areas indicated.

ТЕМАТИЧЕСКИЙ БЛОК: ЦИФРОВОЙ СУВЕРЕНИТЕТ: ТЕХНОЛОГИЧЕСКИЕ ОСНОВЫ И ВЫЗОВЫ

Индекс УДК 004.89:621.311
Код ГРНТИ 50.43.31, 28.23.19
DOI: 10.22204/2410-4639-2026-129-01-16-24

Л.В. МАССЕЛЬ,
А.Г. МАССЕЛЬ*

Методология научного обоснования стратегических решений по цифровой трансформации энергетики на основе ситуационного управления и цифровых двойников

В статье представлена разработанная методология научного обоснования стратегических решений по цифровой трансформации энергетики, основанная на синтезе концепции ситуационного управления Д.А. Поспелова и современных интеллектуальных технологий. Обоснована необходимость интеграции семантического моделирования (онтологического, когнитивного, событийного и вероятностного), методов машинного обучения (глубоких нейронных сетей и генетических алгоритмов) и технологий цифровых двойников для решения задач стратегического планирования в условиях неопределённости. Предложена архитектура многоагентной интеллектуальной среды (МАИС), обеспечивающей взаимодействие цифровых двойников объектов энергетики и «умных» цифровых двойников (цифровых образов) на уровне систем и топливно-энергетического комплекса. Разработаны бионические модели выбора управляющих воздействий, сочетающие информационные методы, нейронные сети и генетические алгоритмы с явным и неявным представлением управляющих воздействий. Рассмотрены методы киберситуационной осведомлённости как синтеза исследований кибербезопасности и ситуационной осведомлённости. Приведены результаты апробации методологии на примерах создания прототипа цифрового двойника солнечной электростанции и реинжиниринга программного комплекса ИНТЭК-А как умного

* **Массель Людмила Васильевна** — доктор технических наук, заведующая отделом систем искусственного интеллекта в энергетике Института систем энергетики им. Л.А. Мелентьева СО РАН (ИСЭМ СО РАН).
E-mail: massel@isem.irk.ru

Массель Алексей Геннадьевич — кандидат технических наук, старший научный сотрудник отдела систем искусственного интеллекта в энергетике ИСЭМ СО РАН.
E-mail: amassel@isem.irk.ru

цифрового двойника топливно-энергетического комплекса. Методология позволяет повысить обоснованность стратегических решений за счёт интеграции качественного анализа на основе семантических моделей и количественного анализа с применением экономико-математических моделей в условиях учёта требований кибербезопасности и обеспечения устойчивости энергетических систем.

Ключевые слова: цифровая трансформация энергетики, ситуационное управление, семантическое моделирование, цифровой двойник, кибербезопасность, многоагентная интеллектуальная среда, стратегические решения, устойчивость энергетических систем, машинное обучение, генетические алгоритмы, киберситуационная осведомлённость, онтологический инжиниринг, бионические модели, умный цифровой двойник

Распространение концепций цифровой экономики и цифровой энергетики в Российской Федерации сопровождается рядом нерешённых проблем, среди которых выделяются когнитивные и управленческие сложности, научные и технологические ограничения, а также дефицит кадров [1]. Анализ Государственной программы «Цифровая экономика» и федерального проекта «Цифровая энергетика» показывает отсутствие в перечне рекомендуемых информационных технологий двух критически важных направлений: «Интеллектуальные технологии поддержки принятия стратегических решений по развитию цифровой энергетики» и «Технологии обеспечения кибербезопасности объектов цифровой энергетики» [2]. В условиях цифровизации энергетических систем информационно-коммуникационная подсистема становится сопоставимой по сложности и уязвимости с физической подсистемой, что повышает риски кибератак и требует новых подходов к обоснованию стратегических решений.

Концептуальные основы методологии

В основе предлагаемой методологии лежит концепция ситуационного управления, разработанная Д.А. Поспеловым в 1960–1980-х гг. [3]. Согласно этой концепции, выбор управляющих воздействий сводится к адекватной оценке состояния объекта и среды, отнесению текущей ситуации к одному из типовых классов и выбору варианта управления из определённого набора альтернатив, приводящего к достижению целевой ситуации. В отличие от традиционного применения концепции к оперативному управлению авторы предложили её адаптацию к стратегическому управлению в энергетике [4].

Для реализации концепции ситуационного управления разработан комплекс методов семантического моделирования:

- онтологическое моделирование для управления знаниями и описания ситуаций;
- когнитивное моделирование для анализа влияний факторов и моделирования угроз;
- событийное моделирование на основе Joiner-сетей для прогнозирования развития экстремальных ситуаций;
- вероятностное моделирование с использованием байесовских сетей доверия для оценки рисков [5].

Эти методы активно используются при интеграции цифровых двойников и многоагентной интеллектуальной среды. Современные тренды цифровизации, в частности технологии цифровых двойников (ЦД), позволили модифицировать архитектуру интеллектуальной системы поддержки принятия решений. Предложена модифицированная архитектура многоагентной интеллектуальной среды (МАИС), интегрирующая цифровые двойники объектов энергетики и «умные» цифровые

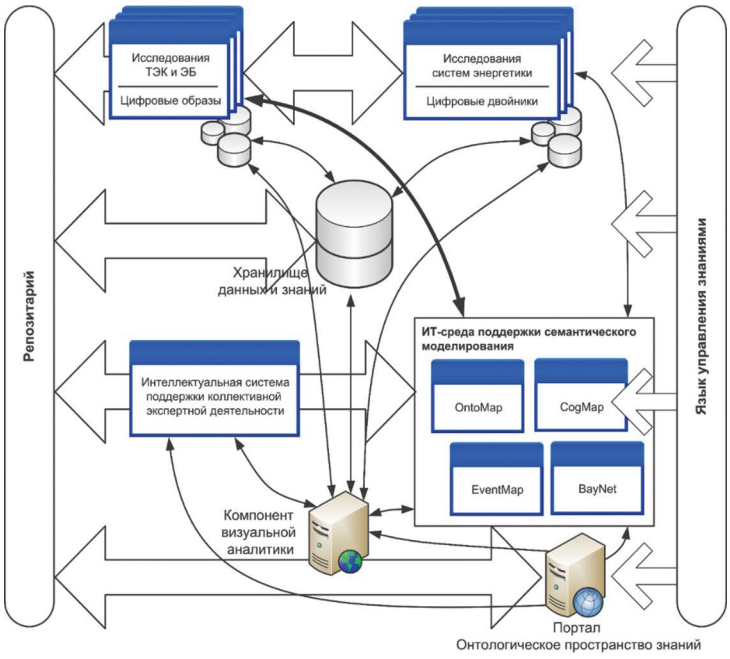


Рис. 1. *Модифицированная архитектура многоагентной интеллектуальной среды с использованием цифровых двойников и цифровых образов*

двойники (цифровые образы) на уровне систем и топливно-энергетического комплекса (ТЭК) (рис. 1).

Под «умным» цифровым двойником (УЦД) предлагается понимать цифровой двойник, ядро которого — математические, имитационные, информационные и онтологические модели — дополнено интеллектуальными моделями, в первую очередь семантическими. Целесообразно использовать классические ЦД на уровне отдельных объектов (например подстанций), УЦД — на уровне систем энергетики, а на уровне ТЭК требуется разработка полноценных цифровых образов с элементами искусственного интеллекта [6].

Бионические модели выбора управляющих воздействий

Для повышения эффективности ситуационного управления разработаны бионические модели выбора управляющих воздействий, основанные на синтезе информационного метода обобщённого показателя (I), искусственных нейронных сетей (ИНС) и генетических алгоритмов (ГА) [7]. Ключевой особенностью является новый принцип представления данных в хромосоме генетического алгоритма.

При явном представлении управляющего воздействия хромосома строится из генов-векторов логических переменных, определяющих наличие или отсутствие конкретных управляющих воздействий. Информация о типе воздействия подаётся на вход нейронной сети одновременно с данными о состоянии объекта.

При неявном представлении каждый ген являет собой вектор весовых коэффициентов модели, описывающей эффект одного управляющего воздействия. Хромосома формируется из «банка» обученных моделей, что позволяет расширить функциональные возможности генетического алгоритма за счёт многомерного представления данных.

Для генерации данных в условиях недостатка измерений от датчиков реализованы генеративно-состязательные сети (GAN) и вариационные автоэнкодеры с использованием предварительно обученных моделей (Transfer Learning — Xception), что позволило успешно синтезировать данные для обучения нейросетевых моделей [8].

Киберситуационная осведомлённость энергетических объектов

В проекте развивалось новое для отечественной науки направление — киберситуационная осведомлённость (КСО), представляющее собой синтез исследований кибербезопасности и ситуационной осведомлённости [9]. Под КСО энергетических объектов понимается осведомлённость о состоянии киберсреды, включающая информацию о критических уязвимостях, киберугрозах и техногенных угрозах энергетической безопасности, вызванных кибератаками.

Разработан интеллектуальный программный комплекс (ИПК) ОКО (Оценка Киберситуационной Осведомлённости), включающий три компонента:

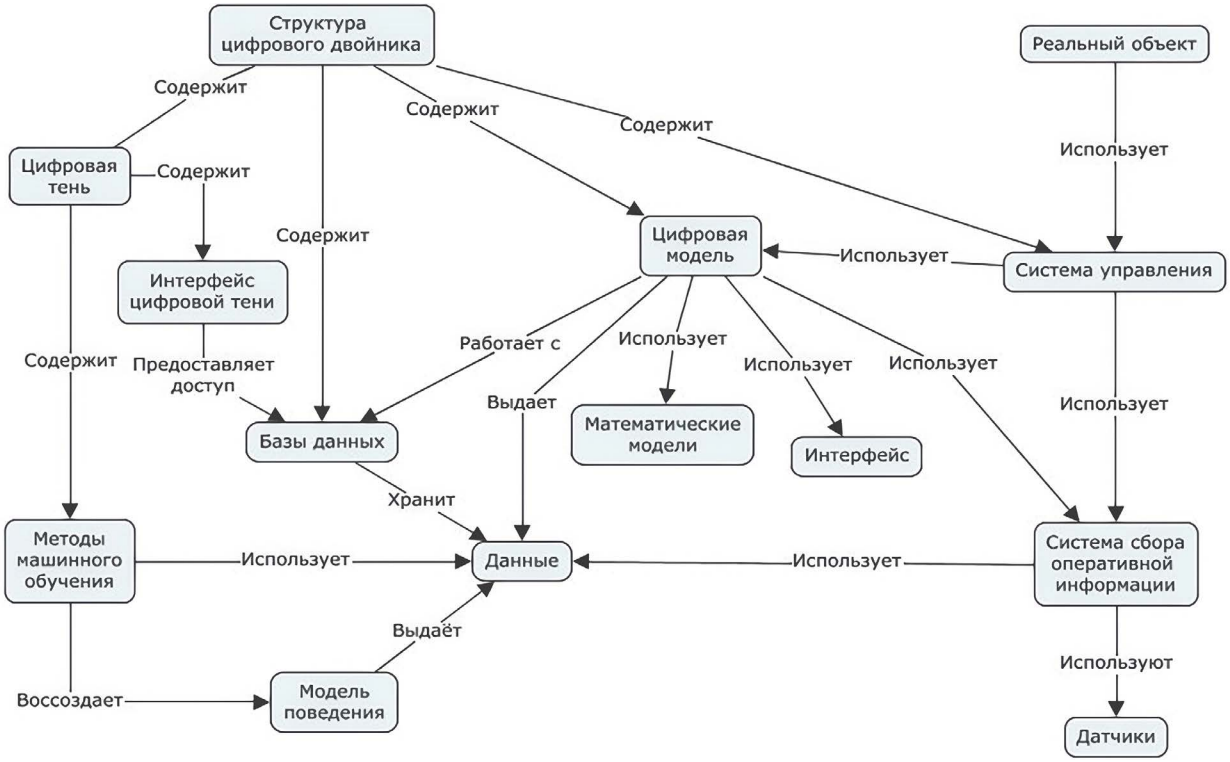


Рис. 2. *Архитектура цифрового двойника солнечной электростанции*

- экспертную систему «Cyber» для формирования векторов атак на критическую информационную инфраструктуру;
- компонент «ThreatNet» для моделирования сценариев нарушения кибербезопасности на основе байесовских сетей;
- компонент «RiskMap» для визуальной оценки рисков с использованием когнитивной графики [10].

Результаты апробации методологии

В рамках проекта реализованы научные прототипы ключевых компонентов МАИС:

- *Прототип цифрового двойника солнечной электростанции*, включающий онтологическую модель фотоэлектрической системы, вычислительное ядро и базу данных (получено свидетельство о регистрации № 2021681401 от 21.12.2021) (рис. 2);
- *Программный комплекс ИНТЭК-А* как умный цифровой двойник ТЭК с агентно-сервисной архитектурой (рис. 3), включающий семь специализированных агентов: формирования сценариев, информационных моделей, мер, классификации угроз, вычислительный, взаимодействия с БД и семантического моделирования [11];
- *Интеллектуальный программный комплекс ОКО* для анализа киберситуационной осведомлённости, прошедший апробацию на примерах анализа угроз критической информационной инфраструктуры энергетики.

Проведены вычислительные эксперименты по оценке влияния угроз энергетической безопасности (например «Недостаток инвестиций») на надёжность энергоснабжения с использованием двухуровневой технологии: качественного анализа на основе когнитивных моделей и количественного анализа с применением экономико-математических моделей оптимизации развития ТЭК.

Заключение

Разработанная методология научного обоснования стратегических решений

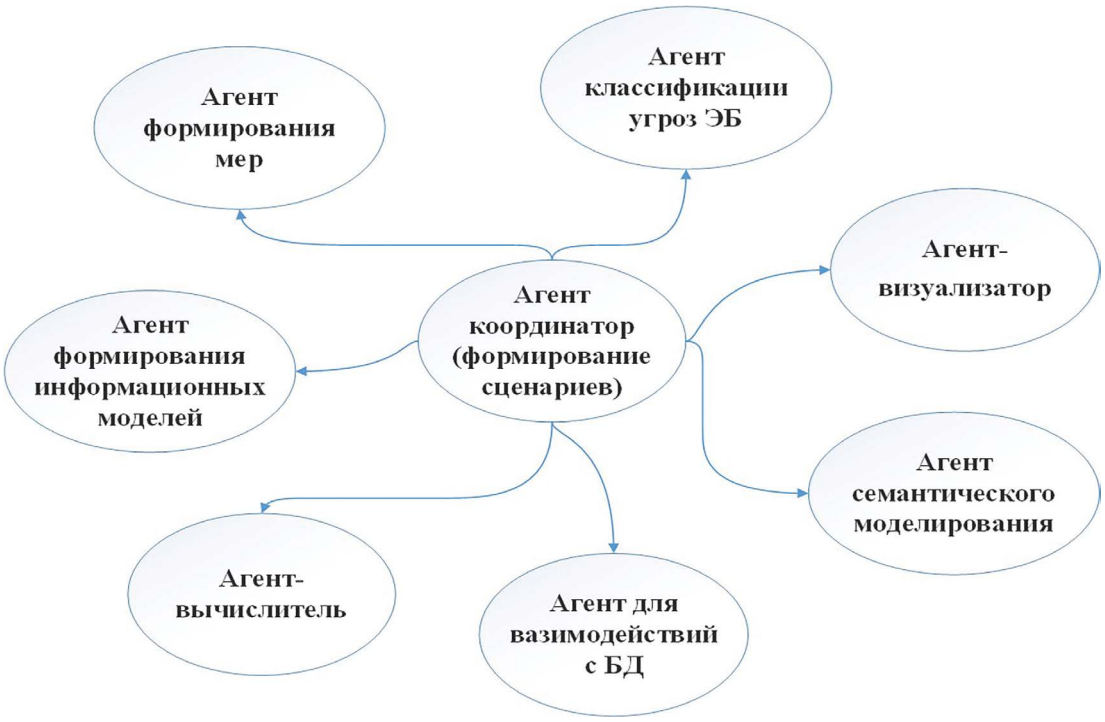


Рис. 3. *Агентно-сервисная архитектура программного комплекса «ИНТЭК-А»*

по цифровой трансформации энергетики обеспечивает интеграцию современных интеллектуальных технологий с концепцией ситуационного управления.

Ключевые результаты проекта:

1. Предложена модифицированная архитектура многоагентной интеллектуальной среды, интегрирующая цифровые двойники объектов и «умные» цифровые двойники систем энергетики.
2. Разработаны бионические модели выбора управляющих воздействий с новым принципом представления данных в генетических алгоритмах.
3. Сформирована методология киберситуационной осведомлённости как инструмента повышения защищённости цифровой энергетики.
4. Созданы научные прототипы инструментальных средств (ЦД солнечной электростанции, ИНТЭК-А, ИПК ОКО), прошедшие апробацию на реальных задачах обоснования стратегических решений.

Перспективы дальнейших исследований связаны с развитием методов интеграции цифровых двойников в единую экосистему «Интернет энергии», с расширением применения методов машинного обучения для прогнозирования развития критических ситуаций и созданием технологий перехода от научных прототипов цифровых двойников к их промышленному внедрению.

ЛИТЕРАТУРА

1. Массель Л.В., Массель А.Г. Интеллектуальная поддержка принятия решений по оценке влияния энергетики на геоэкологию с учётом качества жизни // Труды Международного научно-технического конгресса «Интеллектуальные системы и информационные технологии – 2019» : науч. изд. : в 2 т. Т. 1. Таганрог: Изд-во Ступина, 2019. С. 207–216.
2. Массель Л.В., Ворожцова Т.Н., Пяткова Н.И. Онтологический инжиниринг для поддержки принятия стратегических решений в энергетике // Онтология проектирования. 2017. Т. 7, № 1 (23). С. 66–76.

3. Поспелов Д.А. Ситуационное управление. Теория и практика. М.: Наука, 1986. 288 с.
4. Пяткова Н.И., Массель Л.В., Массель А.Г. Методы ситуационного управления в исследованиях проблем энергетической безопасности // Известия Российской академии наук. Энергетика. 2016. № 4. С. 156–163.
5. Массель Л.В., Массель А.Г. Семантические технологии на основе интеграции онтологического, когнитивного и событийного моделирования // Материалы международной научно-технической конференции «OSTIS-2013». Минск: БГУИР, 2013. С. 247–250.
6. Массель Л.В. Построение цифровых двойников ветровой и солнечной электростанций на основе онтологического подхода / Л.В. Массель, А.Г. Массель, Н.И. Щукин [и др.] // Автоматизация в промышленности. 2022. № 7. С. 28–32. DOI: 10.25728/avtprom.2022.07.04.
7. Use of semi-synthetic data for catheter segmentation improvement / V.V. Danilov, D.Yu. Kolpashchikov, O. M. Gerget [et al.] // Computerized Medical Imaging and Graphics. 2023. Vol. 106. P. 102188. DOI: 10.1016/j.compmedimag.2023.102188.
8. Laptev V.V., Gerget O.M., Markova N.A. Generative Models Based on VAE and GAN for New Medical Data Synthesis // Society 5.0: Cyberspace for Advanced Human-Centered Society. Cham: Springer, 2021. P. 217–226. DOI: 10.1007/978-3-030-63563-3_17.
9. Гаськова Д.А., Массель А.Г. Методы анализа киберситуационной осведомлённости об энергетических объектах // Вопросы кибербезопасности. 2021. № 2 (27). С. 45–59.
10. Massel A.G., Gaskova D.A. Methods to analyze critical facilities in energy with regard to cyber threats // Proceedings of the Vth International workshop «Critical infrastructures». 2018. P. 102–109.
11. Массель А.Г., Мамедов Т.Г., Пяткова Н.И. Технология вычислительного эксперимента в исследованиях работы энергетических отраслей при реализации угроз энергетической безопасности // Информационные и математические технологии в науке и управлении. 2021. № 3 (23). С. 62–73. DOI: 10.38028/ESI.2021.23.3.006.

Methodology for the Scientific Substantiation of Strategic Decisions on the Digital Transformation of the Energy Sector Based on Situational Management and Digital Twins

Liudmila Vasilievna Massel — Doctor of Technical Sciences, Head of Department of Artificial Intelligence Systems in the Energy Sector, Melentiev Energy Systems Institute of Siberian Branch of Russian Academy of Sciences (MESI SB RAS).
E-mail: massel@isem.irk.ru

Aleksei Gennadievich Massel — Candidate of Technical Sciences, Senior Researcher, Department of Artificial Intelligence Systems in the Energy Sector, Melentiev Energy Systems Institute of Siberian Branch of Russian Academy of Sciences (MESI SB RAS).
E-mail: amassel@isem.irk.ru

The article presents a developed methodology for scientific substantiation of strategic decisions on digital transformation of energy industry based on the synthesis of D.A. Pospelov's situational management concept and modern intelligent technologies. The necessity of integrating semantic modeling (ontological, cognitive, event-based and probabilistic), machine learning methods (deep neural networks and genetic algorithms) and digital twin technologies for solving strategic planning tasks under uncertainty is substantiated. The architecture of a multi-agent intelligent environment (MAIE) is proposed, ensuring interaction between digital twins of energy objects and "smart" digital twins (digital shadows) at the level of systems and fuel-energy complex. Bionic models for selecting control actions have been developed, combining information methods, neural networks and genetic algorithms with explicit and implicit representation of control actions.

Methods of cyber-situational awareness as a synthesis of cybersecurity and situational awareness research are considered. The results of methodology approbation are presented on the examples of creating a prototype digital twin of a solar power plant and reengineering of the INTEK-A software complex as a smart digital twin of the fuel-energy complex. The methodology allows increasing the validity of strategic decisions through integration of qualitative analysis based on semantic models and quantitative analysis using economic-mathematical models while taking into account cybersecurity requirements and ensuring the resilience of energy systems.

Keywords: digital transformation of energy industry, situational management, semantic modeling, digital twin, cybersecurity, multi-agent intelligent environment, strategic decisions, resilience of energy systems, machine learning, genetic algorithms, cyber-situational awareness, ontological engineering, bionic models, smart digital twin

REFERENCES

1. Massel L.V., Massel A.G. Intellektualnaya podderzhka prinyatiya resheniy po otsenke vliyaniya energetiki na geoekologiyu s uchetom kachestva zhizni // Trudy Mezhdunarodnogo nauchno-tekhnicheskogo kongressa «Intellektualnye sistemy i informatsionnye tekhnologii — 2019» : nauch. izd. : v 2 t. T. 1. Taganrog: Izd-vo Stupina, 2019. S. 207–216 (in Russian).
2. Massel L.V., Vorozhtsova T.N., Pyatkova N.I. Ontologicheskiy inzhiniring dlya podderzhki prinyatiya strategicheskikh resheniy v energetike // Ontologiya proektirovaniya. 2017. T. 7, № 1 (23). S. 66–76 (in Russian).
3. Pospelov D.A. Situatsionnoe upravlenie. Teoriya i praktika. M.: Nauka, 1986. 288 s. (in Russian)
4. Pyatkova N.I., Massel L.V., Massel A.G. Metody situatsionnogo upravleniya v issledovaniyakh problem energeticheskoy bezopasnosti // Izvestiya Rossiyskoy akademii nauk. Energetika. 2016. № 4. S. 156–163 (in Russian).
5. Massel L.V., Massel A.G. Semanticheskie tekhnologii na osnove integratsii ontologicheskogo, kognitivnogo i sobytiynogo modelirovaniya // Materialy mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «OSTIS-2013». Minsk: BGUIR, 2013. S. 247–250 (in Russian).
6. Massel L.V. Postroenie tsifrovykh dvoynikov vetrovoy i solnechnoy elektrostantsiy na osnove ontologicheskogo podkhoda / L.V. Massel, A.G. Massel, N.I. Shchukin [et al.] // Avtomatizatsiya v promyshlennosti. 2022. № 7. S. 28–32. DOI: 10.25728/avtprom.2022.07.04 (in Russian)
7. Use of semi-synthetic data for catheter segmentation improvement / V.V. Danilov, D.Yu. Kolpashchikov, O.M. Gerget [et al.] // Computerized Medical Imaging and Graphics. 2023. Vol. 106. P. 102188. DOI: 10.1016/j.compmedimag.2023.102188.
8. Laptev V.V., Gerget O.M., Markova N.A. Generative Models Based on VAE and GAN for New Medical Data Synthesis // Society 5.0: Cyberspace for Advanced Human-Centered Society. Cham: Springer, 2021. P. 217–226. DOI: 10.1007/978-3-030-63563-3_17.
9. Gaskova D.A., Massel A.G. Metody analiza kibersituatsionnoy osvedomlennosti ob energeticheskikh obektakh // Voprosy kiberbezopasnosti. 2021. № 2 (27). S. 45–59 (in Russian).
10. Massel A.G., Gaskova D.A. Methods to analyze critical facilities in energy with regard to cyber threats // Proceedings of the Vth International workshop «Critical infrastructures». 2018. P. 102–109.
11. Massel A.G., Mamedov T.G., Pyatkova N.I. Tekhnologiya vychislitelnogo eksperimenta v issledovaniyakh raboty energeticheskikh otrasley pri realizatsii ugroz energeticheskoy bezopasnosti // Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii. 2021. № 3 (23). S. 62–73. DOI: 10.38028/ESI.2021.23.3.006 (in Russian).

Images

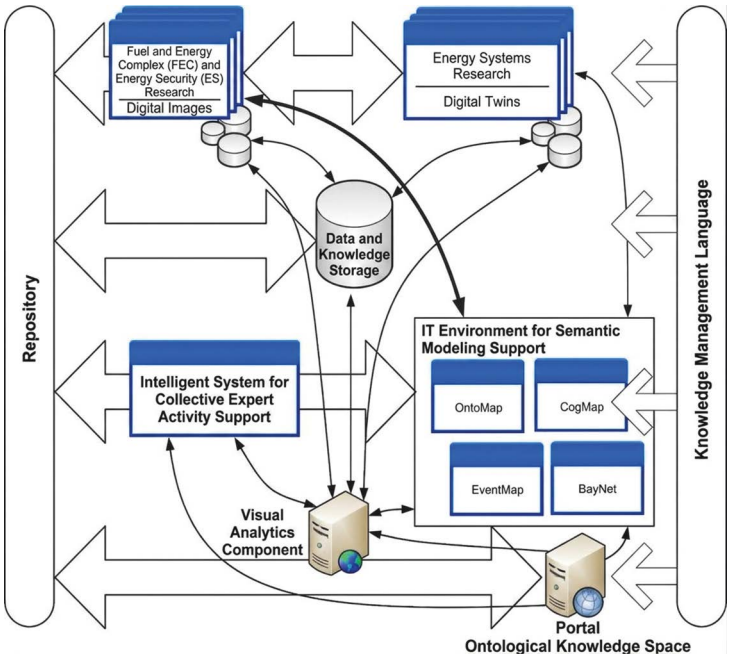


Fig. 1. *Modified architecture of a multi-agent intelligent environment utilizing digital twins and digital images*

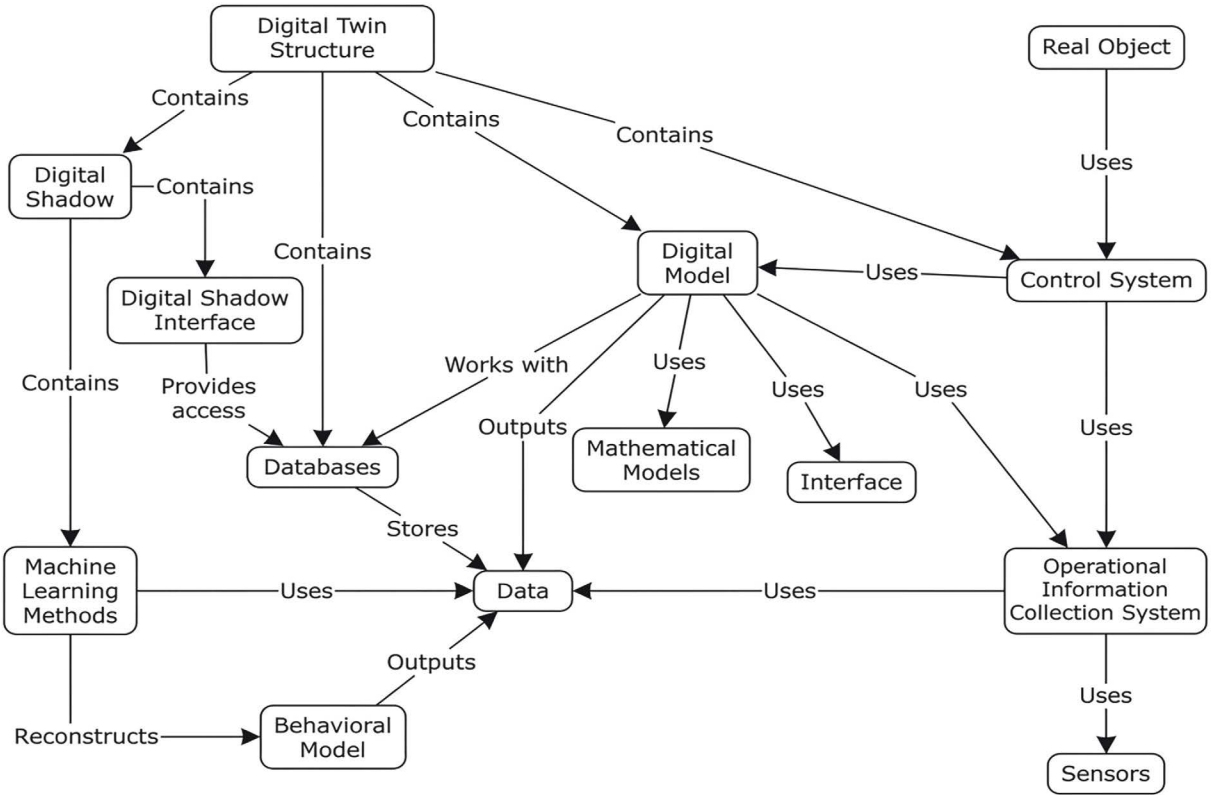


Fig. 2. *Architecture of the digital twin of a solar power plant*

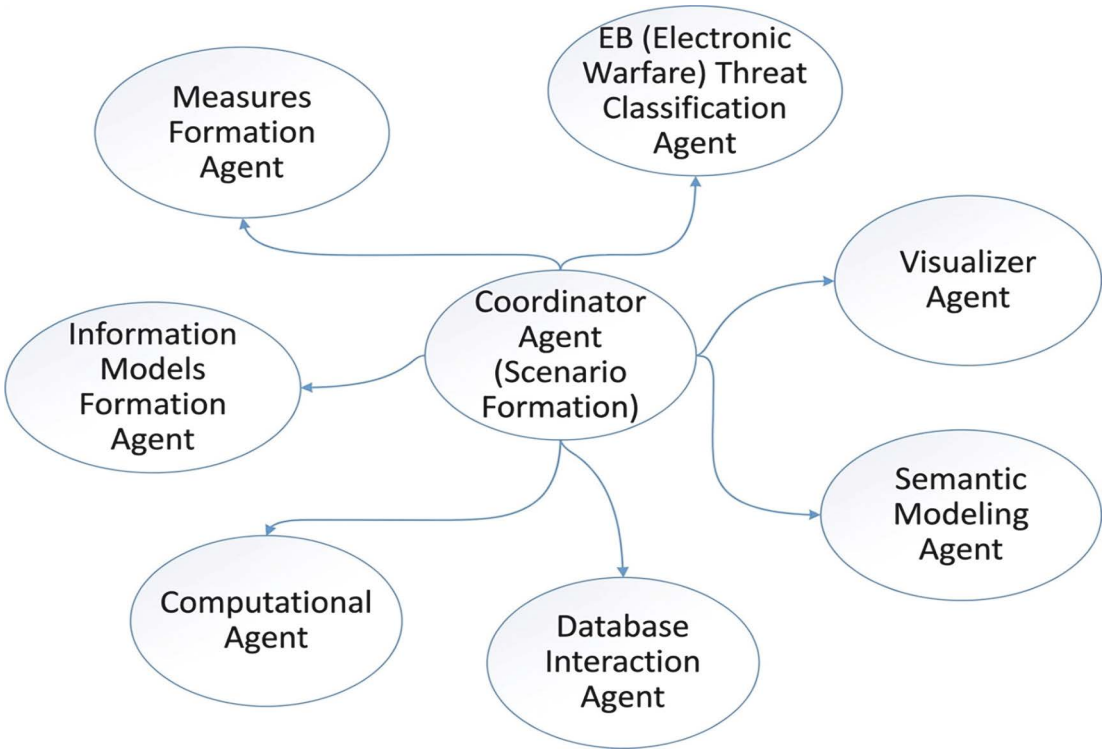


Fig. 3. *Agent-Service Architecture of the «INTEK-A» Software Complex*

Индекс УДК 621.396.93:621.391.8
Код ГРНТИ 28.23.21
DOI: 10.22204/2410-4639-2026-129-01-25-42

А.А. КАРПУК,
П.А. КОХНО*

Модели показателей и параметров качества услуг сотовой связи

В статье определены показатели и параметры качества услуг в сетях стандартов 4G и 5G. Качество обслуживания пользователя зависит от показателей работы самой сети, а также от внешних факторов. Сетевой сервис сети связи описывается параметрами работы оборудования связи на трёх уровнях модели OSI. По своей функциональности значение каждого показателя является компромиссной функцией между обеспечением качества услуги связи и затратами на это обеспечение. Описанные показатели качества относятся к любым сетям связи, в том числе к сетям с коммутацией каналов и коммутацией пакетов. Количественные (объёмные) показатели разделены по зонам ответственности между оператором и пользователем услуг связи. Предложена четырёхуровневая модель параметров качества обслуживания.

Ключевые слова: сотовая связь, показатели, параметры, услуги, модели, трафик, сетевой сервис, стандарты, коммутация каналов, коммутация пакетов

Введение

В своём послании Федеральному собранию 1 декабря 2016 г. Президент РФ предложил «запустить масштабную системную программу развития экономики» [1]. Следом за предложением Президента РФ в декабре 2016 г. была опубликована Стратегия развития информационного общества в России на 2017–2030 годы, где впервые даётся определение цифровой экономики как деятельности, «в которой ключевыми факторами производства являются данные, представленные в цифровом виде, а их обработка и использование в больших объёмах, в том числе их образования, позволяет по сравнению с традиционными формами хозяйствования существенно повысить эффективность, качество и производительность в различных видах производства при хранении, продаже, доставке и потребления товаров и услуг» [2,

* **Карпук Анатолий Алексеевич** — доцент, кандидат технических наук, профессор кафедры программного обеспечения сетей телекоммуникаций Белорусской государственной академии связи.
E-mail: a_karpuk@mail.ru

Кохно Павел Антонович — профессор, доктор экономических наук, заместитель директора по науке Автономной некоммерческой организации «Содействие и развитие инноваций в научно-производственной сфере» г. Москва, АНО «Содействие и развитие инноваций в научно-производственной сфере».
E-mail: pavelkohno@mail.ru

с. 3/17]. Стратегия формулирует понятие «информационное общество» следующим образом: «информационное общество — общество, в котором информация и уровень её применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан» [2, с. 2/17]. То есть, это индустриальное общество в новой исторической фазе развития цивилизации, в которой главными производствами являются информация и её высшая форма знания.

Для реализации Стратегии, утверждённой Указом Президента Российской Федерации от 9 мая 2017 г. № 203, и программы «Цифровая экономика Российской Федерации», принятой распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р, перед отечественными промышленными предприятиями, большинство которых сосредоточено в оборонно-промышленном комплексе, стоит задача развития методов и механизмов их функционирования в условиях внедрения цифровых технологий в процессы производства и управления.

Кроме того, Основы государственной политики в области развития оборонно-промышленного комплекса Российской Федерации на период до 2025 года и дальнейшую перспективу, утверждённые Президентом Российской Федерации от 23 февраля 2017 г. № 91, и Основы военно-технической политики Российской Федерации на период до 2020 года и дальнейшую перспективу, утверждённые Указом Президента Российской Федерации от 24 апреля 2016 г., предусматривают в числе основных задач создание информационно-аналитических и справочных систем на основе современных цифровых технологий, требующих развития существующих и создания новых механизмов функционирования предприятий при внедрении цифровых технологий в процессы их постоянного взаимодействия с вышестоящими органами управления. Поэтому именно сейчас нужно включаться в общий информационный и технологический поток обновлений и стараться эффективно их применить. В России есть возможности для совершения технологического прогресса во многих сферах деятельности. Сейчас России важно выстроить собственные приоритетные ниши для цифровых инноваций, где с наименьшими затратами можно не только добиться самостоятельности на внутреннем рынке, но и стать признанным мировым лидером, в том числе в цифровом оборонном производстве. Одна из приоритетных ниш в области цифровых инноваций — это последовательное развитие мобильной сотовой связи.

Основная часть

С начала 2000-х годов начался запуск сетей сотовой связи третьего поколения (3G) стандарта UMTS с широкополосным кодовым доступом с базовыми радиоинтерфейсами WCDMA и HSPA. Эти сети изначально проектировались для передачи мультимедиа, видео и высокоскоростного Интернета. Первая в мире сеть сотовой связи стандарта UMTS была запущена в 2001 г. фирмой NTT DoCoMo в Японии. В 2010-х годах начался массовый запуск сетей сотовой связи четвёртого поколения (4G) стандарта LTE с полностью пакетным обменом данными по протоколу IP. Первая в мире коммерческая сеть сотовой связи стандарта LTE была запущена в декабре 2009 г. фирмой TeliaSonera в Швеции и Норвегии. Первым российским оператором, запустившим коммерческую сеть стандарта LTE в декабре 2012 г. в Москве, был МегаФон. В июне 2018 г. компания Elisa (Финляндия) первой в мире запустила в городах Тампере (Финляндия) и Таллинн (Эстония) коммерческую сеть сотовой связи пятого поколения (5G) стандарта IMT-2020. В марте 2021 г. оператор МТС запустил в Москве первую в России «пилотную» 5G-зону, доступную обычным пользователям с поддержкой 5G-смартфонов [3, с. 7].

В англоязычной литературе понятие «качество обслуживания в сети связи» имеет устоявшуюся аббревиатуру QoS (Quality of Service). Определение терминов, отно-

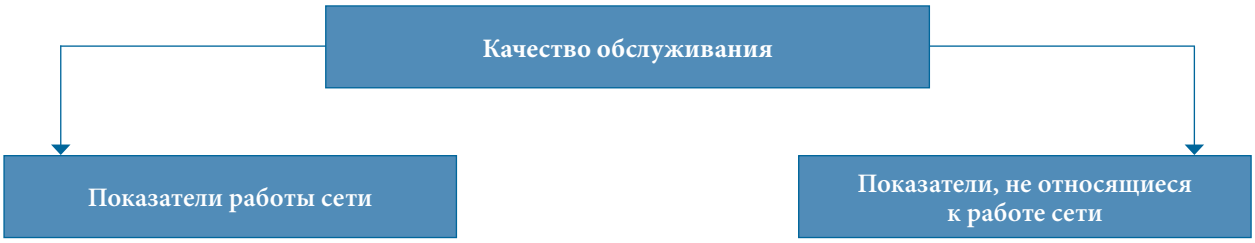


Рис. 1. *Общий состав показателей качества обслуживания*

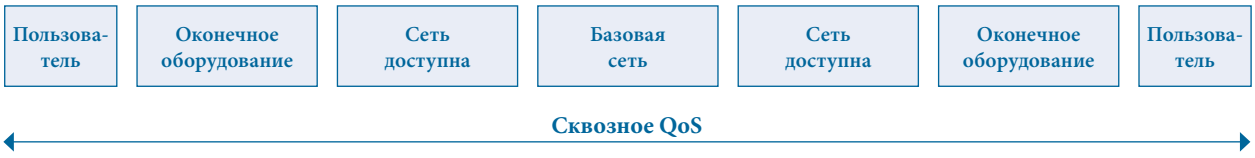


Рис. 2. *Схематическое представление компонентов сквозного QoS*

сящихся к качеству обслуживания в сетях связи, приведено в Рекомендации МСЭ-Т E.800 [4], первая редакция которой была опубликована в 1988 г., а последняя редакция — в 2008 г.

Качество обслуживания пользователя при предоставлении услуги связи в общем случае определяется не только показателями работы самой сети, но и зависит от внешних факторов, схематически это представлено на рис. 1.

Часть показателей качества обслуживания характеризует качество работы технических элементов сети связи, и при этом присутствуют показатели, которые не относятся непосредственно к работе сети, но характеризуют качество обслуживания пользователя услуги связи со стороны оператора связи. В Рекомендации МСЭ-Т E.800 показано, что QoS на пути передачи трафика между пользователями услуги связи определяется вкладами сетевых компонентов. Схематическое представление компонентов QoS приведено на рис. 2.

В связи с большим количеством компонентов сети связи, задействованных в обеспечении качества услуги связи, в Рекомендации МСЭ X.140 [5] выделены составляющие QoS, зависящие непосредственно от качества работы сети связи, качества работы оконечного сетевого оборудования и установленного на нём ПО, и отделена субъективная составляющая пользовательской оценки качества услуги связи.

Разделение оценок QoS на составляющие в зависимости от уровня модели OSI, на котором происходит обеспечение QoS, представлено на рис. 3.

Сетевой сервис сети связи описывается параметрами работы оборудования связи на 1–3 уровнях модели OSI. Для исключения путаницы в понятиях QoS в Рекомендации ITU-T I.350 [6] и Техническом отчёте ETSI TR 102 643 [7] введены уточняющие наименования для оценок качества в соответствии с границами их действия:

- качество функционирования сети NP (Network Performance) — как способность сети или её участка/сегмента обеспечить выполнение функций связи, т.е. обеспечивать сетевой сервис на 1–3 уровнях модели OSI;
- качество предоставления услуги/сервиса QoS (Quality of Service) — характеристика телекоммуникационного сервиса как степень удовлетворения пользователя услугой связи;
- качество восприятия услуги QoE (Quality of Experience) — результат суждения о восприятии общей сущности относительно желаемого восприятия прикладного сервиса с точки зрения конечного

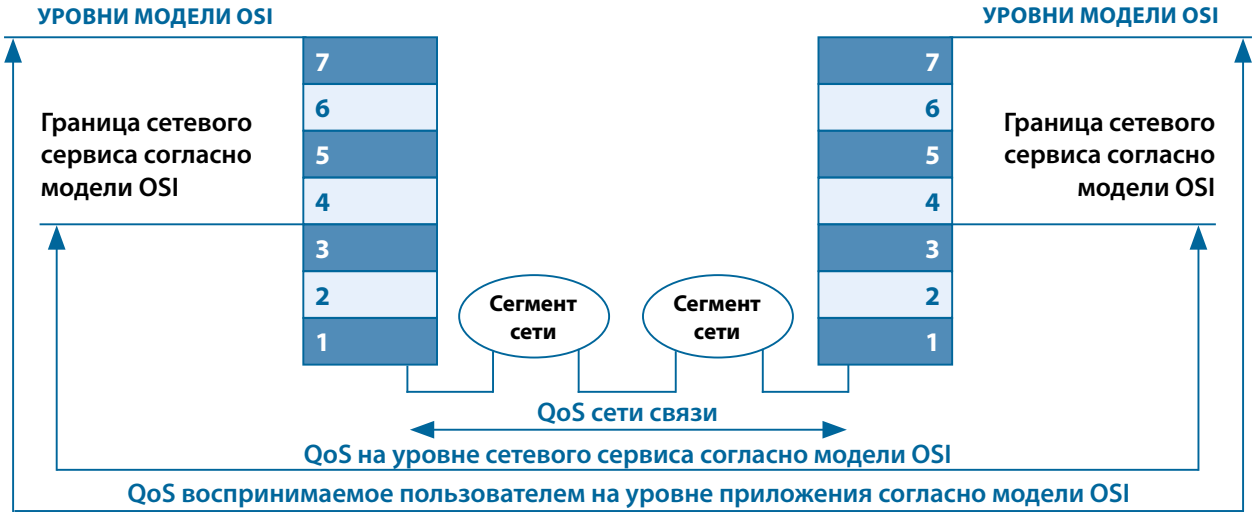


Рис. 3. *Разделение показателей QoS по уровням модели OSI*

пользователя. Области действия групп показателей качества услуг связи показаны на рис. 4.

По своей функциональности значение каждого показателя QoE является компромиссной функцией между обеспечением качества услуги связи и затратами на это обеспечение. Взаимосвязь значений QoS и QoE с экономическими показателями работы сети связи подтверждает важность вопроса обеспечения QoS для услуг связи на сети оператора. В современных сетях связи оценка качества услуг связи производится с использованием сквозной оценки качества, представленной на рис. 5.

Распределение показателей NP, QoS и QoE по уровням оценки качества услуг связи показано на рис. 6. Описанные показатели качества относятся к любым сетям связи, в том числе к сетям с коммутацией каналов и коммутацией пакетов. Сети сотовой подвижной электросвязи стандартов LTE и IMT-2020 (5G) относятся к сетям с коммутацией пакетов. Принципиальные отличия сетей с коммутацией пакетов от сетей с коммутацией каналов приведены в таблице 1.

Из таблицы 1 видно, что для сетей, построенных по технологии коммутации пакетов, требуются показатели качества, ко-

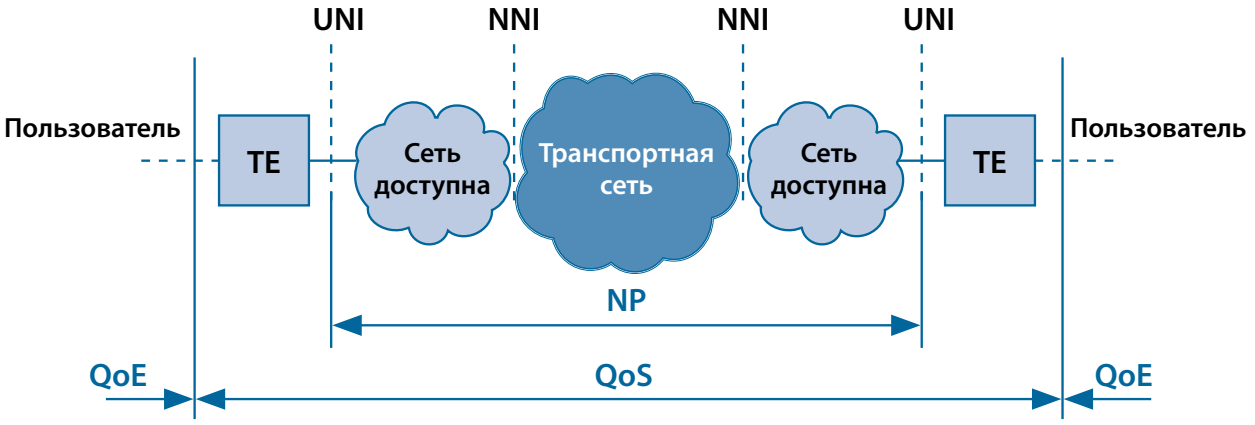


Рис. 4. *Области действия групп показателей качества услуг связи*

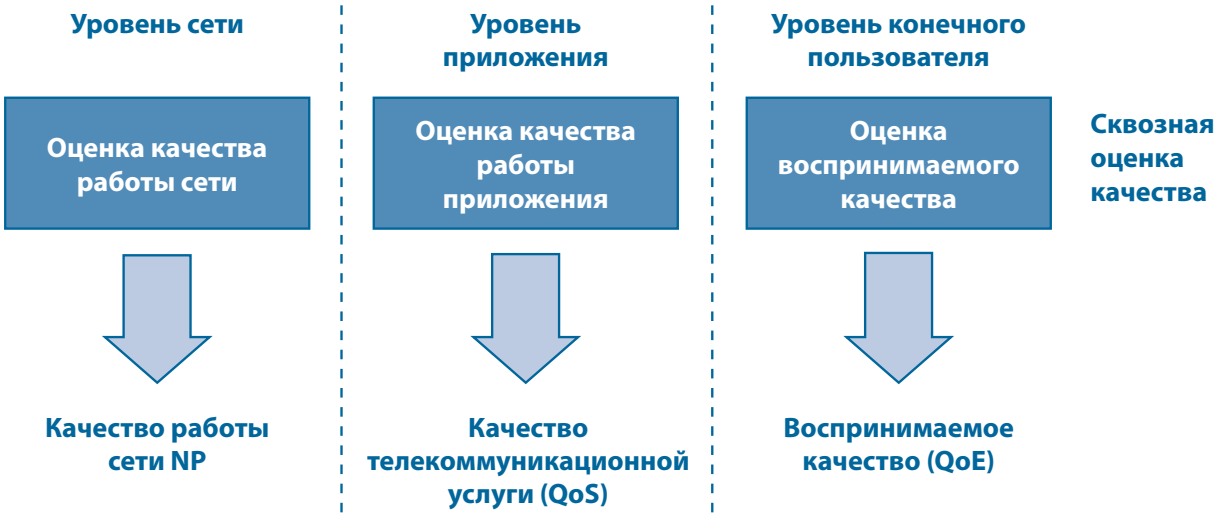


Рис. 5. *Оценка сквозного качества услуги связи*

торые описывают только процесс передачи трафика. Для сетей, построенных по технологии коммутации каналов, дополнительно требуются показатели, описывающие процесс установления соединений и разбора соединения после передачи данных. При этом для сетей, построенных по технологии коммутации пакетов, при описании процесса передачи данных требуются показатели, отражающие качество работы пакетных очередей/буферов и влияние возможности изменения маршрута передачи пакетов данных от отправителя к получателю.

Для сетей с коммутацией пакетов активное сетевое оборудование разделяется на 2 основные категории с учётом выполнения ими функций по передаче пакетных данных согласно модели OSI: коммутаторы и маршрутизаторы. Коммутаторы и маршрутизаторы работают на 2 и 3 уровнях модели OSI с использованием соответствующих протоколов передачи данных. С учётом того,

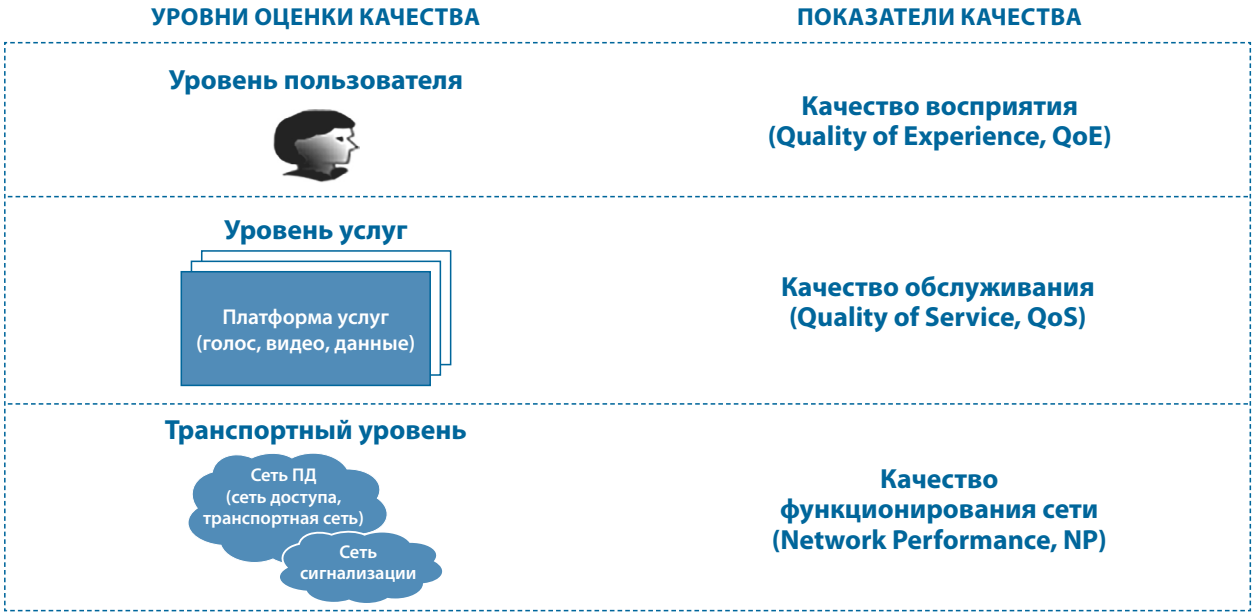


Рис. 6. *Распределение показателей качества услуг связи по технологическим системам*

Таблица 1

Отличия сетей с коммутацией пакетов от сетей с коммутацией каналов

Сетевая функция	Сети с коммутацией каналов	Сети с коммутацией пакетов
Установление соединения	Необходимо предварительно устанавливать соединение	Отсутствует этап установления соединения (дейтаграммный способ)
Порядок выделения ресурсов	Ресурсы предоставляются в соответствие с порядком поступления запроса	Ресурсы предоставляются одновременно по всем запросам при условии, что требуемая для них суммарная полоса пропускания не превосходит возможности канала связи
Передача адреса получателя	Адрес требуется только на этапе установления соединения	Адрес и другая служебная информация передаются с каждым пакетом
Доступность сетевого обслуживания для пользователя	Сеть может отказать пользователю в установлении соединения	Сеть всегда готова принять данные от пользователя
Гарантия пропускной способности	Гарантированная пропускная способность	В общем случае пропускная способность сети для абонентов заранее неизвестна, возможно гарантированное выделение полосы пропускания
Процедура выделения полосы пропускания для трафика пользователя	Статическая	Динамическая (в общем случае), с возможностью статического выделения
Маршрут передачи пакетного трафика	Данные передаются согласно маршруту прокладки канала внутри сети связи	Решение о дальнейшем маршруте передачи пакета данных принимается отдельно для каждой точки коммутации трафика на пути от отправителя к получателю, в рамках передачи одного информационного сообщения, состоящего из нескольких пакетов данных, каждый пакет может быть передан различным путём
Задержка в передаче трафика в канале связи	Задержка определяется временем прохождения электромагнитного сигнала по каналу связи	Величина задержки зависит от задержки в пакетных очередях/буферах на узлах сети и носит случайный характер
Потери трафика на узлах сети	Практически отсутствуют	Возможны потери данных из-за переполнения пакетных очередей буферов
Эффективность использования канала связи	Низкая (в общем случае)	Высокая
Наилучший тип трафика	С фиксированной скоростью, при передаче пульсирующего трафика значительная часть зарезервированной пропускной способности каналов не используется	Пульсирующий, возможно выделение полосы под трафик с фиксированной скоростью
Приоритетность трафика	Отсутствует	Путём установления признака приоритета и организации различных буферов/очередей для трафика с различным значением признака приоритета
Завершение соединения	Происходит «разбор» соединения с освобождением ресурсов сети	Не требуется
Обеспечение соединения другому набору пользователей услуг связи	Передача высвобожденных сетевых ресурсов для организации соединения в интересах других пользователей услуг связи	Возможно установление соединения в «параллельном» режиме при наличии сетевых ресурсов, удовлетворяющих требованиям запроса пользователя, или динамическое перераспределение сетевых ресурсов при отсутствии жёстких требований к сетевым ресурсам со стороны уже установленных соединений

что показатели NP относятся к элементу сетевого соединения (являются его атрибутами), оценка NP должна производиться на уровне работы сетевого элемента в сети передачи данных. Ввиду того, что основными сетевыми элементами являются коммутаторы и маршрутизаторы, оценка качества передачи пакетов данных в сети

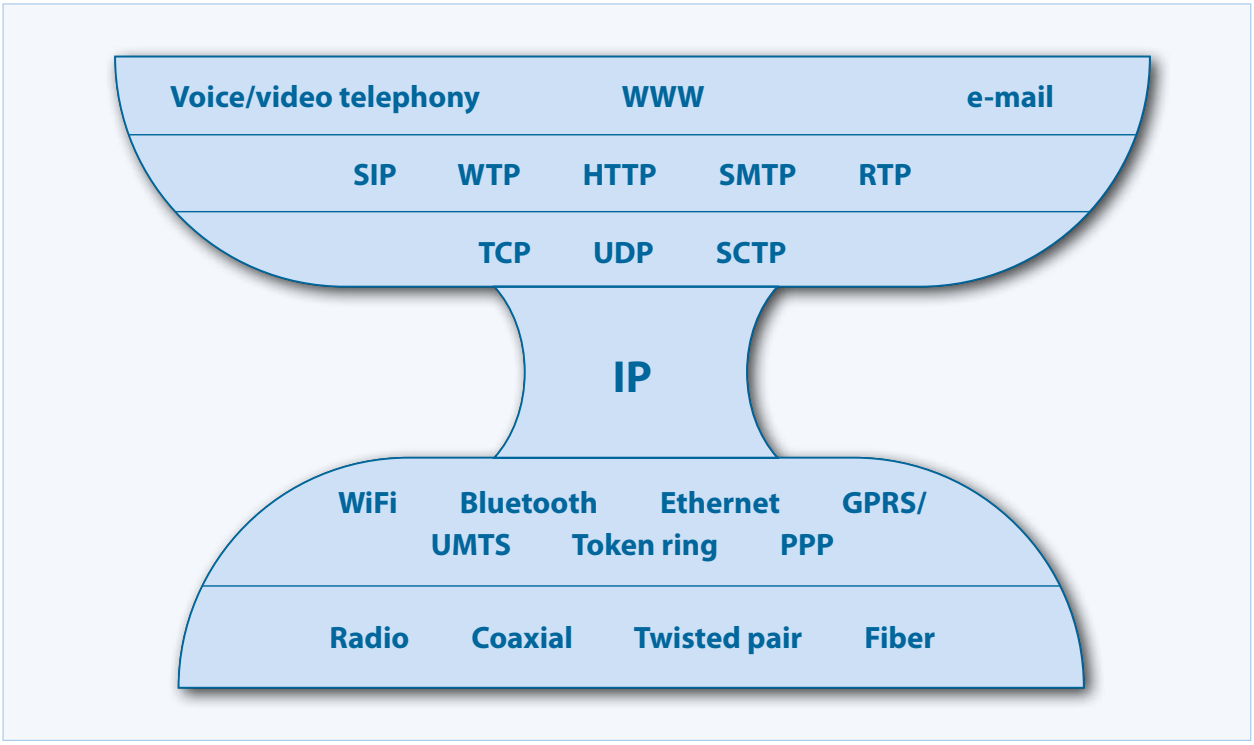


Рис. 7. *Иерархия протоколов сети с коммутацией пакетов*

с коммутацией пакетов должна проводиться для маршрутизаторов на сетевом уровне и для коммутаторов на канальном уровне.

В настоящее время наиболее распространёнными протоколами для обеспечения передачи пакетов данных в сетях с коммутацией пакетов стали протоколы IP (на сетевом уровне) и Ethernet (на канальном уровне). При этом в иерархии модели OSI протокол IP занимает ключевое положение в плане обеспечения обмена данными между отправителем и получателем, т.к. передача пакетов данных происходит на основании адресной информации, содержащейся в IP-заголовке.

Передача пакетов данных на основании адресной информации канального уровня осуществляется только в рамках широковещательных доменов и относится к технологии локальных сетей, которые являются частным случаем при построении сегментов глобальных сетей связи. Иллюстрация ключевого положения протокола IP и его связующей роли представлена на рис. 7 в виде так называемой «модели песочных часов» (HourGlass-model) [8].

Исходя из ключевого положения протокола IP в Рекомендации ITU-T Y.1540 [9] разработаны показатели QoS и NP для сетей передачи данных, построенных с использованием IP-протокола. Показатели NP условно делятся на 2 категории: качественные и количественные (объёмные).

К качественным показателям NP для контроля качества передачи данных между отправителем и получателем относятся:

- величина времени задержки при передаче пакета IPTD (IP-packet Transfer Delay);
- вариация величины времени задержки (джиттер) передачи пакетов IPDV (IP-packet Delay Variation);
- уровень ошибок (доля переданных с ошибкой) пакетов IPER (IP-packet Error Ratio);
- уровень потерь (доля потерянных) пакетов IPLR (IP-packet Loss Ratio);
- уровень нарушения порядка (доля с нарушением порядка следования) пакетов IPRR (IP-packet Reordering Ratio);

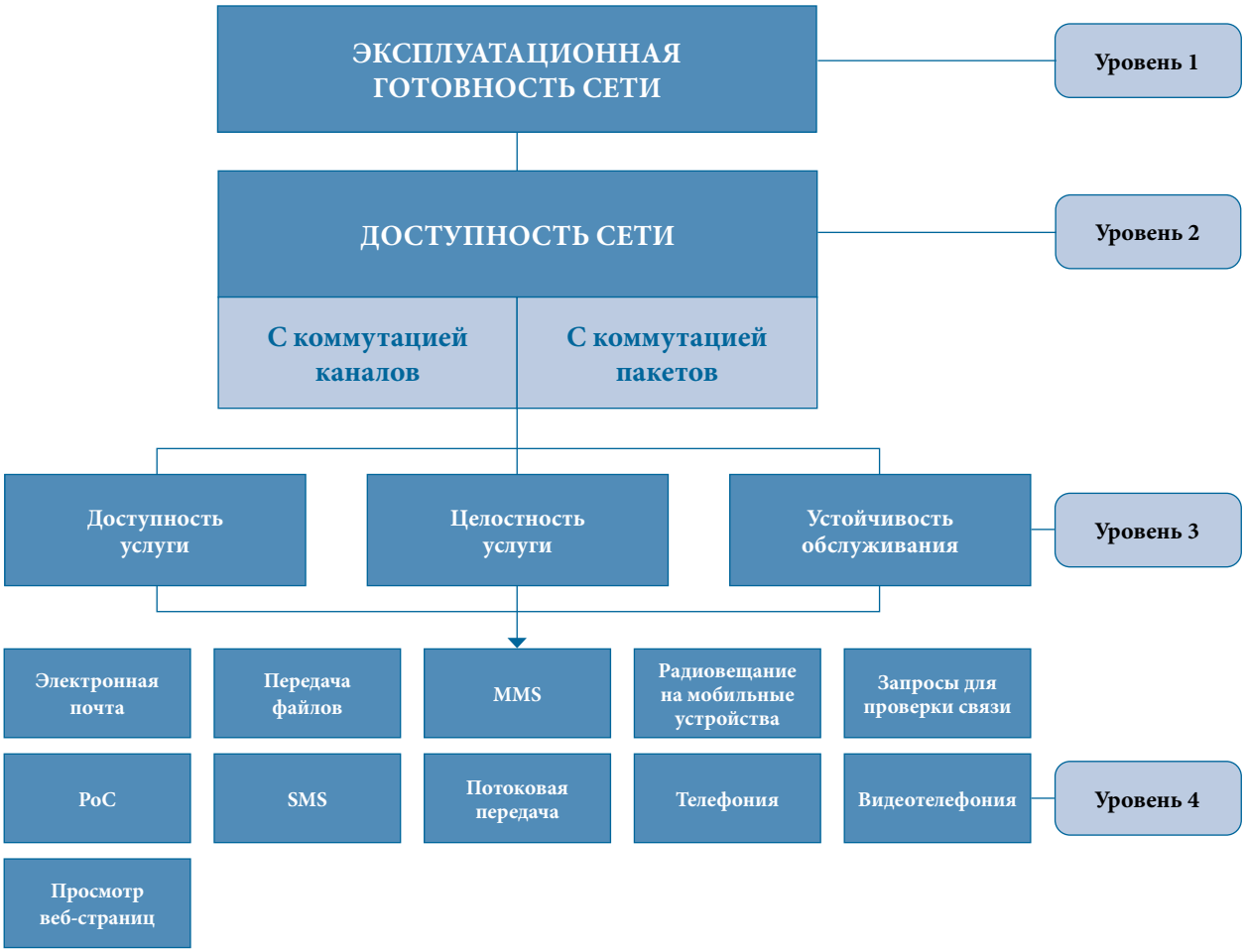


Рис. 8. *Модель параметров качества обслуживания*

- уровень дублирования пакетов IPDupR (IP-packet Duplicate Ratio);
- уровень сброса (доля сброшенных/отказанных в обработке) на сетевом устройстве/элементе пакетов IPDR (IP-packet Discard Ratio).

В качестве количественных (объёмных) показателей NP при передаче данных между двумя соседними сетевыми устройствами, обеспечивающими передачу данных на сетевом уровне модели OSI, рассматриваются:

- ёмкость IP-секции (IP-layer Section Capacity) как наибольшее количество бит, которое может быть передано на сетевом уровне за определённый интервал времени, достаточно часто именуется как полоса пропускания сетевого соединения на сетевом уровне;
- используемая ёмкость IP-секции (IP-layer Used Section Capacity) как количество бит, которое передано на сетевом уровне за определённый интервал времени, достаточно часто именуется как интенсивность пакетного трафика на определённом интервале времени;
- уровень загрузки IP-секции (IP-layer Section Utilization) как относительная величина, равная отношению используемой ёмкости IP-секции к ёмкости IP-секции;
- пакетная скорость при передаче IP-пакетов (IP Packet Rate – IPPR);
- байтовая скорость при передаче IP-пакетов (Octet-based IP packet Rate – IPOR).

Следует иметь в виду, что количественные (объёмные) показатели NP разделены

по зонам ответственности между оператором и пользователем услуг связи. Оператор связи должен гарантировать полосу пропускания сетевого соединения (ёмкость IP-секции). Пользователь услуги связи при передаче или получении пакетного трафика не должен допускать, чтобы интенсивность пакетного трафика (используемая ёмкость IP-секции) превосходила полосу пропускания сетевого соединения. Объём трафика, превышающий ёмкость секции, может быть сброшен или задержан (включая изменение поля приоритетов обработки пакетов данных) со стороны сети оператора связи без отнесения данных потерь на оценку качества работы сетевого соединения [10].

В Рекомендации ITU-T E.804 [11] и Технической спецификации ETSI TS 102 250-2 [12] приводится четырехуровневая модель параметров качества услуг СПЭ (рис. 8).

В модель входят:

- параметры эксплуатационной готовности сети (уровень 1);
- параметры доступности сети (уровень 2);
- параметры доступности услуги, целостности услуги и устойчивости обслуживания (уровень 3);
- параметры качества каждой услуги (уровень 4).

Эксплуатационная готовность сети определяет QoS с точки зрения поставщика, а не потребителя услуги. Доступность сети с точки зрения потребителя услуги является основным требованием относительно всех прочих аспектов и параметров QoS.

Уровень 4 — это уровень разнообразных услуг, их качество определяется ключевыми показателями эффективности QoS, относящимися к конкретным услугам. Когда параметры QoS уровней 1–3 не поддерживаются на стабильно высоком уровне, бесполезно пытаться оценивать QoS какой-либо услуги, поскольку необходимые предварительные условия не соблюдены, и значимость полученных показателей QoS будет близка к нулю.

Разделение на сети с коммутацией каналов и коммутацией пакетов — наследие технологий 2G и 3G. Некоторые из услуг на уровне 4 на самом деле зависят друг от друга или относятся к разным группам. Есть услуги-носители, такие как базовый протокол Интернет (IP), и комбинированные услуги, в которых используется одна или несколько подобных услуг-носителей: например, в составе услуги передачи мультимедийных сообщений (MMS) для уведомления используется услуга передачи коротких сообщений (SMS), которая фактически является услугой для конечного потребителя, а собственно данные передаются в виде пакетов. Услуга, имеющая тот же результат для конечных пользователей, например OTT-чат с вложением файлов, использует только базовую пакетную передачу данных.

Важно отметить некоторые аспекты реализации обеспечения QoS в сетях сотовой подвижной электросвязи стандарта UMTS. В сетях UMTS используются 4 различных класса трафика пакетов (т.е. 4 класса QoS):

- разговорный класс, предназначенный для услуг с требованиями к низкой задержке и сохраняемой разнице во времени между различными IP-пакетами. Эта схема нацелена на услуги операторского класса в режиме реального времени по IP, такие как VoIP, видеотелефония на основе VoIP и инструменты для проведения конференций на основе VoIP;
- потоковый класс, предназначенный для трафика, который требует сохранения разницы во времени между IP-пакетами в данном потоке, но не предъявляет определённых строгих требований к низкой задержке передачи. Следовательно, этот класс подходит для потоковых сервисов (аудио и видео);
- интерактивный класс, предназначенный для услуг не в реальном времени, имеющий определённые требования к задержке передачи (однако не такие строгие, как для услуг в реальном времени), основанные на использовании запроса-ответа конечным пользователем. Этот класс относится к интерактивным служ-

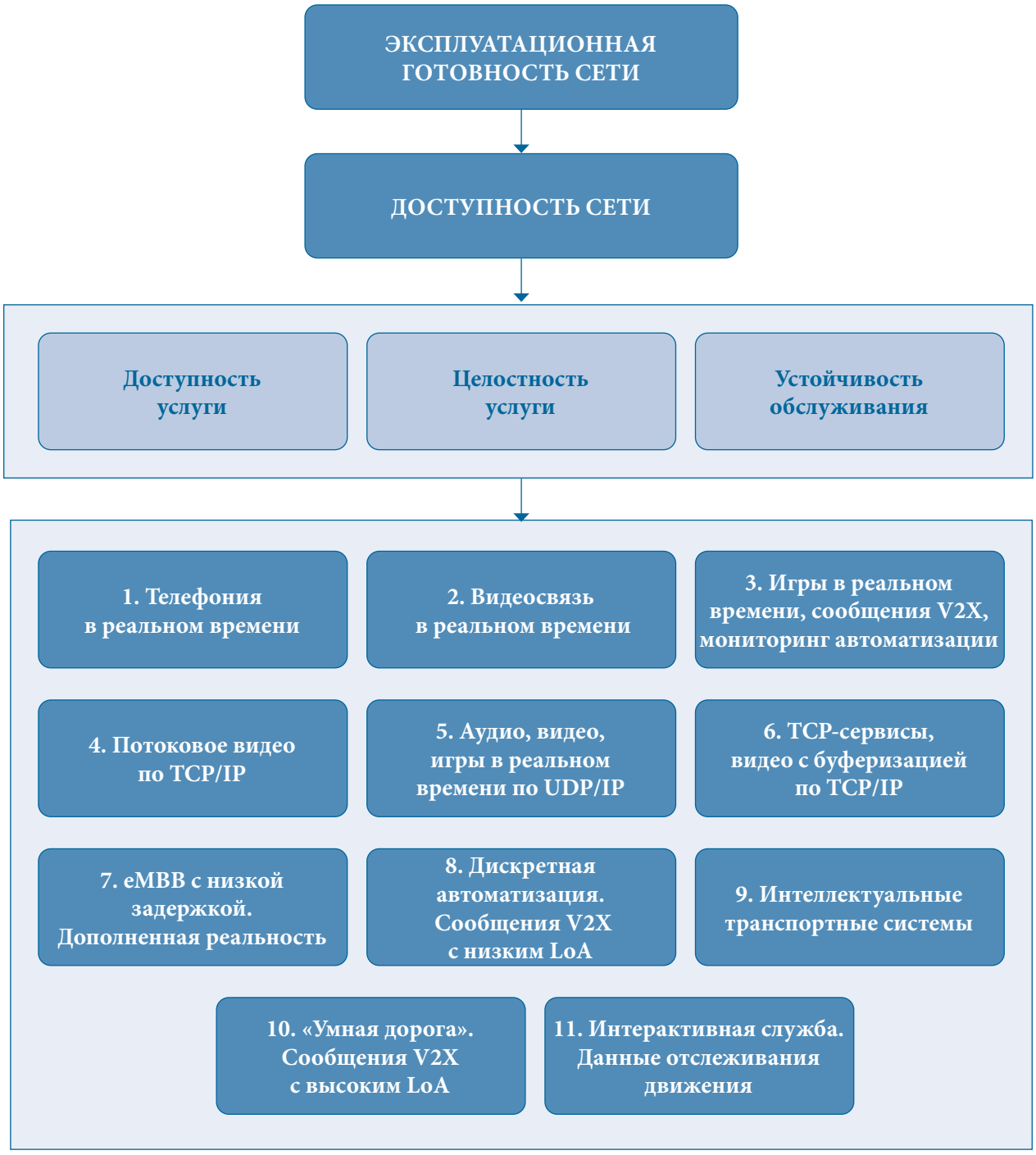


Рис. 9. *Модель параметров качества в сетях LTE и 5G*

бам/приложениям клиент-сервер, таким как Интернет, поиск в базе данных и т.д. Ключевыми параметрами QoS являются низкое время задержки приема-передачи и низкий уровень битовых ошибок;

- фоновый класс, предназначенный для служб, которые могут задерживать пакеты, таких как электронная почта, загрузка файлов и т.д. Этот класс обслуживается с наименьшим приоритетом.

Кроме того, классы QoS в UMTS можно дополнительно дифференцировать по приоритету распределения и удержания параметров (ARP) и приоритету обработки

трафика (THP). На практике в мобильных сетях 3G используются не все классы QoS, поскольку обычно телефония предоставляется через коммутацию каналов, и только услуга доступа в Интернет через мобильную сеть основана на IP-соединении, к которому относятся классы QoS. Однако они существуют как средства для дифференциации QoS, когда оператор связи предоставляет различные услуги операторского класса, такие как VoIP с гарантиями QoS или услуги потокового видео с гарантиями QoS [3, с. 18-19].

Модель параметров качества услуг в сетях LTE и 5G показана на рис. 9.

Параметры и показатели эксплуатационной готовности сети, доступности сети, доступности каждой услуги, целостности каждой услуги и устойчивости обслуживания в сетях LTE и 5G совпадают. Совпадают также нормы на значения показателей и параметров. Параметры и показатели первых шести услуг четвёртого уровня также совпадают для сетей LTE и 5G, последние 6 услуг четвёртого уровня относятся только к сетям 5G [3, с. 65].

В соответствии с авторской теорией качества [13] для устранения недостатков в работе отдельных сот сетей операторы должны иметь технические и программные средства анализа, классификации и прогнозирования состояния каждой работающей соты как нормальное (Active), деградирующее (Degraded) и критически деградирующее (Fault). При этом должны быть востребованы накопленные знания о параметрах и показателях качества работы сот, и происходит процесс их создания и распространения с наименьшими издержками [14].

Заключение

На основе анализа услуг сетей сотовой связи стандартов LTE и IMT-2020 (5G) и технических особенностей сетей стандартов LTE и 5G, влияющих на качество услуг, в статье построены модели показателей и параметров качества услуг сотовой связи стандартов LTE и 5G.

В результате анализа международного опыта определения требований к параметрам и показателям качества, определяющим зону уверенного приёма, и услуг сетей сотовой связи для различных сервисов в сетях LTE и 5G установлено следующее:

- в международных технических нормативно-правовых актах качество услуг связи рассматривается на трёх уровнях: качество функционирования сети NP (Network Performance) на транспортном уровне, качество предоставления услуги/сервиса QoS (Quality of Service) на уровне услуг (приложений) и качество восприятия услуги QoE (Quality of Experience) на уровне конечного пользователя;
- сквозная оценка качества услуги определяется оценками качества услуги на каждом из трёх перечисленных уровней;
- для сетей LTE и 5G, построенных по технологии коммутации пакетов, требуются показатели качества, которые описывают только процесс передачи трафика, отражающие качество работы пакетных очередей/буферов и влияние возможности изменения маршрута передачи пакетов данных от отправителя к получателю;
- в Рекомендациях МСЭ и документах ETSI установлены качественные и количественные показатели QoS и NP для сетей передачи данных, построенных с использованием IP-протокола. К качественным показателям относятся величина времени задержки при передаче пакета, вариация величины времени задержки (джиттер) передачи пакетов, уровень ошибок (доля переданных с ошибкой) пакетов, уровень потерь (доля потерянных) пакетов, уровень нарушения порядка (доля с нарушением порядка следования) пакетов, уровень дублирования пакетов, уровень сброса (доля сброшенных/отказанных в обработке) на сетевом устройстве/элементе пакетов. К количественным

показателям относятся уровень загрузки сети, пакетная и байтовая скорость передачи;

- в Рекомендациях МСЭ и документах ETSI предложено рассматривать 4 уровня показателей качества услуг сетей сотовой связи: параметры эксплуатационной готовности сети, параметры доступности сети, параметры доступности услуги, целостности услуги и устойчивости обслуживания и параметры качества каждой услуги.

ЛИТЕРАТУРА

1. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 01.12.2016 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_207978/
2. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 [Электронный ресурс]. URL: https://xn--h1apes.xn--p1ai/storage/uploads/2022/11/28/6384c39e5cd0e----9--2017--N-203-----.pdf
3. Карпук А.А., Кохно П.А. Качественный эликсир экономики: монография. М.: Изд. дом «Граница», 2026. 212 с.
4. Рекомендация МСЭ-Т Е.800. Определение терминов, относящихся к качеству обслуживания [Электронный ресурс]. МСЭ, 2008. 32 с. URL: https://www.itu.int/rec/T-REC-E.800-200809-I
5. Recommendation ITU X.140. General Quality of Service Parameters for Communication via Public Data Networks [Electronic resource]. ITU, 1992. 22 p. URL: https://www.itu.int/rec/T-REC-X.140-199209-I/en
6. Recommendation ITU-T I.350. General Aspect of Quality of Service and Network Performance in Digital Networks, including ISDNs [Electronic resource]. ITU, 1993. 17 p. URL: https://www.itu.int/rec/T-REC-I.350-199303-I/en
7. Technical Report ETSI TR 102 643 V1.0.2 (2010-01). Human Factors (HF); Quality of Experience (QoE) requirements for real-time communication services [Electronic resource]. ETSI, 2010. 37 p. URL: https://www.etsi.org/deliver/etsi_tr/102600_102699/102643/01.00.02_60/tr_102643v010002p.pdf
8. Akhshabi S., Dovrolis C. The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture // ACM SIGCOMM Computer Communication Review. 2011. Vol. 41, iss. 4. P. 206–217.
9. Recommendation ITU-T Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters [Electronic resource]. ITU, 2019. 102 p. URL: https://www.itu.int/rec/T-REC-Y.1540-201912-I/en
10. Recommendation ITU-T Y.1543. Measurements in Internet protocol networks for inter-domain performance assessment [Electronic resource]. ITU, 2018. 48 p. URL: https://www.itu.int/rec/T-REC-Y.1543-201806-I/en
11. Recommendation ITU-T E.804. QoS aspects for popular services in mobile networks [Electronic resource]. ITU, 2014. 446 p. URL: https://www.itu.int/rec/T-REC-E.804-201402-I/en
12. Technical Specification ETSI TS 102 250-2. Speech and multimedia Transmission Quality (STQ); QoS aspects for popular services in mobile networks; Part 2: Definition of Quality of Service parameters and their computation [Electronic resource]. ETSI, 2015. 258 p. URL: https://www.etsi.org/deliver/etsi_ts/102200_102299/10225002/02.04.01_60/ts_10225002v020401p.pdf
13. Кохно П.А., Кохно А.П., Артемьев А.А. Теория качества: монография / отв. ред. П.А. Кохно. Тверь: Изд-во Твер. гос. ун-та, 2025. 243 с.
14. Кохно П.А., Кохно А.П., Кохно В.О. Мировая конкуренция: монография / отв. ред. П.А. Кохно. М.: Изд. дом «Граница», 2026. 208 с.

Models of Indicators and Parameters of Quality of Cellular Services

Anatoli Alekseevich Karpuk — Associate Professor, Candidate of Technical Sciences, Professor at the Department of Telecommunications Network Software, Belarusian State Academy of Communications.
E-mail: a_karpuk@mail.ru

Pavel Antonovich Kokhno — Professor, Doctor of Economics, Deputy Director for Research at the Autonomous Nonprofit Organization "Promotion and Development of Innovations in the Scientific and Industrial Sphere," Moscow, Autonomous Nonprofit Organization "Promotion and Development of Innovations in the Scientific and Industrial Sphere".
E-mail: pavelkohno@mail.ru

The article defines indicators and parameters of quality of services in networks of standards 4G and 5G. The quality of user service depends on the performance of the network itself, as well as external factors. The network service of the communication network is described by the parameters of the communication equipment at the three levels of the OSI model. In terms of functionality, the value of each indicator is a compromise function between ensuring the quality of the communication service and the costs of this provision. The described quality indicators refer to any communication networks, including networks with circuit switching and packet switching. Quantitative (volume) indicators are divided by areas of responsibility between the operator and the user of communication services. A four-level model of service quality parameters is proposed.

Keywords: cellular communication, indicators, parameters, services, models, traffic, network service, standards, channel switching, packet switching

REFERENCES

1. Poslanie Prezidenta Rossiyskoy Federatsii Federalnomu Sobraniyu Rossiyskoy Federatsii ot 01.12.2016 [Electronic resource]. URL: https://www.consultant.ru/document/cons_doc_LAW_207978/ (in Russian).
2. O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody: Ukaz Prezidenta RF ot 09.05.2017 No 203 [Electronic resource]. URL: https://xn--h1apes.xn--p1ai/storage/uploads/2022/11/28/6384c39e5cd0e----9--2017--N-203-----.pdf (in Russian).
3. Karpuk A.A., Kokhno P.A. Kachestvennyy eliksir ekonomiki: monografiya. M.: Izd. dom «Granitsa», 2026. 212 s. (in Russian).
4. Rekomendatsiya MSE-T E.800. Opredelenie terminov, otnosyashchikhsya k kachestvu obsluzhivaniya [Electronic resource]. MSE, 2008. 32 s. URL: https://www.itu.int/rec/T-REC-E.800-200809-I (in Russian).
5. Recommendation ITU X.140. General Quality of Service Parameters for Communication via Public Data Networks [Electronic resource]. ITU, 1992. 22 p. URL: https://www.itu.int/rec/T-REC-X.140-199209-I/en
6. Recommendation ITU-T I.350. General Aspect of Quality of Service and Network Performance in Digital Networks, including ISDNs [Electronic resource]. ITU, 1993. 17 p. URL: https://www.itu.int/rec/T-REC-I.350-199303-I/en
7. Technical Report ETSI TR 102 643 V1.0.2 (2010-01). Human Factors (HF); Quality of Experience (QoE) requirements for real-time communication services [Electronic resource]. ETSI, 2010. 37 p. URL: https://www.etsi.org/deliver/etsi_tr/102600_102699/102643/01.00.02_60/tr_102643v010002p.pdf

8. Akhshabi S., Dovrolis C. The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture // ACM SIGCOMM Computer Communication Review. 2011. Vol. 41, iss. 4. P. 206–217.
9. Recommendation ITU-T Y.1540. Internet protocol data communication service – IP packet transfer and availability performance parameters [Electronic resource]. ITU, 2019. 102 p. URL: https://www.itu.int/rec/T-REC-Y.1540-201912-I/en
10. Recommendation ITU-T Y.1543. Measurements in Internet protocol networks for inter-domain performance assessment [Electronic resource]. ITU, 2018. 48 p. URL: https://www.itu.int/rec/T-REC-Y.1543-201806-I/en
11. Recommendation ITU-T E.804. QoS aspects for popular services in mobile networks [Electronic resource]. ITU, 2014. 446 p. URL: https://www.itu.int/rec/T-REC-E.804-201402-I/en
12. Technical Specification ETSI TS 102 250-2. Speech and multimedia Transmission Quality (STQ); QoS aspects for popular services in mobile networks; Part 2: Definition of Quality of Service parameters and their computation [Electronic resource]. ETSI, 2015. 258 p. URL: https://www.etsi.org/deliver/etsi_ts/102200_102299/10225002/02.04.01_60/ts_10225002v020401p.pdf
13. Kokhno P.A., Kokhno A.P., Artemyev A.A. Teoriya kachestva: monografiya / otv. red. P.A. Kokhno. Tver: Izd-vo Tver. gos. un-ta, 2025. 243 s. (in Russian).
14. Kokhno P.A., Kokhno A.P., Kokhno V.O. Mirovaya konkurentsiya: monografiya / otv. red. P.A. Kokhno. M.: Izd. dom «Granitsa», 2026. 208 s. (in Russian).

Images and tables

Fig. 1. *General composition of service quality indicators*

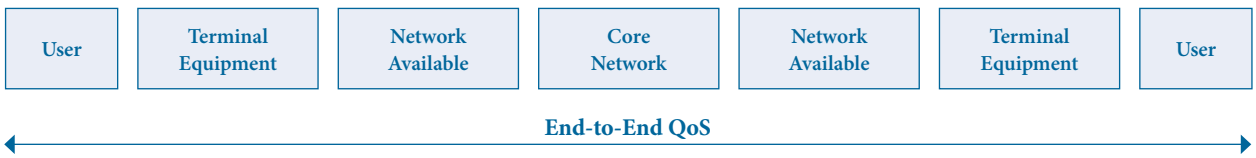


Fig. 2. *Schematic representation of end-to-end QoS components*

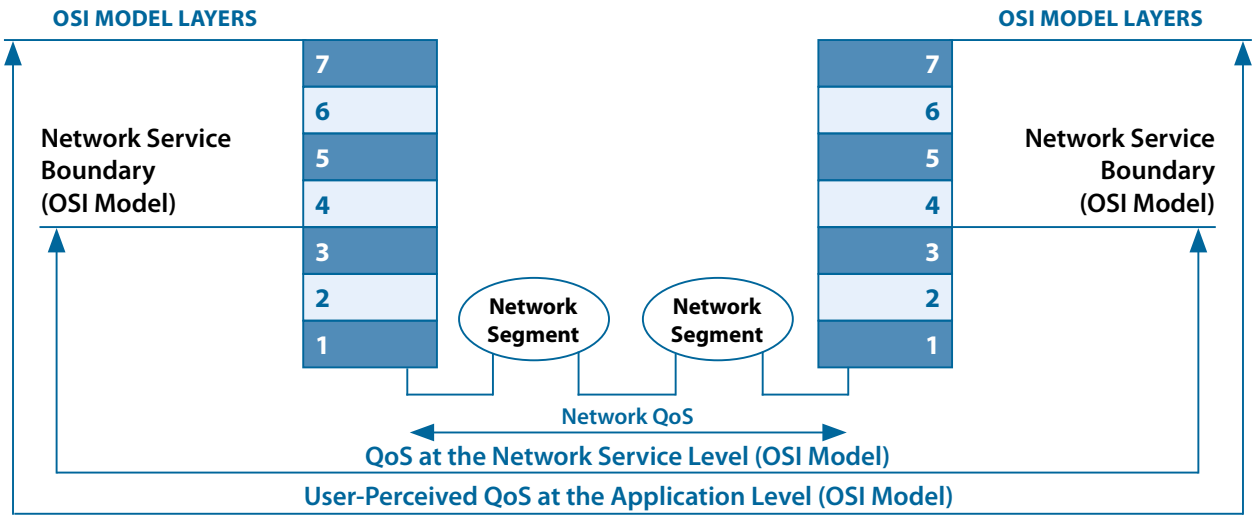


Fig. 3. *Division of QoS indicators by OSI model layers*

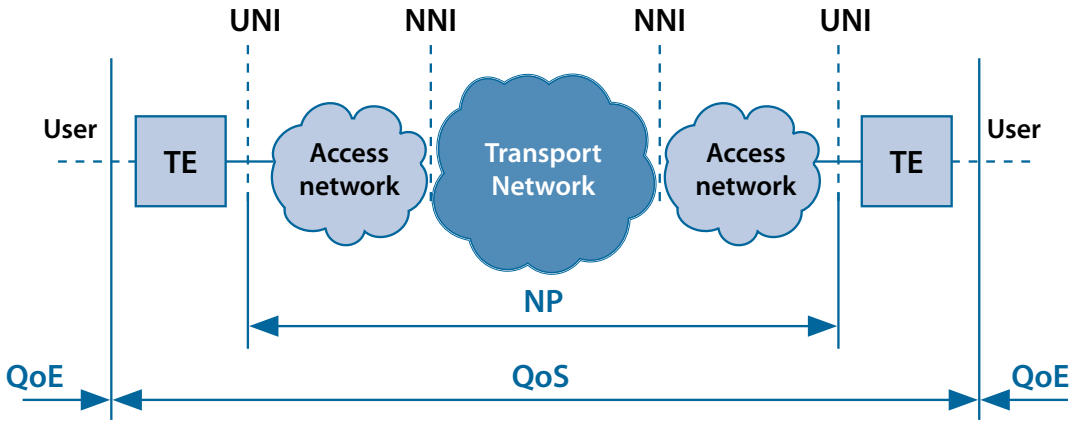


Fig. 4. *Scope of application of groups of communication service quality indicators*

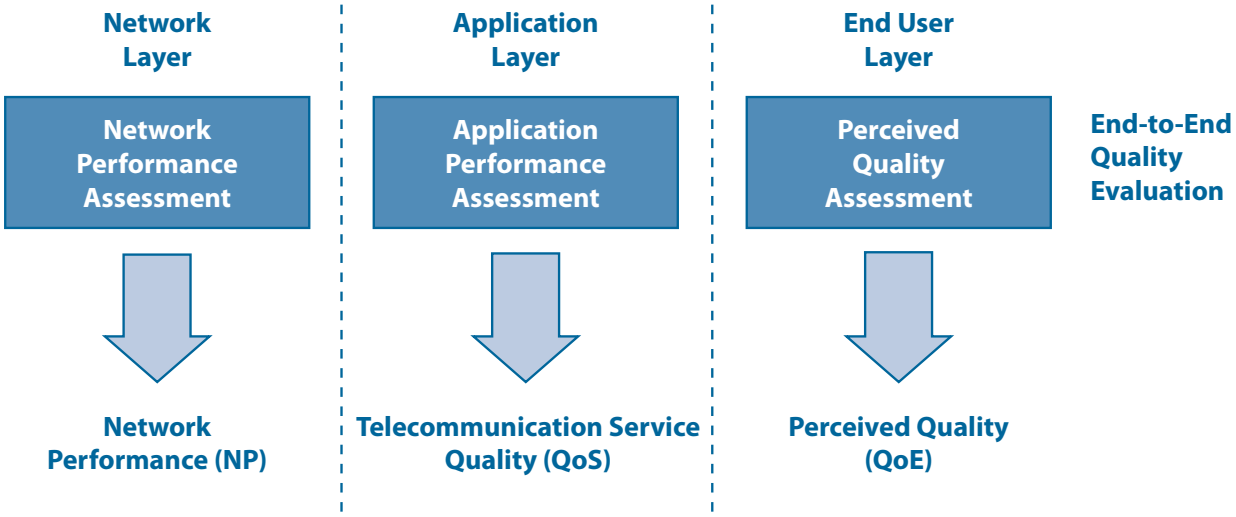


Fig. 5. *Assessment of end-to-end quality of communication service*

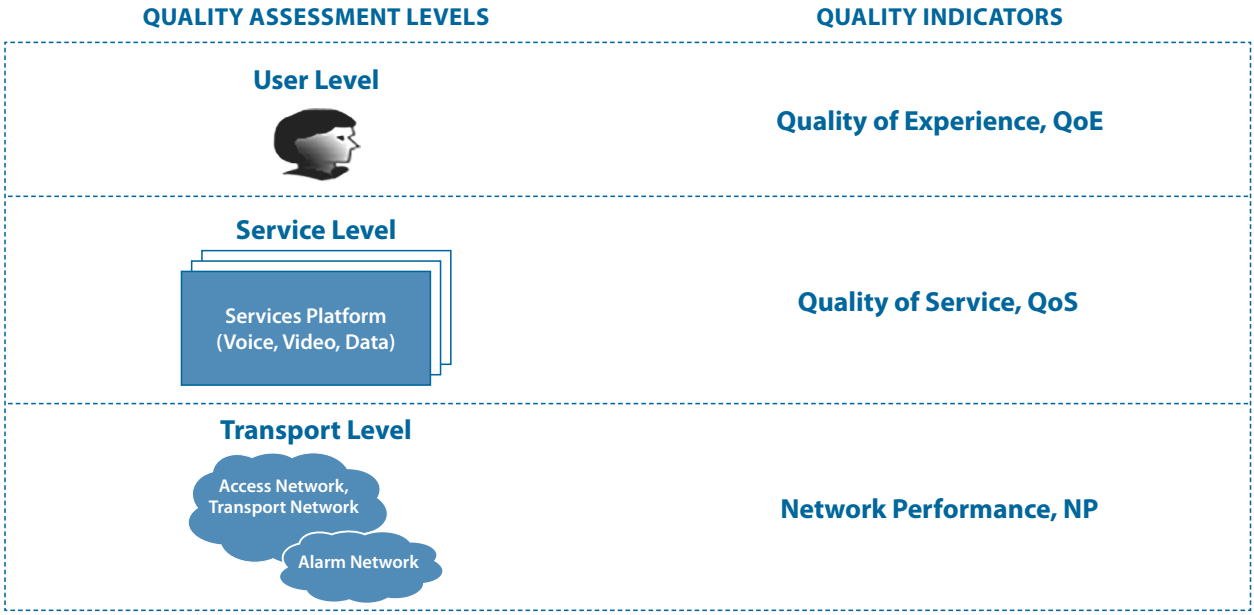


Fig. 6. *Distribution of communication service quality indicators by technological systems*

Table 1

Differences between packet-switched networks and circuit-switched networks

Network function	Switched networks channels	Packet-switched networks
Establishing a connection	A connection must be established in advance	There is no connection establishment stage (datagram method)
Resource allocation procedure	Resources are provided in accordance with the order in which requests are received.	Resources are provided simultaneously for all requests, provided that the total bandwidth required for them does not exceed the capabilities of the communication channel.
Transferring the recipients address	The address is only required at the connection establishment stage.	The address and other service information are transmitted with each packet.
Availability of network service to the user	The network may refuse to allow the user to establish a connection.	The network is always ready to receive data from the user.
Throughput guarantee	Guaranteed throughput	In general, the network bandwidth for subscribers is not known in advance; guaranteed bandwidth allocation is possible.
Procedure allocating bandwidth for user traffic	Static	Dynamic (in general), with the possibility of static allocation
Packet traffic transmission route	Data is transmitted according to the route of the channel within the communication network	The decision on the further route for transmitting a data packet is made separately for each traffic switching point on the path from the sender to the recipient; within the framework of transmitting one information message consisting of several data packets, each packet can be transmitted by a different route.
Delay in traffic transmission in a communication channel	The delay is determined by the time it takes for an electromagnetic signal to travel through a communication channel.	The delay value depends on the delay in packet queues/buffers on network nodes and is random.
Traffic loss at network nodes	Almost none	Data loss may occur due to packet buffer queue overflow.
Efficiency of use communication channel	Low (in general)	High
The best type of traffic	With a fixed rate, when transmitting bursty traffic, a significant portion of the reserved channel capacity is not used	Pulsating, it is possible to allocate a lane for traffic at a fixed speed
Traffic priority	Absent	By setting a priority flag and organizing different buffers/queues for traffic with different priority flag values
Terminating the connection	The connection is being "disassembled" and network resources are being released.	Not required
Providing connectivity to another set of communication service users	Transfer of released network resources to organize a connection in the interests of other users of communication services	It is possible to establish a connection in “parallel” mode if there are network resources that meet the user’s request requirements, or dynamically redistribute network resources in the absence of strict requirements for network resources from already established connections.

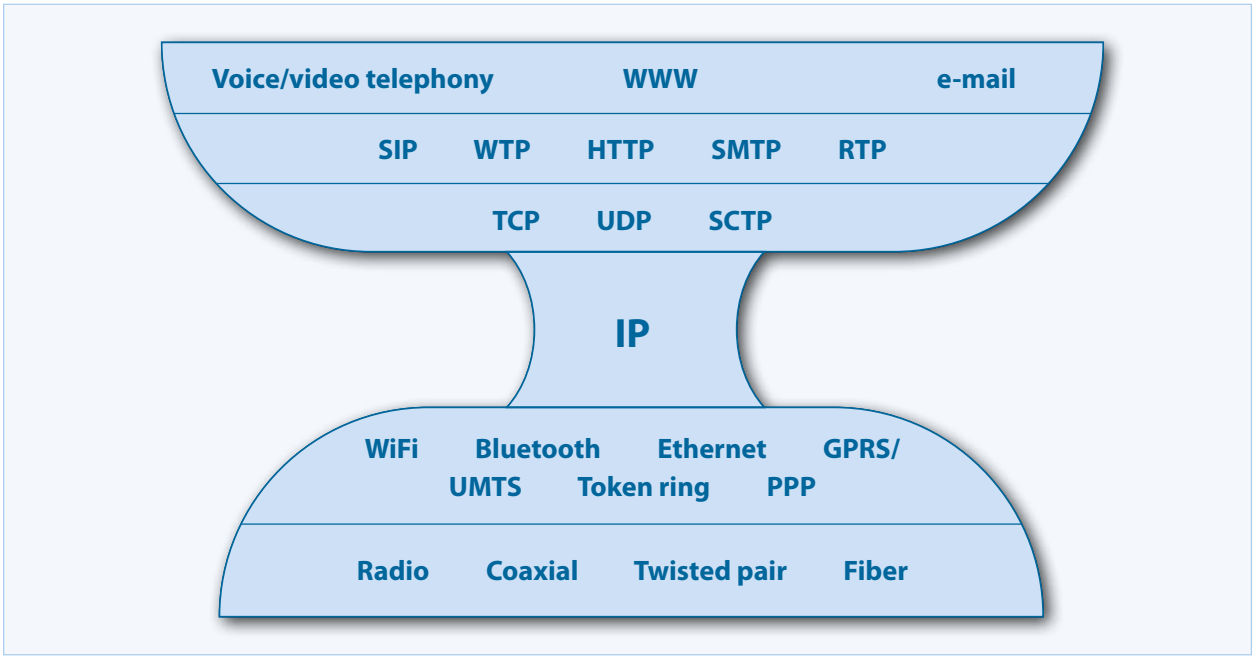


Fig. 7. *Hierarchy of packet-switched network protocols*

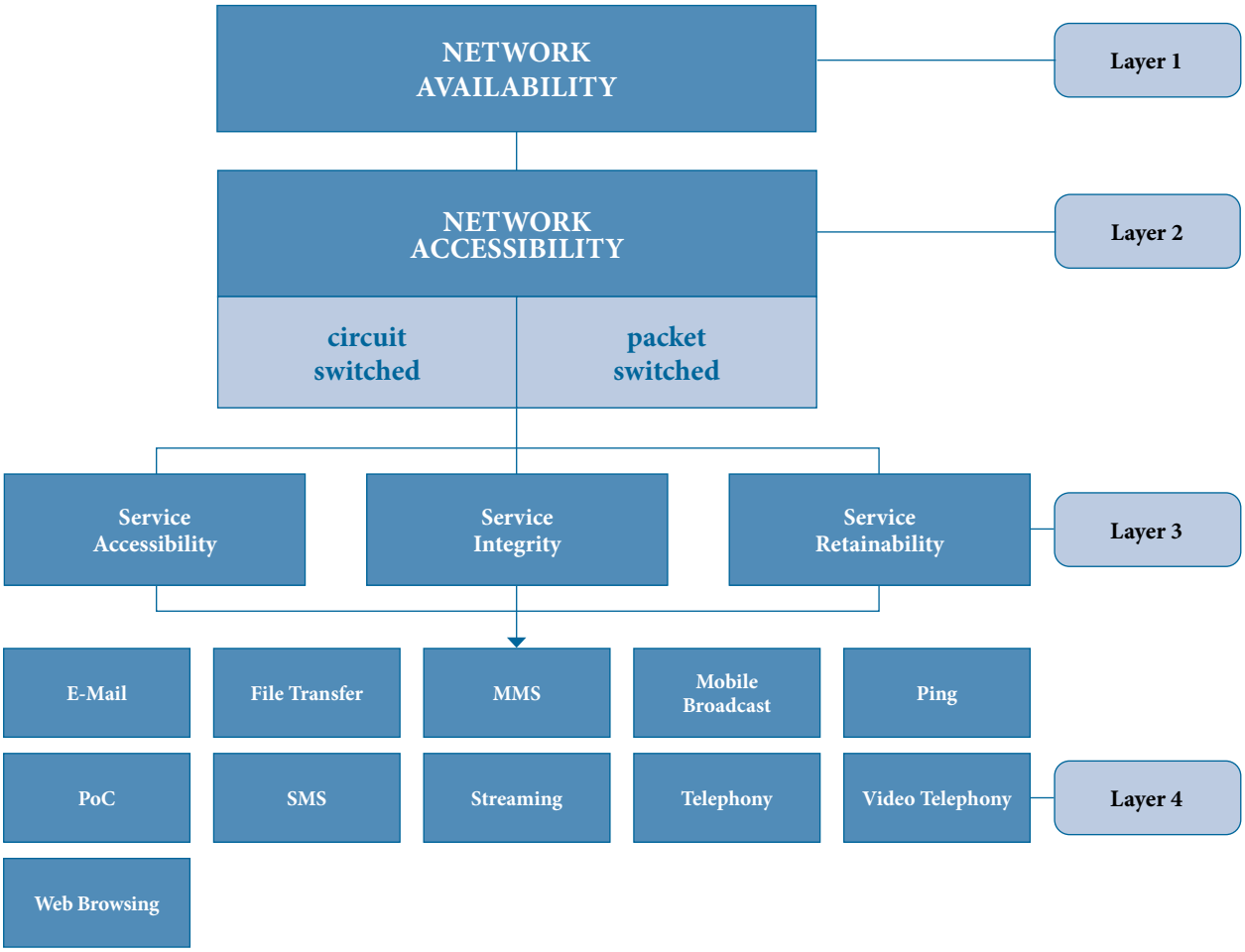


Fig. 8. *Model of service quality parameters*

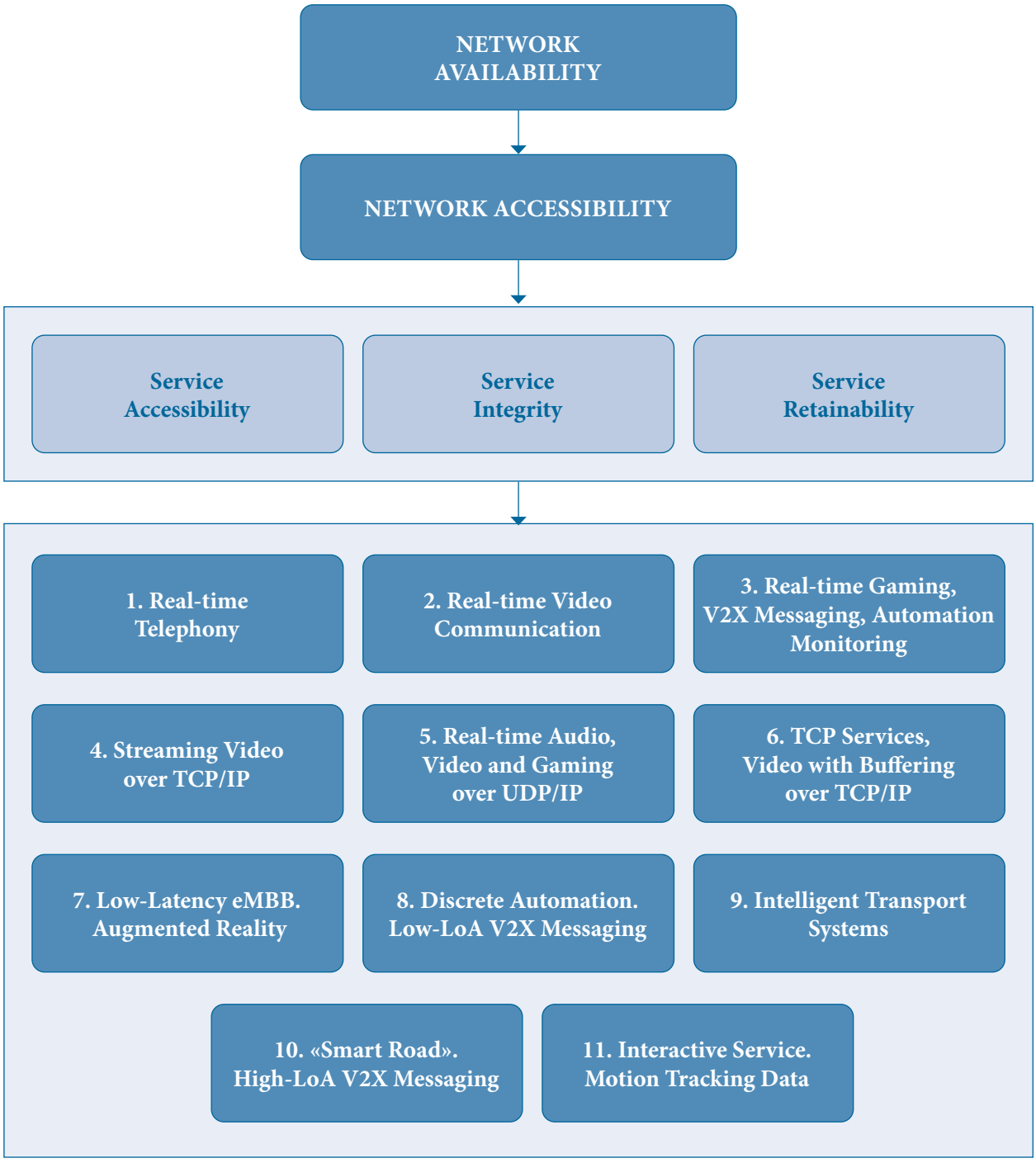


Fig. 9. *Model of quality parameters in LTE and 5G networks*

Индекс УДК 004.622:636.2
Код ГРНТИ 68.85.85
DOI: 10.22204/2410-4639-2026-129-01-43-52

И.И. МИХАЙЛЕНКО,
О.Д. МЕЩЕРЯКОВ,
А.И. ЛИТВИНОВ*

Формирование обучающего датасета для оценки функциональных состояний КРС

В данной статье рассмотрен анализ возможных поведенческих состояний животных крупного рогатого скота (КРС), функционально подходящих для формирования датасета, обучающего и тестирующего нейронные сети. Видеозаписи, на основе которых проводилось аннотирование паттернов, взяты с автоматизированной видеоаппаратуры, установленной в животноводческом помещении. По частоте проявлений различных паттернов поведения установлены предварительные показатели их временных характеристик и построена модель совместных состояний животных. Представлены результаты первичного пробного обучения нейронных сетей.

Ключевые слова: цифровизация, автоматизация, искусственный интеллект, нейронные сети, машинное зрение, распознавание действий

С каждым годом цифровая трансформация сельскохозяйственной отрасли развивается всё активнее, что положительно сказывается на продовольственной безопасности страны. Обусловлено это созданием различных драйверов развития агропромышленного комплекса, таких как внедрение государственных цифровых систем и ведомственных проектов, совершенствование технологий с использованием искусственного интеллекта.

Мониторинг крупного рогатого скота является важным аспектом животноводства, и последние достижения в этой области значительно повысили знания людей

* **Михайленко Ирина Ивановна** — кандидат биологических наук, научный сотрудник лаборатории интеллектуальных сельскохозяйственных технологий, ФГБНУ «Белгородский ФАНЦ РАН».
E-mail: ira-mik86@yandex.ru

Мещеряков Олег Дмитриевич — кандидат сельскохозяйственных наук, научный сотрудник лаборатории интеллектуальных сельскохозяйственных технологий, ФГБНУ «Белгородский ФАНЦ РАН».
E-mail: meshe.64@mail.ru

Литвинов Андрей Игоревич — младший научный сотрудник лаборатории интеллектуальных сельскохозяйственных технологий, ФГБНУ «Белгородский ФАНЦ РАН».
E-mail: zemledel-it@yandex.ru

в изучении поведения животных благодаря использованию специальных устройств, таких как ушные бирки и ошейники. Однако появились отрицательные аспекты решений, связанные с их применением: недостаточная универсальность, малая изученность влияния этих датчиков на здоровье животных, неудобство ношения, амортизационные расходы [1]. В связи с этим на первый план стали выходить бесконтактные системы наблюдения за поведением животных, основанные на машинном обучении по видеоданным.

Биометрия животных — это перспективное направление в области компьютерного зрения, распознавания образов и когнитивистики, которое играет важную роль в регистрации, уникальной идентификации и верификации крупного рогатого скота [2-4]. Существующие методы извлечения текстурных признаков и представления признаков на основе внешнего вида не позволяют распознавать животных в произвольной среде. В последнее время всё больше внимания уделяется подходам на основе глубокого обучения для распознавания видов или отдельных животных с использованием визуальных признаков [5-7].

Цель исследования — анализ возможных поведенческих состояний животных КРС, функционально подходящих для формирования датасета, обучающего и тестирующего нейронные сети.

Материалы и методы исследования

Экспериментальные наблюдения проводили на базе Ериковского молочного комплекса ФГБНУ «Белгородский ФАНЦ РАН». Для формирования набора данных в одном из помещений фермы на специальных рельсах была установлена видеоаппаратура автоматизированного слежения за поведением животных. В дневное время суток камеры снимали в цветном режиме, в ночное — в чёрно-белом (ИК диапазон). Для эксперимента взяли чёрно-пёструю породу КРС. Период съёмок происходил во время привязного содержания коров (ноябрь-апрель). Для исследования взяты 20 суток непрерывных видеоданных с трёх видеокамер.

Идентификация КРС по изображениям относится к задаче машинного обучения, в рамках которой выполняется определение наличия или отсутствия объекта КРС на изображении, нахождение границ этого объекта в системе координат пикселей исходного изображения.

Задача заключается в том, чтобы каждому изображению, I, поставить в соответствие множество положений объектов КРС, K:

$$F : I \to K,\ K = \left\{k_j, j = \overline{0,n}\right\}, \qquad (1)$$

где $k_j = \langle\left(x_1^j, y_1^j\right),\left(x_2^j, y_2^j\right), s^j, c^j\rangle$ — кортеж с координатами ограничивающей рамки объекта, классом объекта s^j («корова», «не корова») и достоверностью $c^j \in \mathbb{R}$ [8].

Для решения задачи используется аппарат искусственных нейронных сетей со свёрточными слоями на базе архитектуры YOLOv10.

Важным этапом построения модели глубокого обучения является подготовка видеоданных, которая включает аннотации паттернов [9]. Для задачи распознавания действий животных датасет должен иметь большое количество данных и содержать разные типы действий животных, которые позволят ускорить обучение нейронных сетей, увеличить обобщающую способность и устойчивость их функционирования. Разработка нейросетевых алгоритмов подразумевает применение соответствующих наборов данных для обучения и тестирования сетей.

Обучение нейросети выполняется с помощью метода обратного распространения ошибки [10]. При этом значение ошибки формируется на основе функции потерь (loss), которая сравнивает предсказанные нейросетью значения со значениями разметки (истинными значениями). Для обучения идентификации КРС применяется функция потерь *VFL*:

$$VFL(p,q) = \begin{cases} -q\left(q\log(p) + (1-q)\log(1-p)\right) & q > 0 \\ -\alpha\ p^{\gamma}\log(1-p) & q = 0 \end{cases} \qquad (2)$$

где p — предсказанные значения, q — истинные значения, α и γ — гиперпараметры обучения.

Качество результатов работы обученной нейросети оценивается по отношению площадей ограничивающих рамок в метрике *IoU* (англ. Intersection over Union):

$$IoU = \frac{S(A \cap B)}{S(A \cup B)}, \quad (3)$$

где A — предсказанная ограничивающая рамка, B — истинная ограничивающая рамка. Метрика *IoU* равна нулю в случае непересекающихся ограничивающих рамок и равна единице в случае идеального наложения.

Результаты и обсуждение

Первоначально для аннотации сформированных тестовых и валидационных наборов видеоданных был подобран перечень паттернов (событий). Формирование перечня паттернов основывалось на возможных аномальных ситуациях в поведении и развитии КРС. Таким образом, проанализировав комплекс возможных поведенческих реакций животных на тот или иной фактор, решено было ввести в работу перечень паттернов, состоящий из простых движений, совокупность которых во временном контексте позволит выявить количественные характеристики, информирующие о наличии аномалий в поведении. Список паттернов выглядит следующим образом (табл. 1).

Первые три паттерна позволяют оценить достаточность и нормальность кормления, руминации и питьевого режима животных. Паттерны «Лежание» и «Неподвижное стояние» помогут сделать вывод о правильности или нарушении времени отдыха животных. Паттерн «Удары рогами о предметы» может говорить, с одной стороны, о темпераменте особи, с другой — о возможных проявлениях недовольства внешними условиями либо внутренними проблемами животного. Паттерн «Проявление интереса к соседней корове» может выражаться в виде облизывания, обнюхивания, бодания, толкания одной коровой другой, что позволяет судить о наступлении состояния эструса (половой охоты).

Таблица 1

Список исследуемых паттернов

Pattern 1	«Руминация»
Pattern 2	«Нет руминации»
Pattern 3	«Водопотребление»
Pattern 4	«Лежание»
Pattern 5	«Неподвижное стояние»
Pattern 6	«Удары рогами о предметы»
Pattern 7	«Проявление интереса к соседней корове»

Таким образом, нарушение 1, 2, 3, 4 паттернов или проявление 5, 6, 7 особенностей поведения сигнализирует о возможной аномалии, выраженной или в начальной стадии заболевания, или в нарушении внешних благоприятных условий, или в каких-либо других негативных проявлениях, что в любом случае должна улавливать и оповещать об этом специалистов потенциальная автоматизированная система слежения за поведением КРС. Ключевой этап разметки проводился методом аннотирования, который предполагает определение местоположения и ориентации КРС, а обнаруженные части тела животного могут быть использованы для извлечения визуальных биометрических характеристик для окончательной идентификации животных.

Процесс аннотирования видеоданных производился с помощью инструмента CVAT (Computer Vision Annotation Tool). Тип аннотаций — ключевые точки. Следует отметить, что аннотирование видеоданных имеет большие преимущества в сравнении с аннотациями отдельных изображений, так как экспериментальные модели искусственного интеллекта при обучении получат больше контекстной информации. Можно выделить следующий ряд преимуществ:

1) возможность интерполяции — не нужно аннотировать каждый кадр, а только отметить начало и конец последовательности;

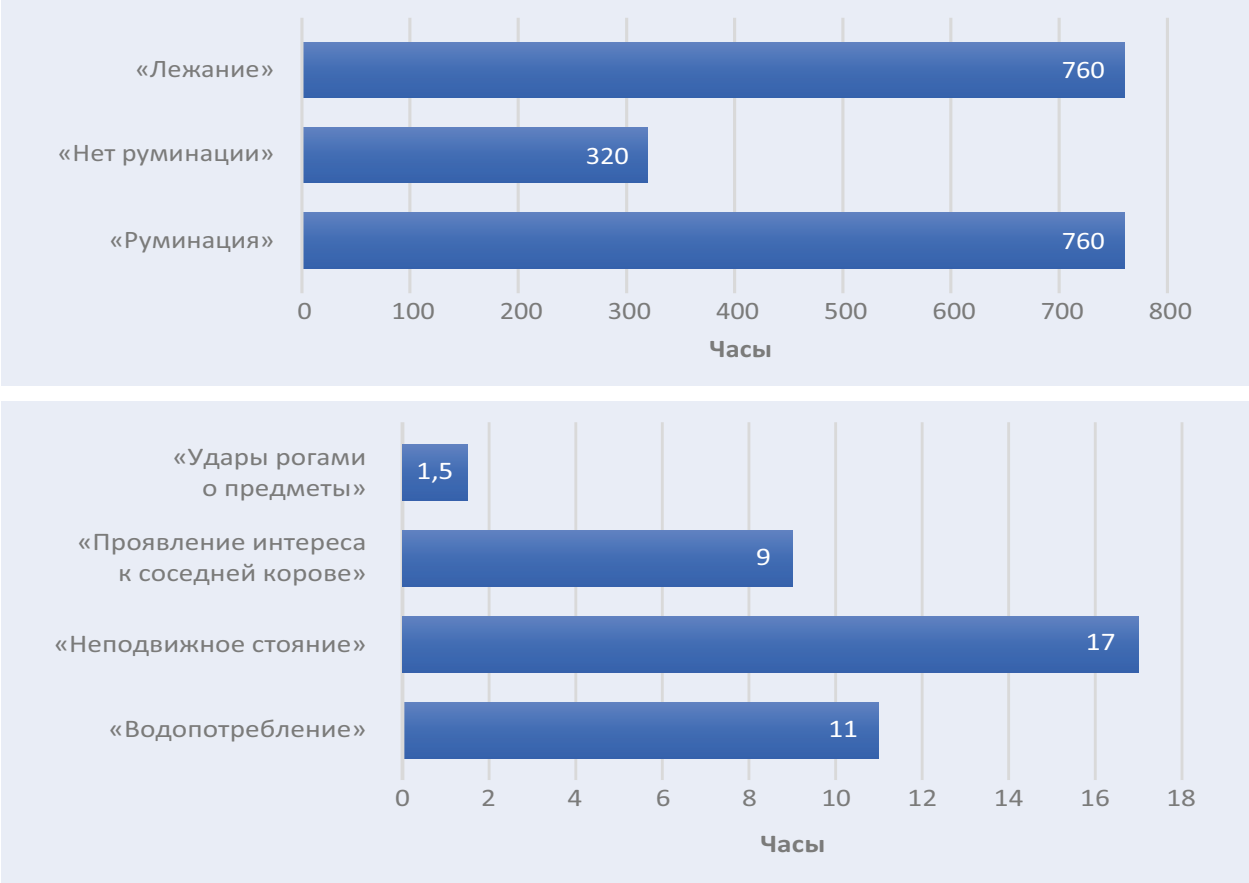


Рис. 1. *График суммарного времени пребывания КРС в различных состояниях*

2) наличие временного контекста — видеоданные могут быстрее обучить модель искусственного интеллекта тому, как перемещаются или изменяются объекты с течением времени;
3) выше качество и точность результатов;
4) экономия времени.

Анализ размеченных видеороликов позволил установить частоту проявлений различных паттернов поведения, а также выявить длительность пребывания животных в различных состояниях. Кроме того, данный анализ обеспечил проверку потенциальных недостатков данных, которые могут повлиять на качество последующего обучения нейронной сети.

На рисунке 1 представлен график суммарного времени пребывания животных в различных состояниях, по оси ординат значения указаны в часах. Можно заметить, что состояния «Руминация» и «Лежание» на порядок превалируют в сравнении с остальными состояниями, количественно они составили по 760 часов. Паттерн «Нет руминации» часто наблюдался, численно он был равен 320 часов. Реже отмечались такие состояния животных, как: «Водопотребление», «Неподвижное стояние» и «Проявление интереса к соседней корове». Их частотность варьировала от 9 до 17 часов. Самым редким событием являлось «Удары рогами о предмет», около 1,5 часов.

Таким образом, становится понятно, что для качественного обучения нейронной сети необходимо разметить дополнительное количество видеоданных по редко проявляемым действиям, чтобы привести в соответствие все рассматриваемые паттерны.

Ниже представлена модель совместных состояний животных, которая отражает прямую одновременную связь одних действий животных с другими действиями [11]. В модели эти связи обозначены взаимообратными стрелками, что отража-

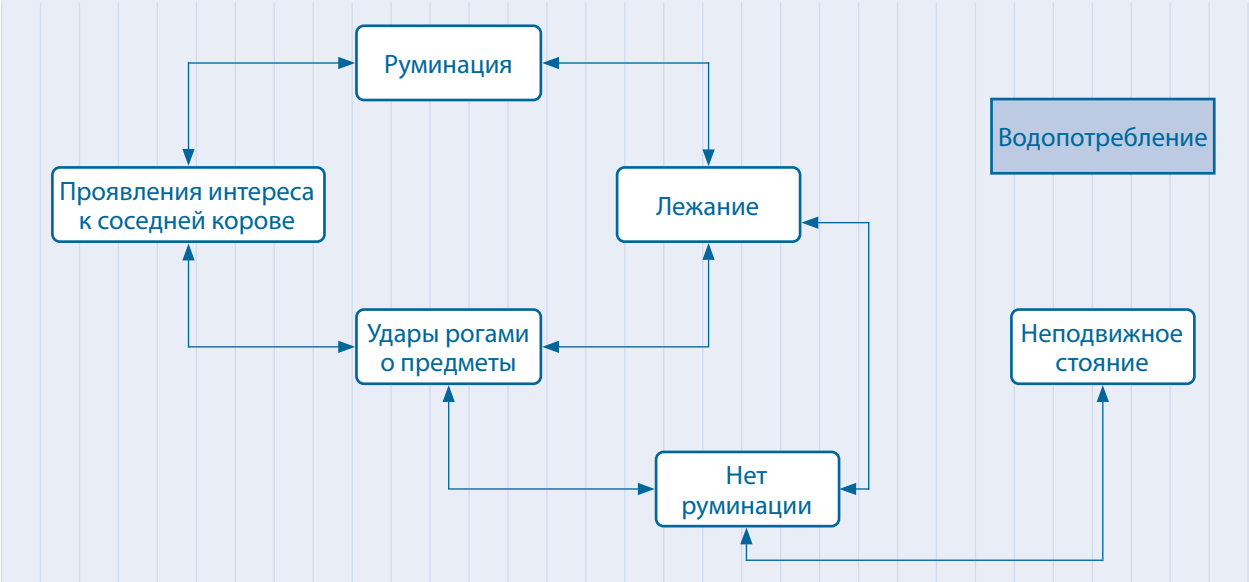


Рис. 2. *Модель совместных состояний КРС*

ет их совместность. В случае отсутствия связи события — не совместны (рис. 2). Таким образом, выявляются два круга возможных одновременных состояний: первый — «Руминация» ↔ «Лежание» ↔ «Удары рогами о предмет» ↔ «Проявление интереса к соседней корове»; второй — «Лежание» ↔ «Удары рогами о предмет» ↔ «Нет руминации». Отдельно отмечаются совместные состояния между паттернами «Нет руминации» и «Неподвижное стояние». Паттерн «Водопотребление» является самостоятельным и несовместным.

Данная модель представляет собой алгоритм поведенческих состояний животных, который необходим для правильного обучения нейронной сети. В случае успешного обучения нейронная сеть должна распознавать одновременно происходящие действия животных разной направленности.

Следующим важным этапом являлось пробное обучение нейросети по детекции коров. Обучение проводилось на 1880 часах аннотированных видеоданных с помощью аппарата искусственных нейронных сетей со сверточными слоями на базе архитектуры YOLOv10. YOLO — это одноэтапный детектор, который выполняет идентификацию и классификацию объектов за один проход по сети. Преимущества этого детектора при решении задачи обнаружения с помощью одноэтапного регрессионного прохода для определения ограничивающих рамок заключаются в высокой скорости и компактности, что позволяет быстрее обучать модели и проще их внедрять, особенно на периферийных устройствах с ограниченными вычислительными ресурсами.

На рисунке 3 представлен конечный результат работы нейросети из семейства YOLO, который показывает, что нейросеть смогла правильно распознать животное «cow — корова» с точностью до 93–96%.

Следует отметить, что нейросеть справилась с заданием, несмотря на кардинальное отличие в положении и движении коров: первая корова лежит, голова опущена; вторая корова стоит, вытягивает шею; третья корова стоит, проявляет интерес к другой корове. Можно сделать вывод о том, что предварительные результаты обучения положительные, но требуются дальнейшие работы по улучшению распознавания животных в нетипичных позах и в условиях плохого или сложного освещения.

Заключение

Таким образом, представленный перечень функциональных состояний КРС позволит выявить аномальное, нехарактерное

Рис. 3. *Результат работы нейросети*

норме поведение животных. Размеченные видеоданные по выделенным паттернам являются прототипом алгоритмов диагностики функциональных состояний животных и могут использоваться для обучения и тестирования глубокой нейронной сети. По частоте проявлений различных паттернов поведения установлены предварительные показатели их временных характеристик и построена модель совместных состояний животных, что представляет интерес в анализе нормальности или аномальности поведения животных КРС.

Данная разработка позволит обеспечить непрерывный в течение суток мониторинг за действиями животных. С помощью мониторинга можно оперативно реагировать на потенциальные проблемы, что способствует снижению уровня заболеваемости и увеличению общей продуктивности стада. Применяться указанная система может в товарных животноводческих хозяйствах любого уровня.

Кроме того, алгоритмы ИИ помогают не только в анализе текущих данных, но и в создании прогнозов, на основе которых можно принимать более осознанные управленческие решения. В связи с этим актуальность аналитических платформ, способных оценивать эффективность работы каждой части хозяйства и предоставлять рекомендации, возрастает всё сильнее. Инвестирование в эти технологии сможет обеспечить конкурентные преимущества для российских фермеров как на внутреннем, так и на международном рынках.

ЛИТЕРАТУРА

1. Sorokina V., Ablameyko S. Data Augmentation Method to Improve the Quality of E-commerce Image Recognition // Reliability Engineering and Computational Intelligence. Studies in Computational Intelligence. 2021. Vol. 976. P. 237–244. DOI: 10.1007/978-3-030-74556-1_14.
2. Dawkins M.S. Does Smart Farming Improve or Damage Animal Welfare? Technology and What Animals Want // Frontiers in Animal Science. 2021. Vol. 2. Art. 736536. P. 64–68. DOI: 10.3389/fanim.2021.736536.
3. Li Y., Zhou L., Yan H., Shan Y., Zheng C., Liu Y., Zuo X., Qiao B. Aircraft Detection for Remote Sensing Images Based on Deep Convolutional Neural Networks // Journal of Electrical and Computer Engineering. 2021. No. 2. P. 1–16. DOI: 10.1155/2021/4685644.

4. Ye S., Bohush R., Chen C., Chen H. Person Tracking and Reidentification for Multicamera Indoor Video Surveillance Systems // Pattern Recognition and Image Analysis. 2020. Vol. 30, No. 4. P. 827–837. DOI: 10.1134/S1054661820040136.
5. Галкин А.И. Применение нейросетей и технологий больших данных в сельском хозяйстве: повышение эффективности и устойчивости агропроизводства // Аграрная наука. 2025. № 4. С. 167–171. DOI: 10.32634/0869-8155-2025-393-04-167-171.
6. Kumar S., Pandey A., Kondamudi S., Singh S. K. [et al.] Deep Learning Framework for Recognition of Cattle Using Muzzle Point Image Pattern // Measurement. 2017. Vol. 116. P. 1–17. DOI: 10.1016/j.measurement.2017.10.064.
7. Порцев Р.Ю., Макаренко А.В. Особенности инициализации сверточных слоев с функцией активации Relu в нейросетевых моделях для распознавания шумовых сигналов // Труды 14-го Всероссийского совещания по проблемам управления (ВСПУ-2024). 2024. С. 3071–3076. EDN: DDFCLK.
8. Musall S., Urai A., Sussillo D., Churchland A. Harnessing Behavioral Diversity to Understand Circuits for Cognition // Current Opinion in Neurobiology. 2019. Vol. 58. P. 229–238. DOI: 10.48550/arXiv.1906.09622.
9. Макаренко А.В., Галкин В.А., Порцев Р.Ю. Свидетельство о гос. регистрации программы для ЭВМ № 2021680716 РФ; Зарег. 14.12.2021.
10. Wang C.-Y., Bochkovskiy A., Liao H. YOLOv7: Trainable Bag-of-Freebies Sets New State-of-the-Art for Real-Time Object Detectors // 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2023. P. 7454–7475. DOI: 10.1109/CVPR52729.2023.00721.
11. Михайленко И.И., Нерубенко О.Е., Мещеряков О.Д. Процесс сегментации видеоданных для обучения глубоких нейронных сетей автоматическому распознаванию функциональных состояний КРС // Аграрная Россия. 2024. № 4. С. 33–36. DOI: 10.30906/1999-5636-2024-4-33-36.

Creating a Training Dataset for Assessing the Functional States of Cattle

Irina Ivanovna Mikhailenko — Candidate of Biological Sciences, Researcher at the Laboratory of Intelligent Agricultural Technologies, Belgorod Federal Research Center of the Russian Academy of Sciences.
E-mail: ira-mik86@yandex.ru

Oleg Dmitrievich Meshcheryakov — Candidate of Agricultural Sciences, Researcher at the Laboratory of Intelligent Agricultural Technologies, Belgorod Federal Research Center of the Russian Academy of Sciences.
E-mail: meshe.64@mail.ru

Andrey Igorevich Litvinov — Junior Researcher at the Laboratory of Intelligent Agricultural Technologies, Belgorod Federal Research Center of the Russian Academy of Sciences.
E-mail: zemledel-it@yandex.ru

This article examines the analysis of possible behavioral states of cattle animals that are functionally suitable for the formation of a dataset that trains and tests neural networks. The video recordings on the basis of which the patterns were marked were taken from automated video equipment installed in a livestock facility. Based on the frequency of manifestations of various patterns of behavior, preliminary indicators of their temporal characteristics have been established and a model of joint animal states has been constructed. The results of the initial trial training of neural networks are presented.

Keywords: digitalization, automation, artificial intelligence, neural networks, machine vision, recognition of actions

REFERENCES

1. Sorokina V., Ablameyko S. Data Augmentation Method to Improve the Quality of E-commerce Image Recognition // Reliability Engineering and Computational Intelligence. Studies in Computational Intelligence. 2021. Vol. 976. P. 237–244. DOI: 10.1007/978-3-030-74556-1_14.
2. Dawkins M.S. Does Smart Farming Improve or Damage Animal Welfare? Technology and What Animals Want // Frontiers in Animal Science. 2021. Vol. 2. Art. 736536. P. 64–68. DOI: 10.3389/fanim.2021.736536.
3. Li Y., Zhou L., Yan H., Shan Y., Zheng C., Liu Y., Zuo X., Qiao B. Aircraft Detection for Remote Sensing Images Based on Deep Convolutional Neural Networks // Journal of Electrical and Computer Engineering. 2021. No. 2. P. 1–16. DOI: 10.1155/2021/4685644.
4. Ye S., Bohush R., Chen C., Chen H. Person Tracking and Reidentification for Multicamera Indoor Video Surveillance Systems // Pattern Recognition and Image Analysis. 2020. Vol. 30, No. 4. P. 827–837. DOI: 10.1134/S1054661820040136.
5. Galkin A.I. Primenenie neyrosetey i tekhnologiy bolshikh dannykh v selskom khozyaystve: povyshenie effektivnosti i ustoychivosti agroproizvodstva // Agrarnaya nauka. 2025. № 4. S. 167–171. DOI: 10.32634/0869-8155-2025-393-04-167-171 (in Russian).
6. Kumar S., Pandey A., Kondamudi S., Singh S.K. [et al.] Deep Learning Framework for Recognition of Cattle Using Muzzle Point Image Pattern // Measurement. 2017. Vol. 116. P. 1–17. DOI: 10.1016/j.measurement.2017.10.064.
7. Portsev R.Yu., Makarenko A.V. Osobennosti initializatsii svertochnykh sloev s funktsiey aktivatsii Relu v neyrosetevykh modelyakh dlya raspoznavaniya shumovykh signalov // Trudy 14-go Vserossiyskogo soveshchaniya po problemam upravleniya (VSPU-2024). 2024. S. 3071–3076. EDN: DDFCLK (in Russian).
8. Musall S., Urai A., Sussillo D., Churchland A. Harnessing Behavioral Diversity to Understand Circuits for Cognition // Current Opinion in Neurobiology. 2019. Vol. 58. P. 229–238. DOI: 10.48550/arXiv.1906.09622.
9. Makarenko A.V., Galkin V.A., Portsev R.Yu. Svidetelstvo o gos. registratsii programmy dlya EVM № 2021680716 RF; Zareg. 14.12.2021 (in Russian).
10. Wang C.-Y., Bochkovskiy A., Liao H. YOLOv7: Trainable Bag-of-Freebies Sets New State-of-the-Art for Real-Time Object Detectors // 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2023. P. 7454–7475. DOI: 10.1109/CVPR52729.2023.00721.
11. Mikhaylenko I.I., Nerubenko O.E., Meshcheryakov O.D. Protsess segmentatsii videodannykh dlya obucheniya glubokikh neyronnykh setey avtomaticheskomu raspoznavaniyu funktsionalnykh sostoyaniy KRS // Agrarnaya Rossiya. 2024. № 4. S. 33–36. DOI: 10.30906/1999-5636-2024-4-33-36 (in Russian).

Images and tables

Table 1

List of patterns to be studied

Pattern 1	"Rumination"
Pattern 2	"No rumination"
Pattern 3	"Drinking"
Pattern 4	"Lying down"
Pattern 5	"Standing still"
Pattern 6	"Banging horns on objects"
Pattern 7	"Showing interest in the neighboring cow"

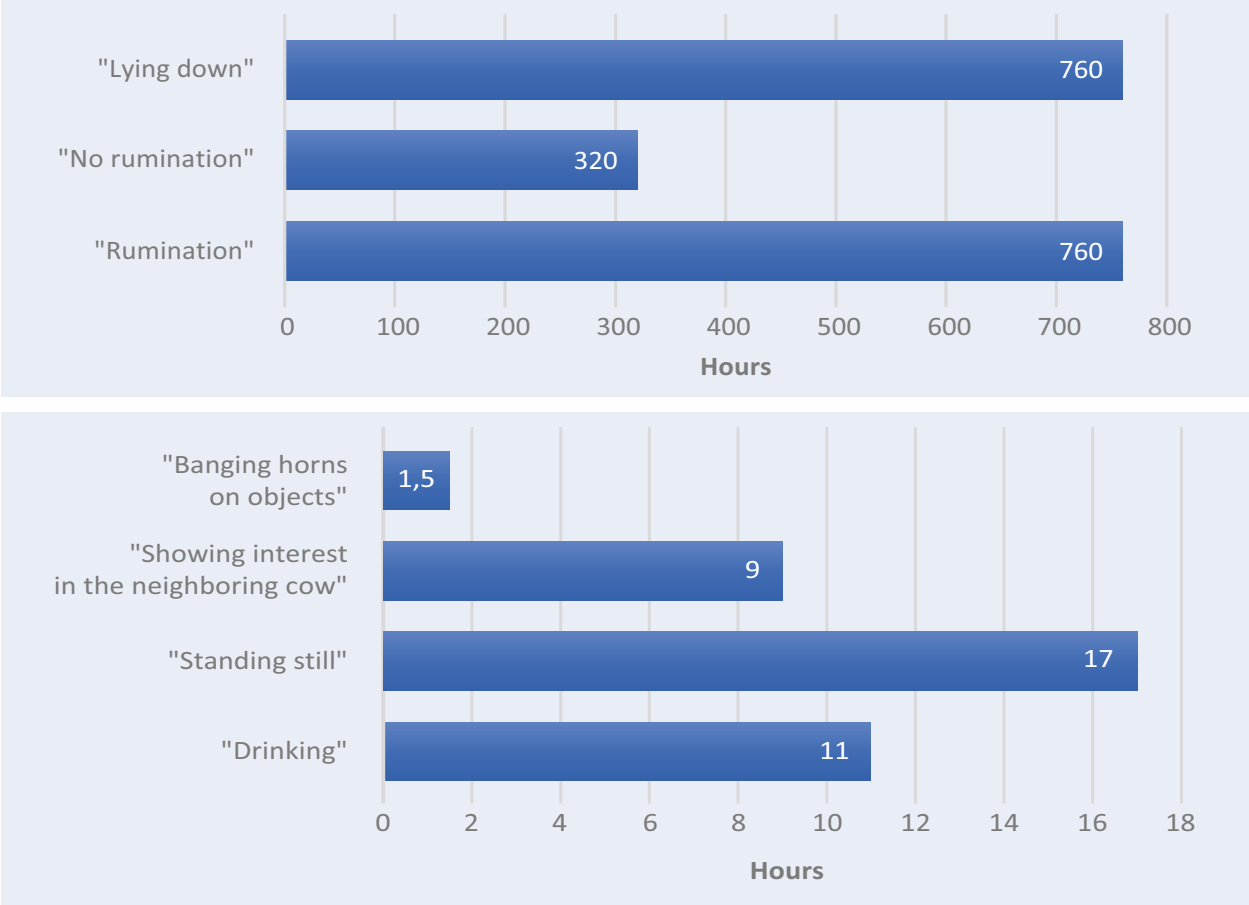


Fig. 1. *Graph of the total time spent by cattle in different states*

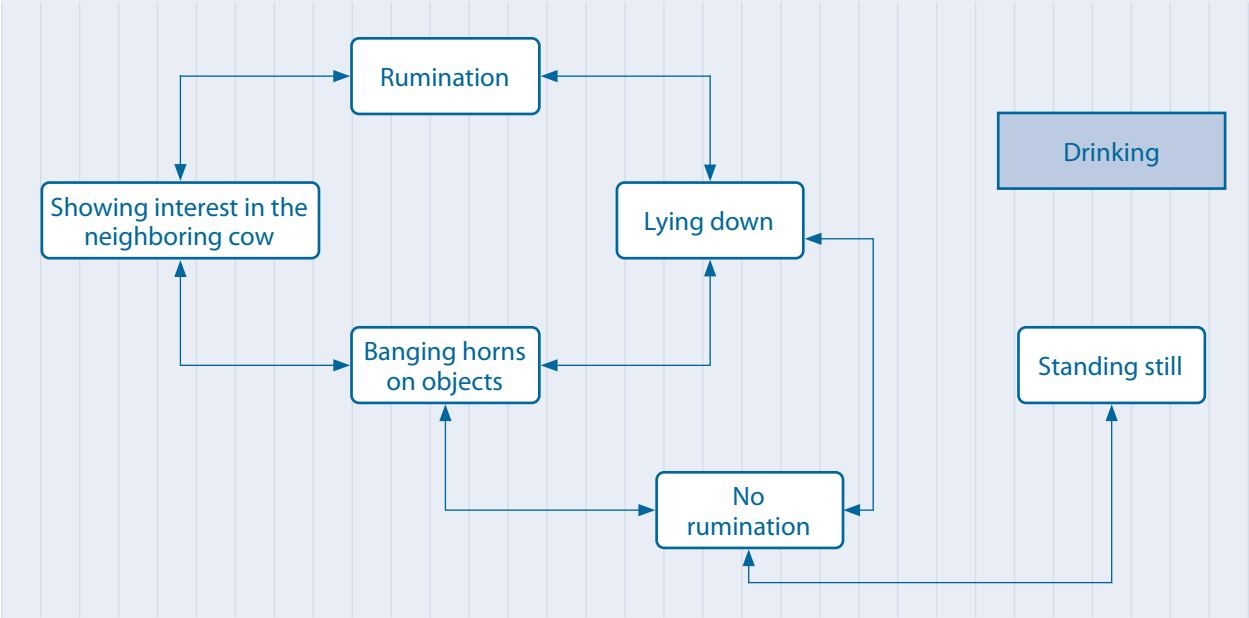


Fig. 2. *Model of joint states of cattle*

Fig. 3. *Result of the neural network operation*

Индекс УДК 330.34:004.9
Код ГРНТИ 06.52.13
DOI: 10.22204/2410-4639-2026-129-01-53-63

**А.Г. ЛОБАНОВ,
М.В. АЛИЕВ,
С.Г. ЧЕФРАНОВ,
М.Ф. АЛИЕВА***

Структурированные данные как фактор производства в цифровой экономике

В статье рассматривается трансформация роли данных в условиях цифровой экономики. Обосновывается тезис о том, что структурированные данные, встроенные в алгоритмическую инфраструктуру цифровых систем, приобретают свойства нематериального капитала и начинают функционировать как самостоятельный фактор производства. В теоретической части формализуется различие между потоками данных, данными как активом и знанием, извлекаемым из данных, а также анализируются механизмы капитализации данных — как в корпоративно-финансовом аспекте через влияние на ожидаемые денежные потоки и стоимость бизнеса, так и в учётно-оценочном аспекте через признание и стоимостную оценку цифровых активов. Показано, что институционализация знания в цифровой экономике происходит через архитектуру данных, включая схемы данных, онтологии, стандарты метаданных, правила качества и интерфейсы обмена. В прикладной части рассматривается селекционная платформа как алгоритмическая производственная система, в которой структурированные данные о генотипе, фенотипе и среде формируют контур принятия решений, автоматизируют аналитические процедуры и повышают продуктивность селекционного цикла.

Ключевые слова: цифровая экономика, экономика данных, капитализация, нематериальные активы, структурированные данные, алгоритмическая инфраструктура, производственный фактор, оценка цифровых активов, цифровая селекция

* **Лобанов Андрей Григорьевич** — старший преподаватель, ФГБОУ ВО «Адыгейский государственный университет».
E-mail: andrey.gl.pro@mail.ru

Алиев Марат Вячеславович — доцент, кандидат физико-математических наук, ФГБОУ ВО «Адыгейский государственный университет».
E-mail: alievmarat@mail.ru

Чефранов Сергей Георгиевич — доцент, доктор экономических наук, профессор кафедры информационной безопасности и прикладной информатики ФГБОУ ВО «Майкопский государственный технологический университет».
E-mail: chefranov@mkgtu.ru

Алиева Маргарита Фёдоровна — кандидат социологических наук, доцент, ФГБОУ ВО «Адыгейский государственный университет».
E-mail: aliyevamargarita@mail.ru

Введение и постановка проблемы

Современное понимание цифровой экономики (в том числе в материалах международных организаций и в российских аналитико-стратегических интерпретациях) фиксирует качественное расширение роли цифровой информации и знаний в производстве, а также рост платформенных моделей процессов, где эффективность определяется не только традиционными факторами, но и цифровыми активами и инфраструктурой [1, 2].

На уровне государственной политики в России эта логика выражается и институционально: с 2025 года заявлен запуск национального проекта «Экономика данных и цифровая трансформация государства» (2025-2030), который прямо увязывает цифровизацию экономики и социальной сферы с управлением на основе данных, развитием цифровых платформ, искусственным интеллектом (ИИ) и инфраструктурой кибербезопасности.

Достигнутый уровень цифровизации, сфера применения искусственного интеллекта и, в особенности, перспективы и темпы расширения и углубления этих процессов позволяют говорить не просто об интенсификации, но об их качественных изменениях, коснувшихся как структуры, так и содержания воспроизводственных процессов.

Связь и телекоммуникации, торговля и логистика, медицина и здравоохранение, транспорт и креативные индустрии — все эти и многие другие отрасли и сферы изменились до неузнаваемости вследствие цифровой революции и интеллектуализации.

Новое качество экономики требует учёта и оценки вклада её цифровой составляющей в национальное богатство, а это в свою очередь — уточнения и развития модельных представлений, конкретизирующих механизмы и основные факторы производства в цифровом пространстве.

Теоретическая рамка и предпосылки формализации механизма воспроизводства в цифровом пространстве

Для экономики знаний характерна цепочка «данные → информация → знание», в которой экономически значимая ценность извлекается через интерпретацию и применение данных человеком (или организацией) — т.е. данные выступают сырьём, а «производственным агентом» превращения в результат является человеческий капитал и организационные процедуры. В цифровых средах сохраняется роль человеческого капитала, но меняется структура посредников: ключевым преобразователем становятся алгоритмы и цифровые сервисы, которые масштабируемо превращают массивы структурированных данных в решения, рекомендации, прогнозы и управленческие действия [1]. Логика «цифровой экономики» в российской практике и международных трактовках прямо указывает на центральность цифровой информации/знаний и цифровых технологий для достижения социально-экономических эффектов [1, 2].

Эта трансформация особенно заметна в областях, где:

- производственный процесс опирается на многомерные наблюдения и повторяемые контуры принятия решений;
- качество решения критически зависит от объёма и сопоставимости данных;
- возможно «встраивание» знания в стандарты, схемы и модели.

В классическом понимании [3] к основным факторам производства относят: земля, труд, капитал, предпринимательские способности. Если в традиционной экономике смысловое содержание каждого из указанных факторов достаточно проработано, то в отношении цифрового пространства не всё так очевидно.

Сырые данные в исследуемом контексте могут рассматриваться как исходное сырьё цифрового производства. Однако лишь в зависимости от готовности данных к обработке можно судить об их эконо-

мической ценности. По аналогии с традиционной экономикой можно сказать, что ценность ресурса определяется степенью его подготовленности к использованию: подобно тому как в сельском хозяйстве различается целина и обработанная пашня, в цифровой среде ценность данных возрастает по мере их структурирования, стандартизации и обеспечения сопоставимости. Таким образом, степень структурирования данных и их предметное соответствие имеющимся технологиям обработки определяют ценность данных как ресурса цифровой экономики.

Капитал — в традиционной экономике здания и сооружения, оборудование и другие активы, многократно участвующие в воспроизводственных процессах. То есть капитал — это всё то, что воплощает в материальной форме технологии производства. В цифровой экономике воплощение технологий — программы и алгоритмы.

Труд — фактор производства, который не столь очевидно поддаётся осмыслению через аналогии цифровой и традиционной экономик, однако можно отметить существенную особенность: производительность труда в традиционной экономике, то есть способность выполнять определённую работу в единицу времени, аналогична техническим возможностям цифровой экономики. Таким образом, фактором производства под названием «Труд» в цифровой экономике является аппаратная составляющая — технические возможности, определяющие скорость обработки информации, возможности её хранения и передачи.

Последний из рассматриваемых здесь факторов — предпринимательство, определяющее способ и связывающее воедино другие факторы производства. Необходимо отметить, что предпринимательство всегда имеет оттенок инновационности, что отличает его от бизнеса. Цель предпринимательства — апробация нового способа соединения факторов производства и достижение на этой основе позитивных эффектов, в то время как цель бизнеса — получение дохода, в том числе за счёт уже известных способов. Однотипность множества цифровых систем и сервисов указывает на их принадлежность скорее к категории бизнеса: маркетплейсы, соцсети, сервисы такси, доставки и др. — примеры растиражированного бизнеса.

Рассмотрение комплекса факторов производства позволяет указать направления развития цифровой экономики: расширение структуры и рост объёмов данных, приращение алгоритмического потенциала — возможностей обработки информации, развитие технической (аппаратной) базы, поиск и фиксация новых эффективных способов соединения цифровых факторов производства.

Логичным продолжением идентификации основных факторов производства цифровой экономики является их оценка. Если для технической составляющей («труд» в цифровой экономике) имеется достаточно адекватная система оценки и учёта, программы и алгоритмы («капитал» цифровой экономики) представляют собой нематериальные активы, для которых также существуют методики оценки, то оценка структурированных данных вряд ли может быть полностью и адекватно учтена в существующих подходах. Современные методики измерения подчёркивают, что данные следует трактовать как нематериальный актив, который «накопляем» и создаёт сервисы в производстве, но часто выпадает из стандартного учёта и статистики, где частично учитываются лишь базы данных в составе «software & databases», при этом стоимость «наполнения» (data stores) и связанных инвестиций может быть недоучтена [4, 5].

В экономической статистике и теории усиливается тенденция рассматривать данные как особый ресурс: они дают прирост эффективности, но остаются неполно отражёнными в макро- и финансовой статистике, поскольку по своей природе ближе к нематериальным активам, чем к материальному капиталу. В международных подходах данные можно концептуализировать как «накопляемый фактор» (intangible

Рис. 1. *Схема потенциала цифровых данных*

asset), способный вносить вклад в выпуск и благосостояние через сервисы данных, а измерение инвестиций в данные требует отдельного методического контура [4, 6].

На этом фоне возникает исследовательская проблема, существенная для экономической теории, учетно-оценочной практики и прикладного управления: каким образом структурированные данные, будучи встроенными в алгоритмическую инфраструктуру, превращаются в основной фактор производства, и почему их роль в цифровой экономике становится всё более значимой.

Алгоритмическая инфраструктура как механизм реализации цифрового актива

Чтобы показать, как данные напрямую участвуют в создании ценности, полезно представить «петлю реализации потенциала цифрового актива», где данные дают услуги, услуги меняют производство, а производство производит новые данные.

В такой схеме (рис. 1) «знание» фиксируется в узлах (2)-(3): в моделях данных, правилах качества, алгоритмах и интерфейсах. Важно, что узел (4) — это уже не интерпретация человеком как обязательная стадия, а генерация предписаний к действию: задания на сбор новых данных, ранжирование альтернатив, выбор объектов для продвижения и т.п. Именно эта «операционализация знания» является отличительным признаком цифровой среды в сравнении с классической парадигмой знания.

В экономических терминах представленный здесь механизм двуедин:

1) механизм продуктивности: данные повышают точность и скорость решений, уменьшая потери и повышая выпуск при тех же ресурсах; механизм масштабирования;
2) данные как актив многократно используются в разных операционных циклах и (при наличии прав/инфраструктуры) переносятся между площадками и организациями [2].

В международных подходах к измерению стоимости данных акцентируется, что оценка должна учитывать и бизнес-модель, и возможность монетизации через разные каналы, а также ограничения (например, барьеры перемещения/агрегации данных), влияющие на способность компаний извлекать экономическую ценность [1].

Технические методы оценки данных как цифрового актива

В прикладной плоскости для оценки и учёта активов применяются три группы подходов, которые в литературе рассматриваются как адаптации классических методик [7]:

1) затратный подход — оценка затрат на создание сопоставимого массива данных (с учётом очистки, разметки, поддержания, инфраструктуры хранения и управления качеством);

2) доходный подход — оценка прироста денежных потоков (или экономии затрат), обусловленных использованием данных и связанных моделей;
3) сравнительный подход — ограниченно применим из-за слабой сопоставимости сделок и закрытости рынков данных, но может работать на частных сегментах.

Российские исследования по оценке цифровых интеллектуальных активов систематизируют факторы стоимости и показывают применимость доходного и сравнительного подходов при условии корректного описания объекта, прав и полезности [7].

Отдельный прикладной контур — оценка персональных данных как специфического вида ресурса, где предлагаются экспериментальные методики, основанные на капитализации «арендной платы» за использование данных в цифровых сервисах, и обсуждаются ограничения таких подходов. Хотя персональные данные не равны производственным данным (например, в селекции), методологическая логика важна: стоимость появляется там, где данные системно включены в цепочку создания продукта и дохода.

Экономическая формализация данных как капитала требует развести три близких, но не тождественных объекта:
1) данные как поток (data flow) — текущие наблюдения, транзакции, измерения, изображения;
2) данные как запас/актив (data asset, data stock) — организованный, управляемый и пригодный к повторному использованию массив данных с метаданными;
3) интеллект/знание, полученное из данных (data intelligence) — модели, правила, предикторы, извлечённые из данных и применяемые в производстве.

Важно отметить, что в отличие от многих традиционных активов данные обладают выраженной контекстной зависимостью экономической ценности. Их полезность определяется не только объёмом или структурой, но и соответствием конкретной технологической и производственной задаче. Поэтому часть накопленных данных со временем может терять прикладную ценность вследствие изменения оборудования, методик измерения или исследовательских задач. Однако это не является уникальным свойством данных: аналогичные процессы наблюдаются и для других видов капитала (например, технологическое устаревание оборудования или обесценение программного обеспечения). В экономическом смысле данные следует рассматривать как **актив с динамической ценностью**, зависящей от архитектуры данных, алгоритмов анализа и возможностей повторного использования в новых исследовательских и производственных контекстах.

В России учётно-оценочная проблематика цифровых активов развивается в двух линиях:
1) линия бухгалтерского учёта нематериальных активов (обновление стандартов, требования к идентификации, признанию и последующей оценке НМА);
2) линия оценочной практики цифровых интеллектуальных активов (факторы стоимости, применимость доходного/затратного/сравнительного подходов для цифровых объектов) [5, 7].

Так, в рамках отечественной исследовательской традиции, по стоимостной оценке цифровых интеллектуальных активов предлагается рассматривать их как объекты гражданского оборота с особыми факторами стоимости и применять классические подходы оценки с адаптацией к цифровой природе актива (ликвидность, полезность, правовой режим, технологические характеристики и др.) [7].

Параллельно учётные стандарты по НМА фиксируют, что объект НМА — это актив без материально-вещественной формы, а также определяют правила оценки и раскрытия информации, что усиливает потребность компаний описывать, идентифицировать и оценивать цифровые активы, возникающие в ходе цифровой трансформации [7].

С корпоративно-финансовой стороны «капитализация данных» означает, что ин-

вестиции в данные и инфраструктуру повышают ожидаемые денежные потоки и/или снижают риск/издержки (например, через автоматизацию и повышение точности решений), что отражается в стоимости бизнеса. Технически это может проявляться в росте производительности, сокращении операционных циклов, снижении транзакционных издержек и масштабировании на многосторонних рынках. Российские и международные обзоры по цифровой экономике связывают рост цифровых рынков с усилением инфраструктуры и платформенных моделей, что косвенно поддерживает механизм «данные → масштабирование → капитализация» [1, 2].

Ключевой тезис статьи требует уточнения: не любой цифровой след автоматически становится активом, а прежде всего данные, которые:

1) стандартизированы и сопоставимы (единые атрибуты, единицы, словари признаков);
2) документированы метаданными так, чтобы обеспечивать повторное использование, контроль качества и интеграцию;
3) встроены в контур алгоритмического действия — т.е. являются входом для автоматизированных процедур принятия решений/управления.

В практиках цифровой селекции, например, это выражается предельно предметно: данные фенотипирования/генотипирования/среды становятся потоковыми, ежедневно поступающими, а производительность селекционной работы связывается с оперативностью обработки и анализа непрерывно получаемого цифрового потока множества данных из различных источников [8, 9].

Стандартизация и структурирование данных — это механизм институционализации знания, потому что в стандартах закрепляются «правила мира»: что считать наблюдаемой переменной, как описывать эксперимент, как обеспечить трассируемость биологического материала и как сделать данные совместимыми. Например, стандарт метаданных MIAPPE задаёт структуру описания фенотипических экспериментов (dataset — study — biological material — observed variables) и ориентирован на гармонизацию описаний экспериментальных и вычисленных данных ради публикации и повторного использования [10].

В цифровой экономике аналогичную роль играют API-стандарты обмена данными: BrAPI описывает синтаксический уровень взаимодействия систем, снижает барьеры интеграции, поддерживает сценарии «полевые фенотипические приложения», «трекинг образцов», «загрузка/выгрузка данных» и тем самым превращает интеграцию данных из разовой «ручной работы» в инфраструктурную функцию [11].

Практический пример селекционной платформы

Почему селекция — «идеальная» область для демонстрации тезиса

Селекция — это длинный, многоцикловый производственный процесс, в котором результат (сорт/линия) создаётся через последовательность решений на основе наблюдений и испытаний. Цифровизация здесь естественно выдвигает данные в центр, потому что селекция опирается на многомерные признаки, повторяемые эксперименты, сложные взаимодействия «генотип — среда» и возрастающие объёмы измерений (включая изображения и сенсорные потоки). Российские материалы по цифровой трансформации в растениеводстве подчёркивают рост потоков цифровых данных с полей, применение машинного зрения и ИИ для сбора фенотипической информации и значимость высокопроизводительных платформ фенотипирования [8, 9].

Таким образом, практика цифровой селекции и фенотипирования демонстрирует удобный для иллюстрации тип процессов: рост потоков цифровых данных с полей, интеграция машинного зрения и ИИ, переход к «сквозным» моделям селекционно-семеноводческих процессов и к интегрированному геномно-экологическому прогнозированию [8, 9].

Кроме того, селекция хорошо иллюстрирует, как структурированные данные начинают структурировать сам процесс производства: если набор признаков (traits), методы измерения и формат описания закреплены стандартами и корпоративными справочниками, то они превращаются в «регламент производства данных», а затем — в регламент производства решений. В этом смысле данные и метаданные работают как «технологическая карта» (но в цифровом виде).

Референсная архитектура селекционной платформы

В качестве иллюстративного кейса рассмотрим типовую архитектуру селекционной платформы управления данными и анализом, совместимую с распространёнными стандартами (MIAPPE/BrAPI) и реализуемую, в частности, в программных комплексах класса BreedBase: платформа поддерживает проектирование полевых раскладок, сбор фенотипов (в т.ч. на мобильных устройствах), сопровождение отбора и трекинг генотипирования, хранение высокоплотных генотипических данных и выполнение анализов/предсказаний для геномной селекции, при этом заявлена поддержка стандарта BrAPI [10, 11].

1. Источники данных:
   a. Поле (фенотипы, изображения, БПЛА/сенсоры)
   b. Лаборатория (генотипирование/секвенирование)
   c. Среда (погода, почва, агрофоны) | v ETL/ELT и управление качеством (валидаторы, справочники признаков, единицы)
2. Хранилище/витрины данных:
   a. Паспорт генетического материала
   b. Эксперименты/испытания
   c. Наблюдения/признаки
3. Аналитика и «контур решения»:
   a. Статистическая обработка/BLUP/индексы
   b. Прогнозирование, ML, геномная/геномно-экологическая модель
   c. Ранжирование линий/решения по продвижению
4. Workflow-движок (задания и регламенты):
   a. План фенотипирования (что/где/когда измерить)
   b. Трекинг образцов и лабораторных партий
   c. План скрещиваний/полевых испытаний
5. Исполнение решений
6. Новые данные

Эта архитектура принципиально отличается от «табличного учёта результатов» тем, что данным приписывается активная роль: они становятся управляющим сигналом в workflow-движке, генерируя задания и ограничивая пространство допустимых операций. Именно здесь и проявляется тезис о данных как факторе производства: без структурированных данных (паспортов, наблюдений, метаданных, связей) платформа не может формировать задания, а алгоритмы не могут производить воспроизводимые решения.

Как структурированные данные «определяют деятельность» селекционеров

Нормирование того, что считать признаком и наблюдением. Стандарты метаданных фиксируют состав объекта исследования и переменных наблюдения. В MIAPPE «observed variable» определяется как сочетание «признак — метод — единица измерения» (с возможностью детализации по части растения), а набор таких переменных становится обязательным «каркасом» сбора данных [10]. Это означает, что решение «что измерять» частично институционализируется в стандарте и корпоративных справочниках.

Автоматизация сбора фенотипов и превращение поля в «поток данных». Материалы по цифровой трансформации селекции фиксируют, что машинное зрение и ИИ позволяют собирать фенотипическую информацию с цифровых изображений посевов, а распространение БПЛА и камер делает массовый сбор изображений доступным; при этом точность распоз-

навания зависит от алгоритма, а объёмы данных в селекционном процессе непрерывно растут и формируют ежедневный цифровой поток [8]. Это фактически переводит часть фенотипирования в режим индустриального производства данных.

Интеграция генотип – фенотип – среда как единый объект управления. Для «умной селекции» описывается переход к интегрированному геномно-экологическому прогнозированию, где продуктивность/фенотип растения представляется функцией генотипа, среды и их взаимодействия (GxE), а объединение этих компонент повышает мощность моделей прогнозирования и снижает ошибку решений [9]. В таком режиме ценность данных возрастает не «после интерпретации», а в момент включения в модель, которая генерирует предписания по отбору.

Превращение анализа в производственную операцию. Платформа осуществляет поддержку геномной селекции в виде анализов и предсказаний. Это означает, что селекционер получает не просто таблицы, а автоматизированный операционный контур: загрузка данных → расчёт показателей → ранжирование линий → формирование планов работ. В такой системе значительная часть «знания о том, как выбирать» схвачена и воспроизводится через данные и алгоритмы.

Экономическая интерпретация эффекта в селекционном цикле. Экономический эффект «данных как фактора» в селекции корректнее описывать не через разовые выгоды, а через изменение параметров производственного цикла:

1) повышается точность решений (выбор линий/скрещиваний) за счёт интеграции больших массивов данных и предиктивного моделирования;
2) сокращается время/издержки на сбор и обработку фенотипов за счёт высокопроизводительного фенотипирования, машинного зрения, автоматизации;
3) снижаются потери качества из-за человеческого фактора, потому что «сквозные модели» и робототехнические/цифровые контуры ориентированы на воспроизводимость и контроль неопределённости [8, 9].

Указанные направления прямо фиксируются в российских материалах по цифровой трансформации селекции (рост потоков данных, автоматизация, «сквозные» модели, повышение производительности и снижение неопределённостей) и в международных обзорах по высокопроизводительному фенотипированию (переход к быстрым, повторяемым, количественным измерениям и рост роли анализа данных, сенсоров, робототехники и вычислительных ресурсов).

С точки зрения капитализации это означает: создаётся актив (данные средовые, фенотипические и генетические), который многократно используется, улучшает производственную функцию селекционного предприятия и увеличивает будущие денежные потоки (через сортовые преимущества, лицензионные доходы, снижение затрат селекционного цикла и т.п.). Чтобы этот эффект стал «стоимостным», требуется механизм оценки: либо через доходный подход (прирост эффекта/денежных потоков), либо через затратный (стоимость воспроизводства данных и сопутствующей инфраструктуры), что хорошо согласуется с российскими рамками оценки цифровых интеллектуальных активов и ИТ-активов [5, 7].

Выводы

Смена логики реализации факторов производства в цифровой экономике проявляется в том, что структурированные данные, будучи встроенными в алгоритмическую инфраструктуру, начинают выступать не только объектом интерпретации, но и операциональным ресурсом, непосредственно функционирующим и создающим экономическую ценность через автоматизированное принятие решений и управление процессами. Это согласуется с современными методическими подходами к трактовке данных как нематериального актива и накопляемого фактора,

который пока неполно отражён в стандартных статистических и учётных контурах, но требует отдельного измерения инвестиций и запасов данных [1, 4].

Ключевой механизм «институционализации знания» в цифровой среде — перенос регулятивной и когнитивной составляющей знания в архитектуру данных: стандарты метаданных (MIAPPE), API-интерфейсы (BrAPI), справочники признаков и единиц, правила качества, процедуры трассируемости и workflow-модели [10, 11]. В результате структурированные данные начинают буквально «структурировать» производство: определяют, что и как собирать, какие проверки выполнять, как интегрировать, какие решения и задания формировать.

Пример селекционной платформы демонстрирует предельную форму этой логики: в цифровой селекции поток фенотипических/генотипических/средовых данных превращается в актив, который задаёт регламенты и решения (от планов фенотипирования до ранжирования линий и планов испытаний), а экономический результат возникает через повышение точности, скорости и воспроизводимости селекционного цикла [8, 9]. Такой пример позволяет рассматривать структурированные данные как фактор производства, сопоставимый по функции с капиталом, поскольку они накопляемы, многократно используются, требуют инвестиций и управления и участвуют в формировании потока доходов.

Наконец, учётно-оценочная практическая импликация заключается в необходимости развивать стандартизированные процедуры идентификации и оценки данных как цифровых активов: через совмещение требований учёта НМА и методик стоимостной оценки цифровых интеллектуальных активов/ИТ-активов, с учётом специфики прав, полезности, качества метаданных и технологической встраиваемости данных в принятие решений [5, 7]. Российская регуляторика НМА и исследования по оценке цифровых активов задают основу для такого контура, но для данных как самостоятельного объекта требуется дополнительная методология (включая оценку «амортизации данных» и дрейфа), что подтверждается международными работами по измерению данных как актива.

ЛИТЕРАТУРА

1. Goldfarb A., Tucker C. Digital Economics // Journal of Economic Literature. 2019. Vol. 57, No. 1. P. 3–43. DOI: 10.1257/jel.20171452.
2. Meltzer J.P. The Internet, Cross-Border Data Flows and International Trade // Asia & the Pacific Policy Studies. 2015. Vol. 2, No. 1. P. 90–102. DOI: 10.1002/app5.60.
3. Макконнелл К.Р., Брю С.Л. Экономикс: принципы, проблемы и политика = Economics: Principles, Problems, and Policies. Т. 2. М.: Республика, 1992. ISBN 5-250-01486-0.
4. Corrado C., Haskel J., Jona-Lasinio C., Iommi M. Intangible Capital and Modern Economies // Journal of Economic Perspectives. 2022. Vol. 36, No. 3. P. 3–28. DOI: 10.1257/jep.36.3.3.
5. Lev B., Zarowin P. The Boundaries of Financial Reporting and How to Extend Them // Journal of Accounting Research. 1999. Vol. 37, No. 2. P. 353–385.
6. Jones C.I., Tonetti C. Nonrivalry and the Economics of Data // American Economic Review. 2020. Vol. 110, No. 9. P. 2819–2858. DOI: 10.1257/aer.20191330.
7. Лосева О.В., Косорукова И.В., Федотова М.А., Тазихина Т.В., Абдикеев Н.М. Оценка стоимости цифровых интеллектуальных активов: принципы, факторы, подходы и методы // Финансы: теория и практика. 2022. Т. 26. № 4. С. 6–28. DOI: 10.26794/2587-5671-2022-26-4-6-28.
8. Araus J.L., Cairns J.E. Field high-throughput phenotyping: the new crop breeding frontier // Trends in Plant Science. 2014. Vol. 19, No. 1. P. 52–61. DOI: 10.1016/j.tplants.2013.09.008.

9. Crossa J., Pérez-Rodríguez P., Cuevas J. [et al.] Genomic selection in plant breeding: methods, models, and perspectives // Trends in Plant Science. 2017. Vol. 22, No. 11. P. 961–975. DOI: 10.1016/j.tplants.2017.08.011.
10. Papoutsoglou E.A., Faria D., Arend D. [et al.] Enabling reusability of plant phenomic datasets with MIAPPE 1.1 // New Phytologist. 2020. Vol. 227, No. 1. P. 260–273. DOI: 10.1111/nph.16544.
11. Selby P., Abbeloos R., Backlund J. E. [et al.] BrAPI – an application programming interface for plant breeding applications // Bioinformatics. 2019. Vol. 35, No. 20. P. 4147–4155. DOI: 10.1093/bioinformatics/btz190.

Structured Data as a Factor of Production in the Digital Economy

Andrey Grigorevich Lobanov — Senior Lecturer, Adyghe State University.
E-mail: andrey.gl.pro@mail.ru

Marat Vyacheslavovich Aliev — PhD in Physics and Mathematics, associate professor, Adyghe State University.
E-mail: alievmarat@mail.ru

Sergey Georgievich Chefranov — Docent, Doctor of economics, Professor of the Department of Information Security and Applied Informatics, Maikop State Technological University.
E-mail: chefranov@mkgtu.ru

Margarita Fedorovna Aliyeva — Ph.D. in Sociology, associate professor, Adyghe State University.
E-mail: aliyevamargarita@mail.ru

The article examines the transformation of the role of data in the context of the digital economy. It substantiates the thesis that structured data embedded in the algorithmic infrastructure of digital systems acquire the properties of intangible capital and begin to function as an independent factor of production. The theoretical section formalizes the distinction between data flows, data as an asset, and knowledge derived from data, and analyzes the mechanisms of data capitalization — both in the corporate-financial sense, through their influence on expected cash flows and firm value, and in the accounting and valuation sense, through the recognition and valuation of digital assets. The study shows that the institutionalization of knowledge in the digital economy occurs through data architecture, including data schemas, ontologies, metadata standards, quality rules, and data exchange interfaces. The applied section examines a breeding platform as an algorithmic production system in which structured data on genotype, phenotype, and environment form the decision-making framework, automate analytical procedures, and increase the productivity of the breeding cycle.

Keywords: digital economy, data economy, capitalization, intangible assets, structured data, algorithmic infrastructure, factor of production, digital asset valuation, digital breeding

REFERENCES

1. Goldfarb A., Tucker C. Digital Economics // Journal of Economic Literature. 2019. Vol. 57, No. 1. P. 3–43. DOI: 10.1257/jel.20171452.
2. Meltzer J.P. The Internet, Cross-Border Data Flows and International Trade // Asia & the Pacific Policy Studies. 2015. Vol. 2, No. 1. P. 90–102. DOI: 10.1002/app5.60.

3. Makkonnell K.R., Bryu S.L. Ekonomiks: printsipy, problemy i politika = Economics: Principles, Problems, and Policies. T. 2. M.: Respublika, 1992. ISBN 5-250-01486-0 (in Russian).
4. Corrado C., Haskel J., Jona-Lasinio C., Iommi M. Intangible Capital and Modern Economies // Journal of Economic Perspectives. 2022. Vol. 36, No. 3. P. 3–28. DOI: 10.1257/jep.36.3.3.
5. Lev B., Zarowin P. The Boundaries of Financial Reporting and How to Extend Them // Journal of Accounting Research. 1999. Vol. 37, No. 2. P. 353–385.
6. Jones C.I., Tonetti C. Nonrivalry and the Economics of Data // American Economic Review. 2020. Vol. 110, No. 9. P. 2819–2858. DOI: 10.1257/aer.20191330.
7. Loseva O.V., Kosorukova I.V., Fedotova M.A., Tazikhina T.V., Abdikeev N.M. Otsenka stoimosti tsifrovykh intellektualnykh aktivov: printsipy, faktory, podkhody i metody // Finansy: teoriya i praktika. 2022. T. 26. № 4. S. 6–28. DOI: 10.26794/2587-5671-2022-26-4-6-28 (in Russian).
8. Araus J.L., Cairns J.E. Field high-throughput phenotyping: the new crop breeding frontier // Trends in Plant Science. 2014. Vol. 19, No. 1. P. 52–61. DOI: 10.1016/j.tplants.2013.09.008.
9. Crossa J., Pérez-Rodríguez P., Cuevas J. [et al.] Genomic selection in plant breeding: methods, models, and perspectives // Trends in Plant Science. 2017. Vol. 22, No. 11. P. 961–975. DOI: 10.1016/j.tplants.2017.08.011.
10. Papoutsoglou E.A., Faria D., Arend D. [et al.] Enabling reusability of plant phenomic datasets with MIAPPE 1.1 // New Phytologist. 2020. Vol. 227, No. 1. P. 260–273. DOI: 10.1111/nph.16544.
11. Selby P., Abbeloos R., Backlund J.E. [et al.] BrAPI – an application programming interface for plant breeding applications // Bioinformatics. 2019. Vol. 35, No. 20. P. 4147–4155. DOI: 10.1093/bioinformatics/btz190.

Image

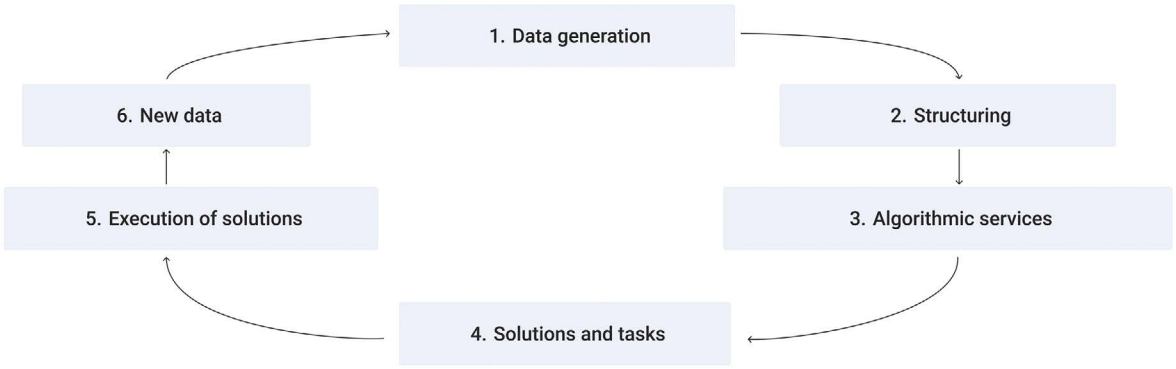
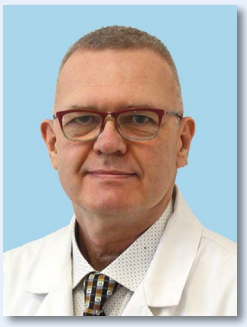


Fig. 1. *Diagram of the potential of digital data*

Индекс УДК 004.82:616.322-002
Код ГРНТИ 28.23.13:76.29.54
DOI: 10.22204/2410-4639-2026-129-01-64-75



В.А. БЕЛОВ,
Б.А. КОБРИНСКИЙ,
А.А. АКИМОВА*

Экспертный подход к формированию признакового пространства факторов риска хронического тонзиллита у детей

Системы искусственного интеллекта в медицине позволяют эффективно решать различные задачи, в частности, связанные с выявлением факторов, угрожающих развитием заболеваний. Профилактика и ранняя диагностика хронического тонзиллита остаётся одной из ведущих проблем оториноларингологии. Воспаление миндалин, в том числе хронический тонзиллит, может приводить к различным осложнениям, включая системные заболевания. Этим определяется значение профилактических мероприятий, учитывающих наличие угрожающих факторов на донозологическом этапе. В статье рассматривается проблема экспертной оценки контролируемых факторов риска развития хронического тонзиллита, их объективная характеристика с учётом возможной неопределённости. В связи с этим введено представление факторов с их характеристиками, сопровождаемыми соответствующими числовыми значениями. Каждая характеристика сопровождается экспертной оценкой уровня риска, что является оригинальным решением для систем искусственного интеллекта. На этой основе построен вопросник с альтернативными ответами, включающий актуальные факторы риска развития хронического тонзиллита. Структурированные показатели – предикторы заболевания – формируют поле знаний риск-факторов хронического тонзиллита, что послужит базой знаний интеллектуальной рекомендательной системы.

Ключевые слова: экспертные знания, признаковое пространство, структуризация знаний, факторы риска, оценка риска, хронический тонзиллит

* **Белов Владимир Алексеевич** — кандидат медицинских наук, заведующий отделением оториноларингологии НИКИ педиатрии и детской хирургии им. Ю.Е. Вельтищева, РНИМУ им. Н.И. Пирогова Минздрава России, ФГБОУ ДПО РМАНПО Минздрава России.
E-mail: belov_v_a@mail.ru

Кобринский Борис Аркадьевич — академик РАЕН, профессор, доктор медицинских наук, заведующий отделом систем интеллектуальной поддержки принятия решений, заслуженный деятель науки Российской Федерации ФИЦ «Информатика и управление» РАН, ФГАОУ ВО РНИМУ им. Н.И. Пирогова Минздрава России.
E-mail: kba_05@mail.ru

Акимова Анна Анатольевна — специалист отдела систем интеллектуальной поддержки принятия решений, ФИЦ «Информатика и управление» РАН.
E-mail: anna.djerg@mail.ru

Введение

В указе Президента № 309 от 7 мая 2024 года «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» важнейшей определена цифровая трансформация государственного и муниципального управления, экономики и социальной среды. Здравоохранение является одним из ведущих направлений социума, и именно искусственный интеллект может послужить решению сложных проблем медицины, включая выявление предболезненных состояний, и реализовать персонализированный подход в профилактике патологических состояний. Сохранение здоровья населения за счёт профилактических мероприятий является одним из приоритетов «Стратегии развития здравоохранения в Российской Федерации на период до 2030 года», утверждённой Указом Президента Российской Федерации от 8 декабря 2025 г. N 896. Рост числа случаев хронических заболеваний отмечается во всех странах, что является одной из важнейших проблем здравоохранения в XXI веке [1]. Длительный характер хронических заболеваний существенно влияет на качество жизни людей и приводит к значительным расходам государства на здравоохранение из-за лечебных мероприятий, повторных госпитализаций и инвалидности [2]. Хронический тонзиллит (ХТ) и его осложнения не являются исключением.

Несмотря на многоплановые исследования и определённые достижения в разработке и оптимизации лечебно-диагностического алгоритма, частота хронической патологии миндалин в настоящее время возросла в 1,5 — 1,8 раза по сравнению с 70-ми годами XX века [3].

Нёбные миндалины служат первым барьером на пути микробных антигенов и участвуют в непрерывных иммунных реакциях, которые помогают поддерживать местный и системный иммунологический гомеостаз. Воспаление миндалин может оказывать влияние на отдалённые органы, в том числе на сердце, почки и суставы. Нёбные миндалины являются естественным природным резервуаром для рецидивирующих инфекций, которые могут являться причиной возникновения таких заболеваний, как гломерулонефрит, острый ревматоидный артрит, эндокардит и миокардит [4,5]. Неблагоприятное течение хронического тонзиллита может приводить к тонзилоиндуцированному аутоиммунному/воспалительному процессу (Tonsil-induced autoimmune/inflammatory syndrome — TIAS), характеризующемуся нарушением регуляции иммунитета и хроническим воспалением. TIAS включает такие заболевания, как ревматическая лихорадка, IgA-нефропатия и псориаз. Предполагается, что эти состояния могут быть вызваны нарушением иммунной толерантности к микроорганизмам, обитающим в миндалинах [4, 6].

Хронический тонзиллит выявляется, в основном, при появлении жалоб и первых симптомов. Это может происходить в процессе профилактических осмотров. Континуум переходных состояний нёбных миндалин при развитии хронического тонзиллита движется через функциональные отклонения (включая клеточный уровень) и пограничные состояния, в направлении нарушения функций (от возникновения ХТ к возникновению вышеназванных заболеваний) [7].

В последнее десятилетие намечается переход от лечения уже развившихся заболеваний к воздействиям на донозологическом этапе: к прогностической, профилактической, персонализированной медицине, учитывающей различные факторы риска, что предполагает вовлеченность пациента и соответствует 4P медицине [7-10]. Этот сдвиг парадигмы в пользу предупреждения хронической патологии в условиях широкой цифровизации системы здравоохранения, включая методы и технологии искусственного интеллекта (ИИ), позволяет, наряду с поддержкой врачей в принятии диагностических, прогностических и лечебных решений, углублять контакты с пациентами в процессе профилактических мероприятий и при контроле за их

состоянием, в том числе с использованием дистанционных средств общения [11, 12].

Существует множество определений понятия «риск для здоровья», в докладе ВОЗ он трактуется как «фактор, повышающий вероятность неблагоприятных последствий для здоровья» [13]. Восприятие риска включает социальное измерение, которое делает его профилактику сложной. Люди подвергаются риску неравным образом. Поэтому важно, чтобы они получали лучшую поддержку в отношении рисков подверженности болезни [14]. Соответственно, рекомендации по снижению рисков должны носить индивидуальный и ситуативный характер, обращая внимание родителей детей на актуальные риски.

Важную роль в регулярном анализе динамически изменяющихся факторов риска (ФР) и профилактике заболеваний играют рекомендательные интеллектуальные медицинские системы, в рамках которых может эффективно осуществляться мониторинг изменений, характерных для нечётких донозологических ситуаций [15, 16]. Они обеспечивают мониторинг факторов, способствующих развитию заболеваний, и предлагают доступные для человека мероприятия. Контроль за появлением и динамикой персональных факторов риска отвечает концептуальному изменению тактики — от лечения возникшего хронического тонзиллита к профилактическим мероприятиям.

Целью настоящего исследования являлась экспертная оценка и концептуализация факторов риска хронического тонзиллита для разработки в дальнейшем интеллектуальной рекомендательной системы профилактической направленности.

Материал и методы

Исходным материалом послужили данные литературы, содержащие информацию о факторах, угрожающих развитием хронического тонзиллита. Были проанализированы литературные источники из баз данных: ELibrary, Google Scholar, PubMed — и отобраны обсервационные исследования (перекрёстные, «случай-контроль», когортные), в которых рассматривались ФР развития хронического тонзиллита.

Аналитический метод был использован в процессе поиска информации о факторах риска в литературе.

Структурирование отобранных экспертным путём факторов риска осуществлялось методами инженерии знаний, являющейся необходимым условием для формирования баз знаний систем искусственного интеллекта [17].

Факторы риска хронического тонзиллита

При воздействии на организм повреждающих факторов имеют место специфические и неспецифические изменения. Неспецифические изменения зависят от реактивности организма, определяя его адаптационную реакцию. Эти изменения могут возникать задолго до клинических проявлений и отражать развитие патологического процесса на ранних стадиях. В случае срыва молекулярных компенсаторных механизмов адаптации создаются условия для перехода патологического процесса на более высокие уровни (субклеточный, клеточный, тканевой, органный), способствуя патологическим изменениям. Это определяет необходимость контроля за предрасполагающими факторами, способствующими нарушению процессов регуляции, что отражает континуальная модель развития и течения хронического тонзиллита [7].

Донозологические мероприятия, ориентированные на предупреждение развития хронического тонзиллита, предполагают выявление факторов риска. На первом этапе был проведён поиск актуальных факторов риска развития хронического тонзиллита. В процессе анализа литературных источников были выявлены наиболее значимые факторы, способствующие развитию хронического тонзиллита, на которые было обращено внимание в проведённых исследованиях [18-22]. Их можно подразделить на этногеографические, наследственные, медико-социальные, медицинские (характеризующие состояние здоровья индивидуу-

ма). Этногеографические факторы включают сведения о проживании местного или мигрирующего населения в приполярных территориях. Воспаление миндалин сравнительно часто развивается в детстве, что можно объяснить влиянием экологических факторов: контакт с холодным воздухом, вирусная и бактериальная агрессия. Математическое моделирование показало, что генетические эффекты объясняют 62% вариабельности предрасположенности к рецидивирующему тонзиллиту [23, 24].

Факторы риска были подразделены на неуправляемые, на которые отсутствует возможность воздействия, и управляемые (модифицируемые). К неуправляемым (не модифицируемым) факторам риска относятся возраст, пол, наследственность (повышение риска при наличии хронического тонзиллита у родственников первой линии родства, в том числе подвергшихся тонзилэктомии), этнические особенности (к примеру, у коренных народов Севера распространённость хронического тонзиллита гораздо выше), воздействие окружающей среды, с которыми человек сталкивается ежедневно (так, на риск развития ХТ влияет география и место проживания, к примеру, длительное проживание некоренного населения в приполярных областях). К управляемым факторам риска, в первую очередь, относятся особенности образа жизни и привычки человека (на повышенный риск развития ХТ влияет активное и пассивное табакокурение, онихофагия). Сопутствующие заболевания, которые могут повышать вероятность развития хронического тонзиллита, можно отнести к частично модифицируемым ФР. Это частые респираторные инфекции, особенно с жалобами на дискомфорт и боли в горле, гипертрофия миндалин, аллергическая патология, ларинго-фарингеальный рефлюкс, кариес, заболевание парадонта и т.п. [18-24].

Формирование признакового пространства факторов риска

Знания о факторах риска, в контексте данного исследования, представляют собой суммацию литературных знаний, подвергнутых опыту эксперта. Их получение и особенности представления в структурированной и формализованной форме являются результатом обработки с помощью методов инженерии знаний, являющейся ветвью искусственного интеллекта.

Каждый ФР описан с указанием его наименования (атрибута, от лат. attributio — свойство), характеристики или вида проявления и соответствующего значения атрибута, представленного в качественной или количественной форме. Тройки «атрибут — характеристика атрибута — значение атрибута» формируют полноценное семантическое понятие фактора риска. Нечёткость и неопределённость, имеющие место в представлении факторов риска, были уточнены в процессе их структурирования. Характеристика атрибута может включать и возрастные ограничения, позволяющие сфокусировать внимание на особенностях, характерных для определённого периода жизни.

Формат структурированного представления факторов риска можно видеть из примеров, включённых в таблицу 1.

Результатом структуризации является поле знаний — структурированное описание понятий и взаимосвязей между понятиями проблемной области, представленными на основе анализа литературы и знаний эксперта. Признаковое пространство уточнялось, что крайне важно, в процессе его формирования и впоследствии, при введении экспертных оценок. Признаковое пространство факторов риска ХТ состояло из 16 факторов, включавших 42 характеристики. Не модифицируемых факторов риска было 5, модифицируемых — 11.

Экспертная оценка факторов риска

Оценка риска — это рациональная процедура, которая вносит значительный вклад в принятие решений [25, 26].

Информация для измерения риска, полученная из баз данных на основе частоты возникновения конкретного события, может быть недостаточной или искажённой. Более

Таблица 1

Фрагмент структурированного представления знаний о факторах риска хронического тонзиллита

Фактор риска (атрибут)	Характеристика атрибута	Значение атрибута
Отягощённый семейный анамнез	Наличие хронического тонзиллита в семье	Родственники I линии родства
	Наличие тонзиллэктомий в семье	Родственники I линии родства
	Коренные народы Севера	Мать
		Отец
География проживания	Проживание в приполярных и заполярных регионах (пришлое население)	> 5 лет
	Проживание в приполярных и заполярных регионах (пришлое население)	< 5 лет
	Сосание пальцев	Присутствует
Кариес	Выявление кариеса, в том числе излеченного (включая пломбированные зубы)	≥ 1 раза в год
		≤ 1 раза в 2 года
		≤ 1 раза в 3 года
Респираторные заболевания	С симптомами тонзиллита, болями в горле	≥ 4 раз в данный год
		2-3 раза в данный год
		1 раз в данный год
		≥ года назад

Таблица 2

Фрагмент структурированного представления факторов риска хронического тонзиллита с экспертными оценками

Фактор риска (атрибут)	Характеристика атрибута	Значение атрибута	Уровень риска
Отягощённый семейный анамнез	Наличие хронического тонзиллита в семье	Родственники I линии родства	Высокий
	Наличие тонзилэктомий в семье	Родственники I линии родства	Очень высокий
Этнические особенности	Коренные народы Севера	Мать	Высокий
	Коренные народы Севера	Отец	Средний
Ринит	Рецидивирующий	В настоящее время	Высокий
		В анамнезе	Средний

точным может быть характеристика риска, уточнённая экспертами [15, 27]. Формализация суждений делает представления более явными и структурированными [26, 28]. Факторы риска, отобранные на основе анализа литературных источников и подвергшиеся структуризации, затем оценивались врачом-экспертом совместно с когнитологом. Некоторая субъективность экспертного суждения может быть преодолена путём использования накопленной информации [15, 26]. Такой подход делает акцент на знаниях, включающих опыт экспертов и доказательства.

Принципиально важным является понимание значимости каждого фактора риска с учётом выделенных характеристик. Экспертная оценка уровня риска осуществлялась по 5-балльной шкале: очень высокий, высокий, средний (умеренный), низкий, очень низкий. Пример факторов риска, сопровождаемых экспертными оценками, представлен в таблице 2.

Анкета-опросник для сбора информации о факторах риска у пациента

На основе отобранных факторов риска для выявления угрозы развития заболевания был разработан опросник с альтернативными ответами, ориентированный на заполнение его как врачом, так и пациентом или его родителями.

Вопросы сформулированы так, чтобы они интерпретировались одинаково, относительно независимо от образовательного, культурного уровня респондентов [29]. Респонденту предлагается сделать выбор из перечня альтернативных ответов на каждый вопрос. Примером может служить ответ на представленный ниже вопрос:

«Переселялись ли Вы в приполярные или заполярные регионы (если проживали и там, и там, то выберите тот вариант ответа, где проживали дольше)?»

- Нет
- Да, в приполярных менее 5 лет
- Да, в заполярных менее 5 лет
- Да, в приполярных более 5 лет
- Да, в заполярных более 5 лет

Более объективным является вариант заполнения анкеты в процессе интервьюирования пациентов или родителей ребёнка врачом. В этом случае появляется возможность корректировки недостаточно ясных ответов. Кроме того, у врача-интервьюера есть возможность представить и объяснить респонденту цель исследования, побудить дать откровенные ответы. Полноценность и правильность ответов повышают качество выявляемых факторов риска.

Обсуждение полученных результатов

В практике здравоохранения в большинстве случаев диагноз хронического тонзиллита опирается на местные клинические проявления. В основном проводится «профилактика развития» уже возникшего хронического тонзиллита, проявляющаяся минимальными значимыми клиническими симптомами [30].

Донозологическая диагностика представляет собой комплекс предсказательных факторов, указывающих на возможность развития болезни. Это видно из начального периода континуума переходных состояний организма в процессе формирования хронического тонзиллита [7].

Для профилактики болезней необходимо выявить причины их возникновения, чтобы затем воздействовать на них, то есть на те ФР, которые лежат в их основе [13]. Подходы к разработке сценариев, основанные на правдоподобии, были выдвинуты на первый план как подходящая практика для управления рисками, такими как системные риски и возникающие риски [25]. Системными рисками являются исходно присутствующие у пациента, такие как наследственные факторы. Возникающими — появляющиеся в процессе жизни, например, кариес. По мнению R. Flage [27], концепция правдоподобия предлагает ряд ценных идей, поскольку она включает в себя два ключевых аспекта риска: вероятность и знание.

Следствием уточняющих вопросов к эксперту явилось выявление определённой нечёткости в характеристике факторов риска хронического тонзиллита у детей. Структурирование факторов риска позволяет более подробно их характеризовать, что приводит к детализации уровня риска (например, различной продолжительности проживания на крайнем севере). Структурированные факторы риска являются основой для учёта их трансформации в процессе жизни. Это позволяет осуществлять оперативную переоценку уровня риска, что будет вести к изменению профилактических рекомендаций.

Заключение

Методы искусственного интеллекта позволяют значительно повысить эффективность исходной медицинской информации, превратив часто расплывчатые данные в чёткие знания, пригодные для построения систем интеллектуальной поддержки принятия клинических решений.

Контроль факторов риска является основой для выявления пациентов, находя-

щихся под угрозой развития хронического тонзиллита. При этом необходимо отметить, что каждый фактор риска должен сопровождаться его характеристикой, указывающей на особенности проявления, и значением, указывающим на качественные или количественные его проявления и временные ограничения. Их мониторинг позволит повысить регулярность контроля динамики изменений и обеспечить персонализированный подход к профилактическим воздействиям, основанный на сопоставлении имеющихся у пациента признаков с известными факторами риска, сопровождающимися оценками уровня угрозы для развития заболевания [26, 28]. Важно отметить, что даже очень высокий уровень риска ХТ не означает, что заболевание манифестирует в ближайшее время.

Рассмотренный подход к представлению факторов риска является основой для создания рекомендательной системы компьютерной поддержки профилактики ХТ на донозологическом этапе.

ЛИТЕРАТУРА

1. Hajat C., Stein E. The Global Burden of Multiple Chronic Conditions: A Narrative Review // Prev. Med. Rep. 2018. Vol. 12. P. 1–14. DOI: 10.1016/j.pmedr.2018.10.008.
2. Holman H.R. The Relation of the Chronic Disease Epidemic to the Health Care Crisis // ACR Open Rheumatol. 2020. Vol. 2, No. 3. P. 167–173. DOI: 10.1002/acr2.11114.
3. Чистякова В.Р. Ангина и хронический тонзиллит (аналитический обзор) // Вестник оториноларингологии. 2012. № 1. С. 68–76.
4. Harabuchi Y. Tonsil-Induced Autoimmune/Inflammatory Syndrome: Current Insights into the Pathogenic Role of Tonsils in Immunoglobulin A Nephropathy, Palmoplantar Pustulosis and Psoriasis // Auris Nasus Larynx. 2025. Vol. 52, No. 4. P. 463–470. DOI: 10.1016/j.anl.2025.06.004.
5. Пальчун В.Т., Крюков А.И., Гуров А.В., Ермолаев А.Г. Небные миндалины: физиология и патология // Вестник оториноларингологии. 2019. Т. 84, № 6. С. 11–16. DOI: 10.17116/otorino20198406111.
6. Abulikemu N., Liu Z., Liu Y. Novel Findings on the Development and Immunological Functions of Palatine Tonsils // Clin. Rev. Allergy Immunol. 2025. Vol. 68, No. 1. Art. 58. DOI: 10.1007/s12016-025-09071-0.
7. Белов В.А. Континуум хронического тонзиллита с общепатологических позиций // Учёные записки Первого Санкт-Петербургского государственного медицинского университета имени академика И.П. Павлова. 2024. Т. 31, № 3. С. 11–18. DOI: 10.24884/1607-4181-2024-31-3-11-18.
8. Flores M., Glusman G., Brogaard K., Price N. D., Hood L. P4 Medicine: How Systems Medicine Will Transform the Healthcare Sector and Society // Per. Med. 2013. Vol. 10, No. 6. P. 565–576. DOI: 10.2217/PME.13.57.
9. Кобринский Б.А. Континуум переходных состояний организма и мониторинг динамики здоровья детей. М.–Берлин: DIRECT-MEDIA, 2016. 220 с.
10. Kobrinskii B.A., Grigoriev O.G., Molodchenkov A.I., Smirnov I.V., Blagosklonov N.A. Artificial Intelligence Technologies Application for Personal Health Management // IFAC-PapersOnLine. 2019. Vol. 52, No. 25. P. 70–74. DOI: 10.1016/j.ifacol.2019.12.448.
11. Кобринский Б.А. Системы искусственного интеллекта в медицинской практике: состояние и перспективы // Вестник Росздравнадзора. 2020. № 3. С. 37–43. DOI: 10.35576/2070-7940-2020-3-37-43.
12. Krishnan G., Singh S., Pathania M., Gosavi S., Abhishek S., Parchani A., Dhar M. Artificial Intelligence in Clinical Medicine: Catalyzing a Sustainable Global Healthcare Paradigm // Front. Artif. Intell. 2023. Vol. 6. Art. 1227091. DOI: 10.3389/frai.2023.1227091.
13. Глобальные факторы риска для здоровья: смертность и бремя болезней, обусловленные некоторыми основными факторами риска [Электронный ресурс]. М.: ВОЗ, 2015. 62 с. URL: https://rumedo.ru/uploads/materials/47bf42d1b28f923b4a3ca2e1b6c7ad65.pdf

14. Assailly J.P. Le risque, au bénéfice du danger // Soins: la revue de reference infirmiere. 2019. Vol. 64, No. 832. P. 16–19. DOI: 10.1016/j.soin.2018.12.003.
15. Кобринский Б.А. Интеллектуальные рекомендательные системы для медицины: особенности и ограничения // Искусственный интеллект и принятие решений. 2022. № 3. С. 51–62. DOI: 10.14357/20718594220304.
16. Cai Y., Yu F., Kumar M., Gladney R., Mostafa J. Health Recommender Systems Development, Usage, and Evaluation from 2010 to 2022: A Scoping Review // Int. J. Environ. Res. Public Health. 2022. Vol. 19, No. 22. Art. 15115. DOI: 10.3390/ijerph192215115.
17. Гаврилова Т.А., Кудрявцев Д.В., Муромцев Д.И. Инженерия знаний. Модели и методы: учебник для вузов. СПб.: Лань, 2023. 324 с.
18. Белов В.А., Воропаева Я.В., Кобринский Б.А. Значимость этнических особенностей коренных народов Севера в формировании хронического тонзиллита у детей // Экология человека. 2013. № 2. С. 50–57.
19. Крюков А.И., Товмасян А.С., Кишиневский А.Е., Данилюк Л.И., Мосин В.В., Шведов Н.В., Филина Е.В., Осипян А.А. Клинико-морфологическая картина хронического тонзиллита и его патогенетическая связь с пародонтопатиями: обзор литературы // Вестник оториноларингологии. 2022. Т. 87, № 5. С. 75–80. DOI: 10.17116/otorino20228705175.
20. Cinamon U., Goldfarb A., Marom T. The Impact of Tobacco Smoking Upon Chronic/Recurrent Tonsillitis and Post Tonsillectomy Bleeding // Int. Arch. Otorhinolaryngol. 2017. Vol. 21, No. 2. P. 165–170. DOI: 10.1055/s-0036-1593835.
21. Косяков С.Я., Лоранская И.Д., Анготоева И.Б., Мулдашева А.А. Ларингофарингеальный рефлюкс: вчера, сегодня, завтра // Медицинский совет. 2016. № 6. С. 78–80.
22. Li'e C., Juan C., Dongying J., Guiling F., Tihua Z., Yanfei W. The Role of Environmental Tobacco Exposure and Helicobacter Pylori Infection in the Risk of Chronic Tonsillitis in Children // Sao Paulo Med. J. 2017. Vol. 135, No. 1. P. 29–33. DOI: 10.1590/1516-3180.2016.023602102016.
23. Kvestad E., Kvaerner K.J., Røysamb E., Tambs K., Harris J.R., Magnus P. Heritability of Recurrent Tonsillitis // Arch. Otolaryngol. Head Neck Surg. 2005. Vol. 131, No. 5. P. 383–387. DOI: 10.1001/archotol.131.5.383.
24. Bani-Ata M., Aleshawi A., Alali M., Kanaan Y., Al-Momani W., Kanaan N., Abdalla K., Alhowary A. Familial and Environmental Risk Predisposition in Tonsillectomy: A Case-Control Study // Risk Management and Healthcare Policy. 2020. Vol. 13. P. 847–853. DOI: 10.2147/RMHP.S258748.
25. Glette-Iversen I., Aven T., Flage R. The Concept of Plausibility in a Risk Analysis Context: Review and Clarifications of Defining Ideas and Interpretations // Safety Science. 2022. Vol. 147. Art. 105635. DOI: 10.1016/j.ssci.2021.105635.
26. Григорьев О.Г., Кобринский Б.А., Благосклонов Н.А., Гинзбург Б.Г. Рекомендательная интеллектуальная система для управления рисками хронических заболеваний // Информационные технологии и вычислительные системы. 2023. № 2. С. 27–37. DOI: 10.14357/20718632230203.
27. Flage R., Aven T., Zio E., Baraldi P. Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment // Risk Anal. 2014. Vol. 34, No. 7. P. 1196–1207. DOI: 10.1111/risa.12247.
28. Toth-Laufer E., Batyrshin I.Z. Similarity-based personalized risk calculation // 2022 IEEE 16th International Symposium on Applied Computational Intelligence and Informatics (SACI 2022, Timisoara, Romania, 25–28 May 2022). IEEE, 2022. P. 129–134. DOI: 10.1109/SACI55618.2022.9919457.
29. Дорофеева С.В., Кокорева Я.А. Лингвистически сбалансированный инструментарий для оценки навыков чтения у взрослых носителей русского языка // Вопросы образования / Educational Studies Moscow. 2025. № 2. С. 32–72. DOI: 10.17323/vo-2025-21026.
30. Портенко Г.М., Шматов Г.П. Хронический тонзиллофарингит и информационная технология его диагностики // Российская оториноларингология. 2017. № 6. С. 100–106. DOI: 10.18692/1810-4800-2017-6-100-106.

Expert Approach to Forming the Signal Space of Chronic Tonsillitis Risk Factors in Children

Vladimir Alekseevich Belov — Candidate of Medical Sciences, Head of the Department of Otorhinolaryngology at the Veltischev Research and Clinical Institute for Pediatrics and Pediatric Surgery, Pirogov Russian National Research Medical University of the Ministry of Health of the Russian Federation, Russian Medical Academy of Continuous Professional Education of the Ministry of Health of the Russian Federation.
E-mail: belov_v_a@mail.ru

Boris Arkadyevich Kobrinsky — Academician of the Russian Academy of Natural Sciences, Professor, Doctor of Medical Sciences, Head of the Department of Intelligent Decision Support Systems, Honored Scientist of the Russian Federation, Federal Research Center "Informatics and Management" of the Russian Academy of Sciences, Pirogov Russian National Research Medical University of the Ministry of Health of the Russian Federation.
E-mail: kba_05@mail.ru

Anna Anatolyevna Akimova — Specialist of the Department of Intelligent Decision Support Systems, Federal Research Center "Informatics and Management" of the Russian Academy of Sciences.
E-mail: anna.djerg@mail.ru

Artificial intelligence systems in medicine allow for the effective solution of various problems, in particular those related to the identification of factors threatening the development of diseases. Prevention and early diagnosis of chronic tonsillitis remains one of the leading problems of otorhinolaryngology. Inflammation of the tonsils, including chronic tonsillitis, can lead to various complications, including systemic diseases. This determines the importance of preventive measures that take into account the presence of threatening factors at the pre-nosological stage. In the article discusses the problem of expert assessment of controlled risk factors for the development of chronic tonsillitis, their objective characteristics, taking into account possible uncertainty. Due to this purpose, a representation of factors with their characteristics, accompanied by corresponding numerical values, is introduced. Each characteristic is accompanied by an expert assessment of the risk level, which is an original solution for artificial intelligence systems. On this basis, a questionnaire with alternative answers has been constructed, including current risk factors for the development of chronic tonsillitis. Structured indicators — disease predictors — form a knowledge field of risk factors for chronic tonsillitis, which will serve as the knowledge base for an intelligent recommendation system.

Keywords: expert knowledge, feature space, knowledge structuring, risk factors, risk assessment, chronic tonsillitis

REFERENCES

1. Hajat C., Stein E. The Global Burden of Multiple Chronic Conditions: A Narrative Review // Prev. Med. Rep. 2018. Vol. 12. P. 1–14. DOI: 10.1016/j.pmedr.2018.10.008.
2. Holman H.R. The Relation of the Chronic Disease Epidemic to the Health Care Crisis // ACR Open Rheumatol. 2020. Vol. 2, No. 3. P. 167–173. DOI: 10.1002/acr2.11114.
3. Chistyakova V.R. Angina i khronicheskiy tonzillit (analiticheskiy obzor) // Vestnik otorinolaringologii. 2012. № 1. S. 68–76 (in Russian).
4. Harabuchi Y. Tonsil-Induced Autoimmune/Inflammatory Syndrome: Current Insights into the Pathogenic Role of Tonsils in Immunoglobulin A Nephropathy, Palmoplantar Pustulosis and Psoriasis // Auris Nasus Larynx. 2025. Vol. 52, No. 4. P. 463–470. DOI: 10.1016/j.anl.2025.06.004.

5. Palchun V.T., Kryukov A.I., Gurov A.V., Ermolaev A.G. Nebnye mindaliny: fiziologiya i patologiya // Vestnik otorinolaringologii. 2019. T. 84, № 6. S. 11–16. DOI: 10.17116/otorino20198406111 (in Russian).
6. Abulikemu N., Liu Z., Liu Y. Novel Findings on the Development and Immunological Functions of Palatine Tonsils // Clin. Rev. Allergy Immunol. 2025. Vol. 68, No. 1. Art. 58. DOI: 10.1007/s12016-025-09071-0.
7. Belov V.A. Kontinuum khronicheskogo tonzillita s obshchepatologicheskikh pozitsiy // Uchenye zapiski Pervogo Sankt-Peterburgskogo gosudarstvennogo meditsinskogo universiteta imeni akademika I.P. Pavlova. 2024. T. 31, № 3. S. 11–18. DOI: 10.24884/1607-4181-2024-31-3-11-18 (in Russian).
8. Flores M., Glusman G., Brogaard K., Price N.D., Hood L. P4 Medicine: How Systems Medicine Will Transform the Healthcare Sector and Society // Per. Med. 2013. Vol. 10, No. 6. P. 565–576. DOI: 10.2217/PME.13.57.
9. Kobrinskiy B.A. Kontinuum perekhodnykh sostoyaniy organizma i monitoring dinamiki zdorovya detey. M.–Berlin: DIRECT-MEDIA, 2016. 220 s. (in Russian).
10. Kobrinskii B.A., Grigoriev O.G., Molodchenkov A.I., Smirnov I.V., Blagosklonov N.A. Artificial Intelligence Technologies Application for Personal Health Management // IFAC-PapersOnLine. 2019. Vol. 52, No. 25. P. 70–74. DOI: 10.1016/j.ifacol.2019.12.448.
11. Kobrinskiy B.A. Sistemy iskusstvennogo intellekta v meditsinskoy praktike: sostoyanie i perspektivy // Vestnik Roszdravnadzora. 2020. № 3. S. 37–43. DOI: 10.35576/2070-7940-2020-3-37-43 (in Russian).
12. Krishnan G., Singh S., Pathania M., Gosavi S., Abhishek S., Parchani A., Dhar M. Artificial Intelligence in Clinical Medicine: Catalyzing a Sustainable Global Healthcare Paradigm // Front. Artif. Intell. 2023. Vol. 6. Art. 1227091. DOI: 10.3389/frai.2023.1227091.
13. Globalnye faktory riska dlya zdorovya: smertnost i bremya bolezney, obuslovlennye nekotorymi osnovnymi faktorami riska [Electronic resource]. M.: VOZ, 2015. 62 s. URL: https://rumedo.ru/uploads/materials/47bf42d1b28f923b4a3ca2e1b6c7ad65.pdf (in Russian).
14. Assailly J.P. Le risque, au bénéfice du danger // Soins: la revue de reference infirmiere. 2019. Vol. 64, No. 832. P. 16–19. DOI: 10.1016/j.soin.2018.12.003.
15. Kobrinskiy B.A. Intellektualnye rekomendatelnye sistemy dlya meditsiny: osobennosti i ogranicheniya // Iskusstvennyy intellekt i prinyatie resheniy. 2022. № 3. S. 51–62. DOI: 10.14357/20718594220304 (in Russian).
16. Cai Y., Yu F., Kumar M., Gladney R., Mostafa J. Health Recommender Systems Development, Usage, and Evaluation from 2010 to 2022: A Scoping Review // Int. J. Environ. Res. Public Health. 2022. Vol. 19, No. 22. Art. 15115. DOI: 10.3390/ijerph192215115.
17. Gavrilova T.A., Kudryavtsev D.V., Muromtsev D.I. Inzheneriya znaniy. Modeli i metody: uchebnik dlya vuzov. SPb.: Lan, 2023. 324 s. (in Russian).
18. Belov V.A., Voropaeva Ya.V., Kobrinskiy B.A. Znachimost etnicheskikh osobennostey korennykh narodov Severa v formirovanii khronicheskogo tonzillita u detey // Ekologiya cheloveka. 2013. № 2. S. 50–57 (in Russian).
19. Kryukov A.I., Tovmasyan A.S., Kishinevskiy A.E., Danilyuk L.I., Mosin V.V., Shvedov N.V., Filina E.V., Osipyan A.A. Kliniko-morfologicheskaya kartina khronicheskogo tonzillita i ego patogeneticheskaya svyaz s parodontopatiyami: obzor literatury // Vestnik otorinolaringologii. 2022. T. 87, № 5. S. 75–80. DOI: 10.17116/otorino20228705175 (in Russian).
20. Cinamon U., Goldfarb A., Marom T. The Impact of Tobacco Smoking Upon Chronic/Recurrent Tonsillitis and Post Tonsillectomy Bleeding // Int. Arch. Otorhinolaryngol. 2017. Vol. 21, No. 2. P. 165–170. DOI: 10.1055/s-0036-1593835.
21. Kosyakov S.Ya., Loranskaya I.D., Angotoeva I.B., Muldasheva A.A. Laringofaringealnyy reflyuks: vchera, segodnya, zavtra // Meditsinskiy sovet. 2016. № 6. S. 78–80 (in Russian).
22. Li'e C., Juan C., Dongying J., Guiling F., Tihua Z., Yanfei W. The Role of Environmental Tobacco Exposure and Helicobacter Pylori Infection in the Risk of Chronic Tonsillitis in Children // Sao Paulo Med. J. 2017. Vol. 135, No. 1. P. 29–33. DOI: 10.1590/1516-3180.2016.023602102016.
23. Kvestad E., Kvaerner K.J., Røysamb E., Tambs K., Harris J.R., Magnus P. Heritability of Recurrent Tonsillitis // Arch. Otolaryngol. Head Neck Surg. 2005. Vol. 131, No. 5. P. 383–387. DOI: 10.1001/archotol.131.5.383.

24. Bani-Ata M., Aleshawi A., Alali M., Kanaan Y., Al-Momani W., Kanaan N., Abdalla K., Alhowary A. Familial and Environmental Risk Predisposition in Tonsillectomy: A Case-Control Study // Risk Management and Healthcare Policy. 2020. Vol. 13. P. 847–853. DOI: 10.2147/RMHP.S258748.
25. Glette-Iversen I., Aven T., Flage R. The Concept of Plausibility in a Risk Analysis Context: Review and Clarifications of Defining Ideas and Interpretations // Safety Science. 2022. Vol. 147. Art. 105635. DOI: 10.1016/j.ssci.2021.105635.
26. Grigoryev O.G., Kobrinskiy B.A., Blagosklonov N.A., Ginzburg B.G. Rekomendatelnaya intellektualnaya sistema dlya upravleniya riskami khronicheskikh zabolevaniy // Informatsionnye tekhnologii i vychislitelnye sistemy. 2023. № 2. S. 27–37. DOI: 10.14357/20718632230203 (in Russian).
27. Flage R., Aven T., Zio E., Baraldi P. Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment // Risk Anal. 2014. Vol. 34, No. 7. P. 1196–1207. DOI: 10.1111/risa.12247.
28. Toth-Laufer E., Batyrshin I.Z. Similarity-based personalized risk calculation // 2022 IEEE 16th International Symposium on Applied Computational Intelligence and Informatics (SACI 2022, Timisoara, Romania, 25–28 May 2022). IEEE, 2022. P. 129–134. DOI: 10.1109/SACI55618.2022.9919457.
29. Dorofeeva S.V., Kokoreva Ya.A. Lingvisticheski sbalansirovannyy instrumentariy dlya otsenki navykov chteniya u vzroslykh nositeley russkogo yazyka // Voprosy obrazovaniya / Educational Studies Moscow. 2025. № 2. S. 32–72. DOI: 10.17323/vo-2025-21026 (in Russian).
30. Portenko G.M., Shmatov G.P. Khronicheskiy tonzillofaringit i informatsionnaya tekhnologiya ego diagnostiki // Rossiyskaya otorinolaringologiya. 2017. № 6. S. 100–106. DOI: 10.18692/1810-4800-2017-6-100-106 (in Russian).

Tables

Table 1

A fragment of a structured presentation of knowledge about the risk factors of chronic tonsillitis

Risk factor (attribute)	Attribute characteristics	Attribute value
Family history of disease	Presence of chronic tonsillitis in the family	First-degree relatives
	Presence of tonsillectomies in the family	First-degree relatives
	Indigenous peoples of the North	Mother
		Father
Geography of residence	Residence in the subpolar and polar regions (non-indigenous population)	> 5 years
	Residence in the subpolar and polar regions (non-indigenous population)	< 5 years
	Finger-sucking	Present
Caries	Detection of caries, including treated caries (including filled teeth)	≥ 1 time per year
		≤ 1 time per 2 years
		≤ 1 time per 3 years
Respiratory diseases	With symptoms of tonsillitis, sore throat	≥ 4 times this year
		2-3 times this year
		1 time this year
		≥ 1 year ago

Table 2

A fragment of a structured presentation of the risk factors of chronic tonsillitis with expert assessments

Risk factor (attribute)	Attribute characteristics	Attribute value	Risk level
Family history of allergies	Presence of chronic tonsillitis in the family	First-degree relatives	High
	Presence of tonsillectomies in the family	First-degree relatives	Very high
Ethnic characteristics	Indigenous peoples of the North	Mother	High
	Indigenous peoples of the North	Father	Medium
Rhinitis	Recurrent	Currently	High
		In the past	Medium

Индекс УДК 004.8:004.056.5
Код ГРНТИ 28.23.25
DOI: 10.22204/2410-4639-2026-129-01-76-87

О.А. БУБНОВ*

Обеспечение информационной безопасности систем искусственного интеллекта в финансовом секторе

В статье исследуется влияние уязвимостей систем искусственного интеллекта (ИИ) на обеспечение цифрового суверенитета Российской Федерации при их эксплуатации в объектах критической информационной инфраструктуры и финансовом секторе. Показано, что неконтролируемое использование зарубежных ИИ-библиотек, отсутствие стандартизированных процедур валидации моделей и недостаточная проработка вопросов безопасности на этапах жизненного цикла ИИ создают прямые угрозы технологической независимости и национальной безопасности.

Систематизированы уязвимости на этапах обучения, вывода, инфраструктурного обеспечения и процессного управления. Предложен подход к уточнению оценки рисков, адаптирующий существующие методики с учётом динамической природы ИИ-систем, каскадных эффектов межсистемного взаимодействия и включающий сценарный анализ методом Монте-Карло. Предлагаемые меры минимизации рисков интегрированы с положениями NIST AI RMF, ГОСТ Р 59276-2020 и требованиями ФСТЭК России по моделированию угроз для ИИ-систем. Обосновано, что внедрение предложенного подхода является необходимым условием укрепления цифрового суверенитета России в условиях санкционного давления и нарастающего геополитического противостояния в киберпространстве.

Ключевые слова: искусственный интеллект, цифровой суверенитет, уязвимости ИИ, адверсарные атаки, отравление данных, каскадные эффекты, оценка рисков, финансовый сектор, технологическая независимость

Введение

Интеграция систем искусственного интеллекта в стратегически важные отрасли экономики и государственного управления приобрела в последние годы масштабный характер. Критическая информационная инфраструктура (КИИ) — энергетика, транспорт, связь, а также финансовый сектор, где ИИ-решения применяются для обнаружения мошеннических операций, алгоритмической торговли, кредитного скоринга и управления рисками, — формирует основу современного технологического ландшафта России.

* **Бубнов Олег Алексеевич** — техник управления цифрового развития; студент Донского государственного технического университета.
E-mail: olegbub07@gmail.com

Однако стремительное внедрение ИИ опережает развитие адекватных механизмов обеспечения их безопасности, надёжности и устойчивости функционирования [10, с. 198].

Цифровой суверенитет, понимаемый как способность государства самостоятельно определять стратегию развития цифровой среды, обеспечивать защиту национальных интересов в киберпространстве и контролировать критически значимые технологии, напрямую зависит от возможности гарантировать безопасное функционирование применяемых ИИ-систем [4, с. 123].

В современных исследованиях справедливо отмечается, что цифровой суверенитет является формой проявления технологического суверенитета и предполагает не только наличие собственных аппаратных решений, но и контроль над алгоритмами, данными и процессами их обработки [4, с. 125].

Особую остроту проблеме придаёт тот факт, что значительная часть используемых в России ИИ-решений базируется на зарубежных библиотеках, открытых датасетах и облачных сервисах, что создаёт потенциальные каналы утечки данных, внедрения «закладок» и недекларированных возможностей. В условиях санкционного давления и необходимости обеспечения технологической независимости контроль над ИИ-системами в КИИ становится приоритетной задачей государства [8].

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) в декабре 2025 года впервые официально включила угрозы, связанные с использованием искусственного интеллекта, в банк данных угроз безопасности информации. В обновлённом перечне описаны сценарии атак на всех этапах жизненного цикла ИИ-систем — от разработки и обучения до практической эксплуатации, включая генеративные модели и ИИ-агентов [1, 9]. Это знаковое событие фиксирует переход вопросов безопасности ИИ из теоретической плоскости в практическую область регулирования и требует разработки соответствующих методик оценки и управления рисками.

Цель настоящего исследования — адаптация существующих подходов к оценке и управлению рисками эксплуатации уязвимостей ИИ для критической инфраструктуры и финансового сектора России с учётом задач обеспечения цифрового суверенитета. Предлагаемый подход интегрирует стохастические модели, сценарный анализ и междисциплинарные практики, обеспечивая устойчивость систем и минимизацию каскадных эффектов.

Научная новизна работы заключается в адаптации классических подходов риск-менеджмента к уникальным характеристикам ИИ-систем (динамическая эволюция моделей, зависимость от качества данных, алгоритмическая непрозрачность); разработке модифицированной формулы оценки риска, учитывающей последовательность событий «угроза → уязвимость → успешная атака»; интеграции сценарного моделирования методом Монте-Карло для прогнозирования каскадных эффектов в финансовом секторе и КИИ; обосновании связи между уязвимостями ИИ-систем и угрозами цифровому суверенитету России.

Практическая значимость исследования состоит в создании универсального фреймворка для прогнозирования, анализа и нейтрализации киберрисков ИИ, что способствует повышению надёжности критически важных систем и формированию научной базы для разработки национальных стандартов устойчивости ИИ [7].

1. Теоретические основы исследования уязвимостей систем искусственного интеллекта

1.1. Систематизация уязвимостей ИИ в контексте обеспечения цифрового суверенитета

Внедрение систем искусственного интеллекта в объекты критической информационной инфраструктуры требует особого внимания к вопросам обеспечения их безопасности, надёжности и устойчивости функционирования, поскольку техноло-

гии ИИ могут как повысить эффективность и автоматизацию процессов, так и одновременно создать новые риски и уязвимости [10, с. 201]. Анализ современных исследований позволяет выделить четыре основные категории уязвимостей ИИ-систем, каждая из которых создаёт специфические угрозы цифровому суверенитету.

Уязвимости на этапе обучения включают риски, возникающие в процессе формирования и подготовки данных для обучения моделей машинного обучения, и представляют наибольшую опасность с точки зрения долгосрочных последствий для национальной безопасности.

Прежде всего, это отравление данных (data poisoning) — целенаправленное искажение обучающих выборок с целью деградации предсказательной способности модели или внедрения преднамеренных аномалий, которые могут активироваться в критический момент управления энергосетью или транспортной системой [3, с. 64]. Как отмечает Гарбук С.В., качество данных является фундаментальным фактором, определяющим функциональность и безопасность систем искусственного интеллекта [2]. Для России, где значительная часть открытых датасетов имеет зарубежное происхождение, риск отравления данных приобретает характер прямой угрозы цифровому суверенитету.

К этой же категории относятся систематические смещения (bias), формирующиеся из-за репрезентативных искажений в обучающих данных и приводящие к некорректным закономерностям, снижающим объективность и этичность ИИ-решений.

В финансовом секторе такие смещения могут проявляться в дискриминации определённых категорий заёмщиков, а в системах видеонаблюдения — в расовых или гендерных искажениях при идентификации личности. Компрометация источников данных, предполагающая вмешательство в каналы получения данных (например, открытые датасеты, API сторонних сервисов), позволяет внедрять вредоносные метки или манипулировать обучающим процессом. Использование зарубежных облачных хранилищ и датасетов создаёт риски внедрения «закладок» на этапе формирования модели.

Уязвимости на этапе вывода (inference) охватывают риски, реализуемые в процессе эксплуатации уже обученной модели, и представляют непосредственную угрозу операционной деятельности объектов КИИ. Наибольшую известность получили адверсарные атаки, основанные на генерации входных данных, минимально отличающихся от легитимных, но вызывающих ошибочные прогнозы модели за счёт эксплуатации её чувствительности к определённым признакам.

В контексте систем компьютерного зрения, используемых на транспорте или в системах безопасности, такие атаки могут привести к фатальным последствиям. Например, нанесение специальных наклеек на дорожные знаки может сделать их невидимыми для автопилота [3, с. 66].

Инверсия модели позволяет реконструировать конфиденциальные данные из обучающей выборки путём анализа выходных предсказаний модели, что в финансовом секторе создаёт риск восстановления персональных данных клиентов, платёжной информации и коммерческой тайны. Атаки на принадлежность (membership inference) определяют присутствие конкретных данных в обучающем наборе, что представляет особый риск для медицинских и финансовых приложений, где конфиденциальность информации защищена законодательством.

Уязвимости инфраструктуры и цепочки поставок связаны с технологической зависимостью России от зарубежных компонентов и платформ, что непосредственно подрывает цифровой суверенитет. Компрометация MLOps-платформ позволяет внедрять вредоносные артефакты в конвейеры непрерывной интеграции и доставки (CI/CD), угрожая целостности моделей на всех этапах их жизненного цикла. Использование непроверенных open-source решений, содержащих потенциальные бэкдоры или эксплойты (уязвимые библиотеки), по оцен-

Таблица 1

Сравнительная классификация уязвимостей ИИ-систем в контексте угроз цифровому суверенитету

Категория	Примеры уязвимостей	Возможные последствия для цифрового суверенитета
Обучение	Отравление данных, систематические смещения, компрометация источников	Некорректные прогнозы в системах госуправления, дискриминационные решения, внедрение «закладок» иностранными разработчиками
Вывод	Адверсарные атаки, инверсия модели, атаки на принадлежность	Утечка конфиденциальных данных, нарушение работы критических систем, подрыв доверия к отечественным ИИ-решениям
Инфраструктура	Уязвимые библиотеки, компрометация MLOps, нарушение целостности	Зависимость от зарубежных компонентов, невозможность гарантировать отсутствие недекларированных возможностей
Процессы и управление	Отсутствие валидации, недостаточный аудит, человеческий фактор	Ошибки стратегических решений, репутационные потери, снижение эффективности импортозамещения

кам экспертов, охватывает до 70% используемых в России ИИ-библиотек, имеющих зарубежное происхождение и не проходящих необходимую сертификацию.

Нарушение целостности модели при хранении или передаче может быть осуществлено как внешними злоумышленниками, так и недобросовестными поставщиками решений.

Операционные и процессные уязвимости отражают недостатки в организации процессов эксплуатации ИИ-систем и человеческий фактор. Некритическое доверие операторов к предсказаниям ИИ, игнорирующее необходимость валидации результатов (особенно в нештатных ситуациях), отсутствие регулярного мониторинга моделей на предмет дрейфа данных и корректности функционирования, а также недостаточная формализация политик эксплуатации ИИ — всё это повышает вероятность ошибочных решений и затрудняет расследование инцидентов.

Сравнительная классификация уязвимостей ИИ-систем с указанием возможных последствий для цифрового суверенитета представлена в таблице 1.

1.2. Российские и международные подходы к стандартизации безопасности ИИ

Вопросы стандартизации в области безопасности искусственного интеллекта активно разрабатываются как на международном, так и на национальном уровне. Для России синхронизация этих подходов с учётом задач обеспечения цифрового суверенитета имеет стратегическое значение.

Наиболее разработанным международным фреймворком является NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0), опубликованный в 2023 году [11]. Документ предлагает системный подход к управлению рисками ИИ, включающий характеристики доверенных ИИ-систем (валидность, надёжность, безопасность, устойчивость, подотчётность, прозрачность, справедливость) и четыре ключевые функции: управление (govern), картирование (map), измерение (measure) и управление (manage). В 2024 году вышло обновление NIST Cybersecurity Framework (CSF 2.0), учитывающее специфику ИИ-систем [12].

В России разработка нормативной базы в области безопасности ИИ ведётся по нескольким направлениям. Ключевым документом является ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения», который устанавливает общие подходы к оценке доверия к ИИ-системам [1]. В стадии разработки находится проект ГОСТ Р «Искусственный интеллект в критической информационной инфраструктуре. Общие

положения», который должен определить специальные требования к ИИ-системам, применяемым на объектах КИИ [10, с. 202].

Значимым событием 2025 года стала разработка первой российской модели угроз кибербезопасности искусственного интеллекта на всех этапах жизненного цикла — от сбора данных до эксплуатации. Документ содержит перечень из 70 различных угроз, разбитых на 5 групп (данные, инфраструктура, модель, приложения, AI-агенты), и по сути представляет собой первый отечественный фреймворк, аналогичный DASF, NIST AI RMF и OWASP [7].

Особого внимания заслуживает включение в декабре 2025 года ФСТЭК России угроз, связанных с использованием искусственного интеллекта, в банк данных угроз безопасности информации. В перечень вошли уязвимости, характерные для ИИ-технологий: модели машинного обучения, обучающие датасеты, RAG-подходы и механизмы адаптации больших языковых моделей. Это означает обязательный учёт данных угроз при моделировании угроз для государственных информационных систем и объектов критической инфраструктуры [1, 9].

Совместное исследование Ассоциации ФинТех (АФТ) и Positive Technologies «Тренды кибербезопасности финансовой отрасли в 2026 году» показывает, что порядка 25% финтех-организаций уже сталкивались с инцидентами, связанными с применением ИИ. При этом особую проблему представляет «теневой ИИ» (Shadow AI) — массовое использование сотрудниками внешних ИИ-сервисов без согласования с ИТ-отделами, что приводит к утечкам чувствительных данных.

2. Совершенствование подходов к оценке рисков эксплуатации уязвимостей ИИ для критической инфраструктуры и финансового сектора

2.1. Базовые принципы и адаптация классических подходов

Предлагаемый подход базируется на комбинации вероятностных и стоимостных показателей. Уровень риска предлагается определять как произведение двух факторов: вероятности эксплуатации уязвимости и величины возможного ущерба. Для учёта многостадийности современных кибератак вероятность эксплуатации уязвимости целесообразно декомпозировать на последовательные этапы: наличие мотивации и возможностей у злоумышленника, наличие уязвимости, пригодной для эксплуатации, и успешность её использования.

Данный подход позволяет распределить ответственность за различные этапы противодействия между специалистами разного профиля [7]. Величина воздействия (ущерба) определяется как взвешенная комбинация метрик, отражающих различные аспекты ущерба для национальной безопасности и экономической стабильности: финансовые потери (прямые и косвенные), операционные последствия (сбои в работе, простой, деградация качества), репутационный ущерб и утрата доверия, регуляторные последствия (штрафы, ограничения деятельности), а также ущерб цифровому суверенитету (потеря контроля над критическими технологиями, зависимость от иностранных решений).

Весовые коэффициенты определяются исходя из приоритетов конкретного сектора (критическая информационная инфраструктура или финансовый сектор). Учёт ущерба цифровому суверенитету позволяет количественно оценивать влияние инцидентов на технологическую независимость и национальную безопасность.

2.2. Критерии оценки воздействия для критической инфраструктуры

Для объектов критической информационной инфраструктуры приоритетное значение имеют следующие критерии оценки воздействия: угрозы безопасности населения (риски, реализация которых может привести к гибели людей, нарушению жизнеобеспечения, техногенным катастрофам — например, сбои в управлении энергосетями способны спровоцировать массовые отключения электроэнергии и каскадные аварии [4, с. 128]); операционные сбои системо-

образующего характера (остановка транспортных систем, нарушение связи, сбои в работе систем водоснабжения и теплоснабжения); риски национальной безопасности (компрометация промышленных ИИ, используемых в оборонно-промышленном комплексе, утечка данных о критических технологиях, внедрение «закладок» в системы управления); экологические последствия (аварии на опасных производственных объектах, неконтролируемые выбросы вредных веществ).

Исследование динамики киберугроз в России свидетельствует об увеличении числа кибератак на объекты КИИ. Согласно данным аналитического центра RED Security SOC, общее число киберинцидентов в России достигло 130 тысяч в 2024 году, что превышает показатели предыдущего периода в 2,5 раза. Объекты КИИ стали объектами более 208 тысяч особо опасных атак [4, с. 128].

2.3. Критерии оценки воздействия для финансового сектора

Финансовый сектор России в 2026 году отвечает на рост каскадных и экосистемных кибератак переходом к модели киберустойчивости — способности сохранять и быстро восстанавливать критически важные процессы даже при реализованных киберугрозах [5].

Приоритетные критерии оценки воздействия включают финансовые убытки от некорректных решений ИИ-систем или успешных атак, включая прямые потери, затраты на восстановление и упущенную выгоду; системные рыночные риски — неконтролируемое поведение торговых алгоритмов, способное вызвать резкие колебания рынка, панику среди инвесторов и дестабилизацию финансовой системы; репутационный ущерб и утрата доверия клиентов и контрагентов, что в долгосрочной перспективе может привести к оттоку капитала и снижению конкурентоспособности; нарушение конфиденциальности данных клиентов, включая платёжную информацию, персональные данные, коммерческую тайну; регуляторные последствия — штрафы, ограничения деятельности, приостановка лицензий, усиление надзорных требований.

Современный ландшафт киберугроз в финансовом секторе характеризуется значительным ростом числа каскадных комбинированных атак на экосистемы организаций. Злоумышленники всё чаще атакуют не головные офисы банков, а их менее защищённых партнёров — ИТ-подрядчиков и дочерние организации. Поэтому компании переходят к централизованной модели информационной безопасности с едиными стандартами для всех участников экосистемы [5].

2.4. Сценарное моделирование методом Монте-Карло

Для учёта неопределённости и стохастической природы многих факторов, влияющих на реализацию рисков, предлагается использование метода Монте-Карло для сценарного моделирования.

Данный подход позволяет моделировать распределение вероятностей различных сценариев развития событий при заданных исходных условиях, оценивать вероятность каскадных эффектов и системных сбоев, определять наиболее критичные параметры модели, требующие первоочерёдного контроля, и обосновывать выбор мер защиты на основе количественных оценок ожидаемого ущерба.

Процедура сценарного моделирования включает следующие этапы: идентификация ключевых факторов риска (параметры, неопределённость которых существенно влияет на итоговую оценку риска: частота атак определённого типа, вероятность успеха, время обнаружения, скорость распространения, эффективность контрмер); задание распределений вероятностей для каждого фактора на основе экспертных оценок или статистических данных (нормальное, логнормальное, равномерное, треугольное и т.д.); генерация методом Монте-Карло случайных сценариев (обычно 10 000 и более), каждый из которых представляет

собой конкретную комбинацию значений факторов риска; расчёт последствий для каждого сценария с учётом моделируемых каскадных эффектов; анализ результатов — построение распределений вероятностей различных уровней ущерба, определение наиболее вероятных сценариев.

Применение метода Монте-Карло особенно актуально для финансового сектора, где высокая скорость транзакций и сложность взаимосвязей между участниками рынка создают предпосылки для быстрого распространения сбоев.

2.5. Учёт каскадных эффектов и системных рисков

Ключевой особенностью предлагаемой методологии является системный учёт каскадных эффектов — явлений, при которых локальный сбой или инцидент в одном элементе системы приводит к цепочке последующих отказов, распространяющихся на смежные и зависимые компоненты.

Для количественной оценки каскадных эффектов вводится коэффициент усиления, показывающий, во сколько раз итоговый совокупный ущерб (с учётом распространения инцидента на смежные и зависимые компоненты) превышает прямые потери от первоначального инцидента. На основе анализа инцидентов последних лет можно выделить следующие типовые сценарии каскадного развития атак на ИИ-системы: технологическая каскадность — сбой в работе ИИ-системы управления энергосетью приводит к отключению электроэнергии на промышленных объектах, что вызывает остановку производства, сбои в работе транспорта, нарушение связи; финансовая каскадность — некорректное решение торгового алгоритма вызывает цепную реакцию продаж, лавинообразное падение котировок и панику на рынке; репутационная каскадность — утечка данных из одного банка подрывает доверие ко всей банковской системе, вызывая отток вкладов и проблемы с ликвидностью у других участников; регуляторная каскадность — инцидент в одной организации приводит к ужесточению требований для всего сектора, увеличению издержек на соответствие и снижению эффективности.

Исследование Ассоциации ФинТех подчёркивает, что в условиях растущего числа киберугроз участники рынка всё больше отдают предпочтение измеримой модели, при которой важно не просто наличие средств защиты, а их реальная эффективность и способность снижать ущерб. Для оценки эффективности защиты используются такие показатели, как time to attack (TTA) и time to response (TTR) [5].

3. Практическая реализация методологии и меры минимизации рисков

3.1. Интеграция с NIST AI RMF и российскими стандартами

Предлагаемая методология органично интегрируется с существующими фреймворками управления рисками ИИ, прежде всего с NIST AI RMF, и адаптирует их к российским условиям с учётом задач обеспечения цифрового суверенитета. Соответствие разработанной методологии функциям NIST AI RMF и их реализация в контексте российского регулирования показаны в таблице 2.

3.2. Байесовские методы динамического обновления вероятностей

Учитывая динамическую природу ИИ-систем и быстрое изменение ландшафта угроз, предлагается использование байесовского подхода для непрерывного уточнения вероятностных оценок по мере поступления новых данных об инцидентах и уязвимостях. Байесовское обновление позволяет пересчитывать априорные вероятности P(U) в апостериорные с учётом наблюдаемых событий:

$$P(I|E) = [P(E|U) \times P(U)]/P(E), \qquad (1)$$

где $P(U|E)$ — апостериорная вероятность эксплуатации уязвимости после наблюдения события E; $P(E|U)$ — вероятность наблюдения события E при условии, что уяз-

Таблица 2

Интеграция методологии с NIST AI RMF и российскими стандартами

Функция NIST AI RMF	Реализация в предлагаемой методологии	Учёт российских требований
Govern (Управление)	Определение политик и процедур управления рисками ИИ, распределение ответственности	Соответствие ГОСТ Р 59276-2020, учёт требований ФСТЭК по моделированию угроз
Map (Картирование)	Идентификация активов, угроз, уязвимостей, сценариев атак	Использование БДУ ФСТЭК, включая новый раздел по угрозам ИИ
Measure (Измерение)	Количественная оценка рисков с использованием P(U) и I(U), анализ чувствительности, сценарное моделирование	Применение метрик, рекомендованных регуляторами финансового сектора
Manage (Управление)	Выбор и реализация контрмер, мониторинг эффективности, инцидент-менеджмент	Внедрение российских средств защиты, сертифицированных ФСТЭК

вимость существует и может быть эксплуатирована; $P(U)$ — априорная вероятность; $P(E)$ — полная вероятность события E.

Данный подход особенно эффективен при организации непрерывного мониторинга угроз и может быть реализован в автоматизированных системах управления рисками.

3.3. Практические рекомендации по минимизации рисков

На основе проведённого анализа можно сформулировать следующие рекомендации по минимизации рисков эксплуатации уязвимостей ИИ в критической инфраструктуре и финансовом секторе.

Организационные меры включают создание центров компетенций по безопасности ИИ на отраслевом уровне, объединяющих усилия регуляторов, участников рынка и научного сообщества; разработку отраслевых стандартов безопасной разработки и эксплуатации ИИ с учётом специфики конкретных секторов; внедрение процедур обязательной сертификации ИИ-систем, предназначенных для использования на объектах КИИ и в финансовом секторе; проведение регулярных киберучений с моделированием атак на ИИ-компоненты критических систем.

Технические меры предполагают внедрение алгоритмов обнаружения аномалий для мониторинга поведения ИИ-систем в реальном времени и выявления признаков атак; использование методов состязательного обучения (adversarial training) для повышения устойчивости моделей к адверсарным атакам; применение гомоморфного шифрования и дифференциальной приватности для защиты конфиденциальных данных при обучении и эксплуатации моделей; регулярное тестирование моделей на проникновение (AI red teaming) с использованием актуальных методик моделирования угроз [7]; внедрение систем контроля целостности моделей и обнаружения несанкционированных изменений.

Меры в области импортозамещения и технологической независимости включают разработку реестра доверенных отечественных компонентов и библиотек для создания ИИ-систем, прошедших сертификацию на отсутствие недекларированных возможностей; создание национальных датасетов для обучения моделей, используемых в критических приложениях, с обеспечением контроля их целостности и чистоты; развитие собственных MLOps-платформ и инструментов разработки, не зависящих от зарубежных поставщиков; стимулирование перехода на открытые отечественные ИИ-решения в государственных корпорациях и компаниях с госучастием.

Правовые и регуляторные меры предполагают закрепление в нормативных документах требований к безопасности ИИ-систем на всех этапах жизненного цикла; введение ответственности разработчиков

и эксплуатантов за ущерб, причинённый вследствие недостаточной защищённости ИИ-систем; гармонизацию российских и международных стандартов в области безопасности ИИ с учётом необходимости защиты национальных интересов.

3.4. Перспективные направления исследований

Дальнейшее развитие предложенной методологии видится в разработке количественных метрик для оценки ущерба цифровому суверенитету C_{sov}, позволяющих сопоставлять различные виды рисков и обосновывать инвестиции в защиту; создании автоматизированных инструментов аудита моделей, включая системы обнаружения «закладок», анализа на предмет систематических смещений и оценки устойчивости к адверсарным атакам; исследовании возможностей применения когнитивных карт и нейронных сетей для моделирования сложных взаимосвязей в системах управления рисками [2]; разработке методов обеспечения доверия к результатам работы ИИ-систем, включая подходы к объяснимости принимаемых решений (XAI) и верификации корректности [3, с. 68]; исследовании специфики безопасности ИИ-агентов и мультиагентных систем, включая риски каскадных атак в распределённых архитектурах [7].

Заключение

Проведённое исследование позволяет сформулировать следующие основные выводы и положения. Уязвимости систем искусственного интеллекта, эксплуатируемых в критической информационной инфраструктуре и финансовом секторе, создают прямые угрозы цифровому суверенитету Российской Федерации. Эти угрозы обусловлены как технологическими особенностями ИИ (зависимость от качества данных, алгоритмическая непрозрачность, чувствительность к адверсарным воздействиям), так и высокой степенью зависимости от зарубежных компонентов, библиотек и платформ. Предложенная адаптация существующих подходов к оценке рисков, учитывающая взвешенную оценку воздействия с включением ущерба цифровому суверенитету, а также декомпозицию вероятности реализации угрозы на последовательные этапы, обеспечивает комплексный подход к анализу и нейтрализации рисков эксплуатации ИИ-систем. Интеграция предлагаемого подхода с положениями NIST AI RMF, ГОСТ Р 59276-2020 и требованиями ФСТЭК России по моделированию угроз для ИИ-систем позволяет создать единый фреймворк управления рисками, адаптированный к российским условиям и учитывающий необходимость защиты национальных интересов. Сценарное моделирование методом Монте-Карло и учёт каскадных эффектов являются необходимыми компонентами оценки рисков для финансового сектора, где локальные сбои способны вызывать системные последствия, затрагивающие значительное число субъектов и создающие угрозы национальной безопасности. Реализация предложенных мер минимизации рисков требует междисциплинарного сотрудничества специалистов по кибербезопасности, искусственному интеллекту, праву и риск-менеджменту, а также координации усилий государства, бизнеса и научного сообщества.

Значимость настоящего исследования для обеспечения цифрового суверенитета России заключается в создании научно обоснованного подхода к прогнозированию, анализу и нейтрализации киберрисков ИИ, что способствует повышению надёжности критически важных систем и формированию базы для разработки национальных стандартов устойчивости ИИ.

В условиях санкционного давления, нарастающего геополитического противостояния в киберпространстве и ускоренной цифровизации экономики, обеспечение безопасности ИИ-систем становится не просто технической задачей, а фактором стратегической стабильности и национальной безопасности.

Перспективы дальнейших исследований включают разработку количествен-

ных метрик для оценки ущерба цифровому суверенитету, создание автоматизированных инструментов аудита моделей, исследование специфики безопасности ИИ-агентов и мультиагентных систем, а также совершенствование методов обеспечения доверия к результатам работы ИИ-систем. Решение этих задач станет основой для безопасной и устойчивой цифровизации экономики и государственного управления, укрепления технологической независимости и защиты национальных интересов России в долгосрочной перспективе.

ЛИТЕРАТУРА

1. ГОСТ Р 59276–2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения. М.: Стандартинформ, 2021. 16 с.
2. Гарбук С.В. Функциональность и безопасность систем искусственного интеллекта: качество данных // Открытые системы. СУБД. 2024. № 1. С. 18–23. DOI: 10.51793/OS.2024.95.90.004.
3. Грушо А.А., Грушо Н.А., Забежайло М.И., Писковский В.О., Тимонина Е.Е. Логика обмана в машинном обучении // Информатика и её применения. 2024. Т. 18. № 1. С. 63–68. DOI: 10.14357/19922264240111.
4. Цифровой суверенитет и экономическая безопасность России в условиях роста современных киберугроз // Вестник экономической безопасности. 2025. № 4. С. 121–136.
5. Тренды кибербезопасности финансовой отрасли в 2026 году: совместное исследование Ассоциации ФинТех и Positive Technologies. М.: АФТ, 2026. 48 с.
6. Милославская Н.Г., Дворянкин С.В. Уязвимости систем искусственного интеллекта, применяемых в активах информационно-телекоммуникационных сетей организаций // Безопасность информационных технологий. 2026. Т. 33. № 1. С. 42–58. DOI: 10.26583/bit.2026.1.10.
7. Модель угроз кибербезопасности искусственного интеллекта (версия 1.0). Сбер, 2025. 86 с.
8. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203.
9. Банк данных угроз безопасности информации [Электронный ресурс] / ФСТЭК России. 2025. URL: https://bdu.fstec.ru/
10. Аменицкий А.В. Кибербезопасность. AI hacking. Двойное назначение искусственного интеллекта // Наука, общество, образование: актуальные вопросы, достижения и инновации: сб. статей. Пенза: Наука и Просвещение, 2025. С. 197–216.
11. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST, 2023. 42 p.
12. The NIST Cybersecurity Framework (CSF) 2.0. NIST, 2024. 27 p.
13. Lee M.J., Sinha R. Data Security, AI, and Infrastructure: Examining Cyber Risk in the Financial System [Электронный ресурс] // Teller Window. 2025. URL: https://tellerwindow.newyorkfed.org/
14. Understanding AI Data Poisoning [Электронный ресурс]. HiddenLayer, 2024. URL: https://hiddenlayer.com/
15. Securing Critical Infrastructure in the Age of AI [Электронный ресурс]. CSET, 2025. URL: https://cset.georgetown.edu/
16. Managing AI-related cyber risks [Электронный ресурс]. HM Treasury, 2025. URL: https://www.regulationtomorrow.com/
17. Boamah F. A., Jin X., Senaratne S., Perera S. AI-driven risk identification model for infrastructure projects: Utilising past project data // Expert Systems with Applications. 2025. Vol. 283 (10). Art. 127891. DOI: 10.1016/j.eswa.2025.127891.
18. Mohamed N. Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms // Knowledge and Information Systems. 2025. Vol. 67, No. 8. P. 6969–7055. DOI: 10.1007/s10115-025-02429-y.

On Ensuring Information Security of Artificial Intelligence Systems in the Financial Sector

Oleg Alekseevich Bubnov — Technician, Digital Development Department, Student, Don State Technical University.
E-mail: olegbub07@gmail.com

The article examines the impact of artificial intelligence (AI) system vulnerabilities on the digital sovereignty of the Russian Federation when deployed in critical information infrastructure and the financial sector. It is shown that uncontrolled use of foreign AI libraries, lack of standardized model validation procedures, and insufficient attention to security throughout the AI lifecycle pose direct threats to technological independence and national security. Vulnerabilities are systematized across the stages of training, inference, infrastructure, and process management. An approach to refining risk assessment is proposed, adapting existing methodologies to account for the dynamic nature of AI systems, cascading effects of inter-system interactions, and incorporating Monte Carlo scenario analysis. Proposed risk mitigation measures are integrated with the NIST AI RMF, GOST R 59276–2020, and the requirements of the FSTEC of Russia for threat modeling of AI systems. It is substantiated that implementing the proposed approach is a necessary condition for strengthening Russia's digital sovereignty under sanctions pressure and escalating geopolitical confrontation in cyberspace.

Keywords: artificial intelligence, digital sovereignty, AI vulnerabilities, adversarial attacks, data poisoning, cascading effects, risk assessment, financial sector, technological independence

REFERENCES

1. GOST R 59276–2020. Sistemy iskusstvennogo intellekta. Sposoby obespecheniya doveriya. Obshchie polozheniya. M.: Standartinform, 2021. 16 s. (in Russian).
2. Garbuk S.V. Funktsionalnost i bezopasnost sistem iskusstvennogo intellekta: kachestvo dannykh // Otkrytye sistemy. SUBD. 2024. № 1. S. 18–23. DOI: 10.51793/OS.2024.95.90.004 (in Russian).
3. Grusho A.A., Grusho N.A., Zabezhaylo M.I., Piskovskiy V.O., Timonina E.E. Logika obmana v mashinnom obuchenii // Informatika i ee primeneniya. 2024. T. 18. № 1. S. 63–68. DOI: 10.14357/19922264240111 (in Russian).
4. Tsifrovoy suverenitet i ekonomicheskaya bezopasnost Rossii v usloviyakh rosta sovremennykh kiberugroz // Vestnik ekonomicheskoy bezopasnosti. 2025. № 4. S. 121–136 (in Russian).
5. Trendy kiberbezopasnosti finansovoy otrasli v 2026 godu: sovmestnoe issledovanie Assotsiatsii FinTekh i Positive Technologies. M.: AFT, 2026. 48 s. (in Russian).
6. Miloslavskaya N.G., Dvoryankin S.V. Uyazvimosti sistem iskusstvennogo intellekta, primenyaemykh v aktivakh informatsionno-telekommunikatsionnykh setey organizatsiy // Bezopasnost informatsionnykh tekhnologiy. 2026. T. 33. № 1. S. 42–58. DOI: 10.26583/bit.2026.1.10 (in Russian).
7. Model ugroz kiberbezopasnosti iskusstvennogo intellekta (versiya 1.0). Sber, 2025. 86 s. (in Russian).
8. O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017–2030 gody: Ukaz Prezidenta RF ot 09.05.2017 № 203 (in Russian).
9. Bank dannykh ugroz bezopasnosti informatsii [Electronic resource] / FSTEK Rossii. 2025. URL: https://bdu.fstec.ru/ (in Russian).
10. Amenitskiy A.V. Kiberbezopasnost. AI hacking. Dvoynoe naznachenie iskusstvennogo intellekta // Nauka, obshchestvo, obrazovanie: aktualnye voprosy, dostizheniya i innovatsii: sb. statey. Penza: Nauka i Prosveshchenie, 2025. S. 197–216 (in Russian).

11. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST, 2023. 42 p.
12. The NIST Cybersecurity Framework (CSF) 2.0. NIST, 2024. 27 p.
13. Lee M.J., Sinha R. Data Security, AI, and Infrastructure: Examining Cyber Risk in the Financial System [Electronic resource] // Teller Window. 2025. URL: https://tellerwindow.newyorkfed.org/
14. Understanding AI Data Poisoning [Electronic resource]. HiddenLayer, 2024. URL: https://hiddenlayer.com/
15. Securing Critical Infrastructure in the Age of AI [Electronic resource]. CSET, 2025. URL: https://cset.georgetown.edu/
16. Managing AI-related cyber risks [Electronic resource]. HM Treasury, 2025. URL: https://www.regulationtomorrow.com/
17. Boamah F.A., Jin X., Senaratne S., Perera S. AI-driven risk identification model for infrastructure projects: Utilising past project data // Expert Systems with Applications. 2025. Vol. 283 (10). Art. 127891. DOI: 10.1016/j.eswa.2025.127891.
18. Mohamed N. Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms // Knowledge and Information Systems. 2025. Vol. 67, No. 8. P. 6969–7055. DOI: 10.1007/s10115-025-02429-y.

Tables

Table 1

Comparative classification of AI system vulnerabilities in the context of threats to digital sovereignty

Category	Vulnerability examples	Potential consequences for digital sovereignty
Training	Data poisoning, systematic bias, source compromise	Incorrect forecasts in public administration systems, discriminatory decisions, insertion of "backdoors" by foreign developers
Inference	Adversarial attacks, model inversion, membership inference	Confidential data leakage, disruption of critical systems, undermining trust in domestic AI solutions
Infrastructure	Vulnerable libraries, MLOps compromise, model integrity violation	Dependence on foreign components, inability to guarantee the absence of undeclared capabilities
Processes and management	Lack of validation, insufficient audit, human factor	Errors in strategic decisions, reputational damage, reduced effectiveness of import substitution

Table 2

Integration of the methodology with NIST AI RMF and Russian standards

NIST AI RMF function	Implementation in the proposed methodology	Consideration of Russian requirements
Govern	Definition of AI risk management policies and procedures, allocation of responsibilities	Compliance with GOST R 59276-2020, consideration of FSTEC requirements for threat modeling
Map	Identification of assets, threats, vulnerabilities, attack scenarios	Use of the FSTEC Threat Database, including the new section on AI threats
Measure	Quantitative risk assessment using P(U) and I(U), sensitivity analysis, scenario modeling	Application of metrics recommended by financial sector regulators
Manage	Selection and implementation of countermeasures, effectiveness monitoring, incident management	Implementation of Russian protection tools certified by FSTEC

Индекс УДК 004.056
Код ГРНТИ 81.93.29
DOI: 10.22204/2410-4639-2026-129-01-88-102

С.В. ЛЕБЕДЬ*

Киберугрозы и безопасность банковской инфраструктуры: анализ в контексте обеспечения цифрового суверенитета России

В статье рассматриваются современные киберугрозы, влияющие на устойчивость банковской инфраструктуры Российской Федерации в контексте обеспечения цифрового суверенитета страны. Анализируется информационная инфраструктура крупных финансовых организаций, включая серверные парки, сети банкоматов, автоматизированные рабочие места, сетевое оборудование и системы кибербезопасности. Особое внимание уделяется регуляторным требованиям, предъявляемым к кредитным организациям, включая Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры», Федеральный закон № 161-ФЗ «О национальной платёжной системе», а также нормативным актам Банка России. Систематизированы основные киберриски, представлена типология современных угроз, включая фишинг, APT-атаки, программы-вымогатели, DDoS-атаки, а также новые вызовы, связанные с применением технологий искусственного интеллекта, больших языковых моделей и мультиагентных систем. Сделан вывод о необходимости комплексного подхода к обеспечению кибербезопасности банковского сектора как важнейшего элемента цифрового суверенитета России.

Ключевые слова: кибербезопасность, банковская инфраструктура, цифровой суверенитет, киберугрозы, критическая информационная инфраструктура, APT-атаки, искусственный интеллект, мультиагентные системы, регуляторные требования, финансовый сектор

Введение

Цифровой суверенитет представляет собой способность государства контролировать и защищать свою информационную среду, включая данные, системы связи, программное обеспечение и другие информационные ресурсы и технологии таким образом, чтобы обеспечить независимость от внешних факторов, включая иностранных поставщиков программного обеспечения, оборудования и услуг.

Современный этап развития глобальной цифровой экономики характеризуется активным внедрением цифровых технологий практически во все сферы жизни общества. Особое значение приобретает сфера финансовых услуг, где цифровизация привела к кардинальным изменениям в моделях оказания банковских услуг, появлению новых продуктов и сервисов. Однако наряду с преимуществами цифровизации возникли серьёз-

* **Лебедь Сергей Владимирович** — вице-президент по кибербезопасности ПАО Сбербанк.
E-mail: svlebed@sberbank.ru

ные вызовы в области кибербезопасности, ставящие под угрозу стабильность функционирования всей финансовой системы.

Стабильность финансовой системы напрямую влияет на обеспечение национального суверенитета и безопасность страны. Проблемы в сфере денежного обращения и функционирования финансовых рынков способны приводить к серьёзным социальным потрясениям и оказывать разрушительное воздействие на экономику в целом, затрагивая такие чувствительные сферы, как ВПК. Подобные негативные явления могут быть использованы заинтересованными сторонами для дестабилизации обстановки в отдельных регионах и в стране в целом.

Несмотря на усилия регуляторов и надзорных органов, направленные на повышение уровня информационной безопасности, российские банки сталкиваются с множеством серьёзных угроз, таких как фишинг, целенаправленные атаки типа Advanced Persistent Threat (APT), инсайдерская деятельность, промышленный шпионаж, кибервандализм, переходящий в последнее время к вандализму в физическом мире.

Проблематика информационной безопасности становится важнейшим фактором устойчивости всей банковской системы государства. Банковская отрасль сталкивается с такими трудностями, как недостаток эффективных механизмов раннего предупреждения угроз, сложность эффективного реагирования на киберинциденты, трудности оперативного выявления попыток мошенничества и недостаточная интеграция разнородных информационных систем. Поэтому создание надёжной и устойчивой системы защиты от компьютерных угроз приобретает первостепенное значение.

В настоящей статье рассматривается современное состояние цифровой экономики и финансовых рынков, характеризующее динамику появления новых типов атак и рост опасности цифровых угроз. Основной целью автора статьи является установление контекста глобальных изменений и выявление ключевых факторов риска для финансовых организаций.

Типовая банковская инфраструктура

Информационная инфраструктура современной финансовой организации представляет собой разветвлённую и технически сложную гетерогенную систему, включающую широкий спектр элементов: центры обработки данных, телекоммуникационное оборудование, глобальные сети передачи данных, распределённую сеть банкоматов, автоматизированные рабочие места (АРМ) сотрудников, мобильные приложения и web-сервисы для взаимодействия с клиентами, а также интеграционные сервисы с внешними партнёрами. Растущий масштаб и многообразие этой инфраструктуры неизбежно увеличивают поверхность возможных атак, создавая дополнительные точки проникновения.

Серверная инфраструктура

Крупные финансовые организации эксплуатируют десятки и сотни тысяч серверов, размещая их преимущественно в центрах обработки данных (ЦОД). Внутри каждого ЦОД обеспечивается надёжная организация бесперебойной работы, дублирование критически важных узлов и данных, а также строгое соблюдение норм кибербезопасности и физической охраны.

Значительное количество серверов объясняется необходимостью обеспечения масштабируемых экосистем, охватывающих разнообразные сегменты рынка, не только финансовые, но и такие как: розничная торговля, логистика, автомобильные услуги, индустрия развлечений, туристические сервисы, медицинское обслуживание и другие. В результате крупнейшие российские банки управляют одним из самых мощных серверных парков в стране.

Одной из заметных тенденций последних лет стало расширение использования отечественных серверных решений. Такой подход увеличивает независимость

отечественной IT-инфраструктуры от зарубежных поставщиков комплектующих и ПО, что служит укреплению цифрового суверенитета России.

Тем не менее остаётся открытым ряд стратегических задач, связанных с повышением операционной независимости и самостоятельности финансовых организаций в части серверной инфраструктуры. Дальнейшая модернизация парка серверов должна сопровождаться постоянным мониторингом мировых технологических достижений и разработкой принципиально новых решений, гарантирующих конкурентоспособность национальных игроков на международном рынке.

Банкоматная сеть

Российские банки обслуживают одну из крупнейших в мире сетей банкоматов, обеспечивая население удобством и доступностью наличных расчётов и базовых банковских операций. Лидером в этой области традиционно выступает Сбербанк, чья банкоматная сеть насчитывает 46 тысяч устройств, что составляет значительную долю от общероссийского показателя [17]. Другие крупные игроки рынка, такие как ВТБ, Альфа-Банк, Газпромбанк и Т-банк, также поддерживают значительные объёмы собственной сети. Российские банки уделяют большое внимание равномерному покрытию территорий страны, особенно регионов с низкой плотностью отделений и офисов банков.

Особую тревогу вызывает сценарий длительного и масштабного сбоя в сети банкоматов, который способен вызвать волну паники среди населения и представителей бизнеса, спровоцировав резкий всплеск спроса на снятие наличных. В случае неспособности банков оперативно удовлетворить этот повышенный спрос даже в отдельно взятом регионе, ситуация может перерасти в серьёзные социальные беспорядки, ставящие под угрозу стабильность всей страны.

Банкоматы оборудованы специализированным ПО для повышения уровня безопасности и надёжности обслуживания клиентов. Дополнительную надёжность обслуживанию придают эффективные системы мониторинга и удалённого технического обслуживания. Все устройства оснащены современными датчиками и видеокамерами, способными мгновенно фиксировать попытки неправомерного вмешательства или повреждения оборудования [4]. Во многих случаях применяется технология автономного режима работы банкомата, позволяющая продолжить оказание стандартных услуг даже при кратковременных перебоях связи или электропитания.

Широкая география распространения банкоматов вкупе с продуманными техническими и организационными мерами безопасности превращает российскую банкоматную сеть в один из важнейших элементов системы оказания качественных банковских услуг. Она удовлетворяет потребности граждан и малого бизнеса в быстром доступе к своим средствам и поддерживает экономический рост страны.

Автоматизированные рабочие места

Российский рынок банковских услуг представлен большим числом организаций, каждая из которых оснащена значительным количеством АРМ, масштабы инфраструктуры требуют особого внимания к решению вопросов безопасности АРМ.

Одной из центральных задач российских банков в последнее десятилетие стало импортозамещение ПО и ИТ. Осознавая стратегическую важность независимости от зарубежных компаний-разработчиков, банки предпринимают шаги по переводу сотрудников на отечественную инфраструктуру. Показательным примером является инициатива Сбербанка, начатая в сентябре 2024 года, когда банк приступил к поэтапному переводу около 150 тысяч сотрудников на новую российскую платформу виртуальных рабочих мест Termidesk, заменяя ранее использовавшееся иностранное ПО Citrix [18].

Переход на собственную инфраструктуру имеет важное значение для укрепления

цифрового суверенитета России и снижения рисков санкционного давления со стороны западных государств.

Сетевое оборудование и коммуникационные каналы

Российские банки представляют собой мощные цифровые экосистемы, соединённые высокоскоростной и надёжной сетевой инфраструктурой. Количество единиц сетевого оборудования ведущих банков, таких как Сбербанк, ВТБ, Альфа-Банк и другие, превышает десятки тысяч устройств, что позволяет организовать бесшовное подключение многочисленных подразделений, филиалов и офисов, расположенных по всей стране. Сети охватывают региональные подразделения, многочисленные филиалы, расположенные в городах и посёлках, а также внешние точки подключения, доступные миллионам клиентов через интернет-банки и мобильные приложения.

Сегодня ёмкость скоростных каналов достигает пропускной способности в несколько Тбит/с, что позволяет быстро передавать огромные массивы данных, обеспечивая высокое качество обслуживания [22].

Ещё одна важная особенность сетевых каналов российских банков — обеспечение высокого уровня безопасности. Современные системы защиты включают шифрование передаваемых данных, глубокую фильтрацию пакетов и интеллектуальные системы обнаружения вторжений, что препятствует возможным атакам и снижает риски компрометации ценных данных.

Благодаря развитию сетевой инфраструктуры банки России готовы не только качественно обслуживать миллионы клиентов ежедневно, но и предлагать надёжные сервисы другим участникам финансовой экосистемы. Таким образом, российская банковская отрасль, инвестируя значительные средства в развитие сетевой инфраструктуры, смогла создать единую высокоэффективную информационную магистраль, поддерживающую интероперабельность их систем, обеспечивающую быстрое и безопасное перемещение огромных объёмов данных по всей стране.

Система кибербезопасности

Современная финансовая система России функционирует в условиях повышенной угрозы со стороны киберпреступников, поэтому вопрос кибербезопасности выходит на первый план для всех крупных кредитных учреждений. Учитывая огромный масштаб проводимых операций и объём обрабатываемых данных, именно хорошо организованные системы защиты обеспечивают безопасность как самого банка, так и его клиентов.

Высокий уровень защиты возможен благодаря современному программному обеспечению, новейшему оборудованию и высококвалифицированным специалистам, которые круглосуточно контролируют ситуацию и реагируют на малейшее подозрение. Автоматизированные системы обнаружения и реагирования на инциденты позволяют оперативно идентифицировать и нейтрализовать любую попытку несанкционированного доступа или другой вид атаки.

Стоит отдельно подчеркнуть, что ведущую роль в борьбе с кибератаками на финансовый сектор играет Центр мониторинга и реагирования на компьютерные инциденты в кредитно-финансовой сфере (ФинЦЕРТ). Под руководством Банка России, ФинЦЕРТ осуществляет сбор, анализ и распространение информации о киберугрозах, помогая банкам своевременно выявлять и устранять инциденты.

Это коллективное усилие, подкреплённое бюджетом и самыми современными инструментами, позволяет российским банкам вести успешную борьбу с киберпреступностью: защищать собственную цифровую инфраструктуру, предпринимать действия для защиты клиентов и в итоге способствовать обеспечению национального цифрового суверенитета.

Инфраструктура российских банков демонстрирует высокую степень готовности к различным сценариям и позволяет решать самые сложные задачи. Накопленный опыт и отработанные технологии находят

применение не только внутри организаций, но и распространяются на государственные проекты и коммерческие структуры, оказывая позитивное влияние на национальную кибербезопасность и технологическую независимость страны.

Регуляторные требования и риск-ориентированный подход

ФЗ № 187 «О безопасности критической информационной инфраструктуры РФ» (с 01.01.2018г.) установил ряд обязательных требований для различных объектов критической информационной инфраструктуры (КИИ), включая банковские организации. Эти требования направлены на минимизацию рисков нарушения доступности, целостности и конфиденциальности важных ИС и обеспечивают повышенную защиту государственных и корпоративных структур от внешних и внутренних угроз.

Банки, будучи важнейшим элементом национальной экономики, попадают под действие этого закона.

Закон № 187-ФЗ предусматривает обязательные требования для участников банковской системы:

- установку сертифицированных средств защиты информации;
- ограничение физического доступа к серверам и устройствам;
- регулярное обновление программного обеспечения и операционных систем;
- ведение журналов регистрации событий безопасности;
- проведение регулярных проверок и аудитов систем безопасности.

Российские банки активно внедряют централизованные системы мониторинга событий безопасности (SIEM), позволяющие оперативно реагировать на любые подозрительные активности в информационной системе. Данная мера способствует раннему выявлению угроз и снижает риск успешной кибератаки.

Законом установлено требование обязательного резервирования и дублирования информационных систем и каналов связи (статья 10 Закона № 187-ФЗ).

Организация обязана осуществлять подготовку специалистов, занимающихся вопросами информационной безопасности (Приказ ФСТЭК № 235). Сотрудники, работающие с системой КИИ, проходят специальную аттестацию и периодически подтверждают свою квалификацию.

Исполнение этих требований положительно сказывается на повышении общей устойчивости банковской системы и гарантирует эффективную защиту важной государственной инфраструктуры от любых воздействий, что укрепляет позиции российского государства в области информационной безопасности.

ФЗ № 161 «О национальной платёжной системе» вступил в силу в июне 2011 года и регулирует деятельность операторов платёжных систем, организаторов расчётов и банковских организаций. Закон закрепляет правовой статус НПС и вводит важные положения, касающиеся информационной безопасности:

1. Регистрация и лицензирование операторов платёжных систем, включая оценку соответствия утверждённым критериям безопасности и надёжности.
2. Банки обязаны принять меры по защите информации, содержащейся в платёжных сервисах, от несанкционированного доступа, утраты или искажения.
3. Банки обязаны хранить и обрабатывать личные данные клиентов исключительно в предусмотренных законом целях и в соответствии с требованиями законодательства РФ о защите персональных данных.
4. Граждане имеют право на возмещение средств в случае необоснованного списания, ошибок в платежах или сбоев в системе. Банки обязаны незамедлительно уведомлять клиентов обо всех операциях и возвращать деньги в установленный срок.
5. Банки, осуществляющие международные расчёты, обязаны соблюдать действующие в России законы и нормативные акты, регулирующие международные платежи и операции.

6. Выявление нарушений влечёт наложение административных взысканий, вплоть до приостановления лицензии на проведение платёжных операций.

Одним из важных эффектов введения Федерального закона № 161-ФЗ стало укрепление позиций России в вопросах цифрового суверенитета. Национальная платёжная система, регулируемая на законодательном уровне, уменьшает зависимость от зарубежных платёжных систем и повышает управляемость процессом электронных платежей. Закон стимулирует развитие отечественного программного обеспечения и аппаратных решений, что снижает риски санкций и форс-мажорных обстоятельств, связанных с зависимостью от иностранных поставщиков.

Постановление Правительства РФ от 8 февраля 2018 г. № 127 категорирует объекты критической информационной инфраструктуры (КИИ) Российской Федерации, устанавливает показатели критериев значимости. Поскольку банковская система признана объектом КИИ, данное постановление распространяется и на банки.

Благодаря установлению единых требований и механизмов контроля российские банки улучшают свои системы защиты, снижают риски кибератак и обеспечивают защиту информации, находящейся в их распоряжении. Нормативные акты действуют как инструменты государственного регулирования, формирующие необходимую правовую базу для полноценного функционирования банковской системы России в условиях повышенного риска информационных угроз.

В ответ на резкое увеличение числа кибератак на российские организации после начала СВО российское государство предприняло ряд законодательных инициатив, направленных на укрепление технологического суверенитета и информационной безопасности.

Указ Президента РФ № 166 от 30 марта 2022 года:

- запрещает закупку иностранного ПО для значимых объектов критической информационной инфраструктуры без согласования с уполномоченными органами;
- устанавливает поэтапный переход на отечественные решения, завершившийся полным запретом на использование иностранного ПО с 1 января 2025 года;
- поручает правительству создать систему мониторинга и контроля, а также наладить подготовку кадров в сфере разработки и сопровождения отечественных решений [20].

Основной целью Указа является обеспечение технологической независимости и безопасности критической информационной инфраструктуры РФ.

Указ Президента РФ № 250 от 1 мая 2022 года:

- определяет порядок реагирования на кибератаки и привлечения к мероприятиям по кибербезопасности только аккредитованных и лицензированных организаций;
- вводит запрет на использование средств защиты информации из недружественных иностранных государств [13].

Эти меры направлены на снижение зависимости от зарубежных технологий и повышение устойчивости российской инфраструктуры к внешним угрозам.

Риск-ориентированный подход представляет собой комплексное сочетание методов управления киберрисками и сбалансированного применения мер защиты, что позволяет свести к минимуму остаточный киберриск. Процесс управления рисками начинается с их тщательного выявления и качественной оценки, после чего формируются планы по минимизации рисков в зависимости от их критичности. Далее осуществляется постоянный мониторинг существующих рисков и своевременное выявление новых угроз.

Инфраструктура банковской отрасли должна соответствовать ряду нормативных требований, но дополнительно к этому эффективно реализовывать риск-

ориентированный подход. Это означает, что все составляющие банковской инфраструктуры — от серверных ферм и сетевого оборудования до автоматизированных рабочих мест и банковских приложений — нуждаются в постоянной модернизации и мониторинге для обеспечения необходимого уровня защиты, что приводит к повышению уровня киберустойчивости банковской отрасли, которая является одной из важнейших составляющих цифрового суверенитета нашей страны.

Основные киберриски типовой банковской инфраструктуры

Важнейшими факторами риска банковской инфраструктуры являются:

- масштаб клиентской базы: большой круг клиентов, обладающих доступом к крупным финансовым ресурсам, делает банковскую инфраструктуру привлекательной целью для преступников;
- постоянное обновление технологий и устройств: быстрое развитие новых технологий и устройств создаёт дополнительную поверхность для атак. Банки вынуждены оперативно реагировать на новые виды угроз, внедряя передовые решения по защите данных и систем;
- интеграция физических и виртуальных элементов инфраструктуры: современная банковская инфраструктура сочетает физические активы (офисы, банкоматы, дата-центры) и виртуальные компоненты (интернет-банкинг, мобильные приложения, облака). Такое переплетение создаёт дополнительные уязвимости и увеличивает сложность управления рисками. Рост доли онлайн-взаимодействий и расширение дистанционного обслуживания приводят к увеличению числа возможных объектов атак.

Несмотря на значительное улучшение качества и скорости обслуживания клиентов, цифровая трансформация сопровождается появлением новых рисков, среди которых выделяют:

- финансовую уязвимость: увеличение доли цифровых операций ведёт к росту числа мошеннических операций. По данным Банка России, в 2025 году объём похищенных мошенниками средств составил 29,3 млрд рублей [12];
- операционные сбои: нарушение работоспособности цифровых каналов способно приводить к значительным экономическим убыткам и потере доверия клиентов;
- утечку данных: масштабное накопление больших объёмов данных создаёт предпосылки для массовых утечек персональной информации;
- правовые и регуляторные риски: быстрое развитие цифровых технологий опережает темпы формирования адекватного правового регулирования, создавая правовую неопределённость и затрудняя эффективное реагирование на инциденты [8].

Таким образом, цифровая трансформация, являясь мощным драйвером экономического роста, одновременно порождает комплекс новых рисков. Риск-ориентированный подход необходим для эффективного управления киберрисками в банковской сфере. Он позволяет банкам лучше подготовиться к возможным угрозам, заблаговременно выявлять новые риски и грамотно распределять ресурсы на их минимизацию. Только комплексный подход, основанный на сочетании мониторинга, анализа и постоянных улучшений, способен обеспечить высокий уровень киберустойчивости и надёжно защитить банковскую инфраструктуру от атак.

Типология современных угроз

Геополитические потрясения, начавшиеся в феврале 2022 года, оказали радикальное влияние на состояние кибербезопасности в России. Эти изменения привели к возникновению новой реальности, в рамках которой традиционные угрозы многократно усилились, а также появились совершенно новые вызовы, требующие немедленной реакции и переосмысления существующих практик защиты.

Сразу после начала специальной военной операции (СВО) наблюдается резкое увеличение числа кибератак на российские организации, включая финансовые. По данным Банка России, число кибератак на российские банки в первом полугодии 2022 года увеличилось в три раза по сравнению с аналогичным периодом прошлого года. Всего за указанный период было зафиксировано более 1 миллиона кибератак различной направленности, что сопоставимо с объёмом атак за предшествующие семь лет.

Необходимо отметить ограничение взаимодействия с западными поставщиками. Ряд российских организаций попали в список Specially Designated Nationals (SDN), введённый Министерством финансов США. Это означает полное ограничение возможностей взаимодействия с американскими компаниями, включая поставщиков решений в области кибербезопасности. Фактически более 85% зарубежных вендоров прекратили свою деятельность на территории России, оставив многие организации без необходимого оборудования и программного обеспечения для защиты от киберугроз.

Российские компании столкнулись с рядом непредвиденных трудностей, вызванных уходом западных поставщиков:

- рост числа таргетированных атак и усложнение используемых злоумышленниками техник;
- ограничение поставок импортного IT-оборудования;
- удаление российских приложений из мировых магазинов мобильных приложений;
- полный отказ от технической поддержки и прекращение выпуска обновлений, включая патчи безопасности;
- угроза отзыва сертификатов международных удостоверяющих центров;
- проблемы с использованием открытого ПО (OpenSource) для организаций, попавших под санкции.

Все перечисленные факторы привели к деградации средств защиты информации (СЗИ) многих организаций, что выразилось в отключении или полном выходе из строя межсетевых экранов, прекращении подписки на базы уязвимостей, отсутствии актуальной аналитики по киберугрозам и прекращении работы сервисов динамического анализа почтового трафика.

Международные группировки начали организованную кампанию против российских организаций. Было выявлено более 45 активных хакерских объединений, преимущественно проукраинской и прозападной ориентации, объединивших более 1 миллиона участников. Среди наиболее заметных группировок:

- IT Army of Ukraine (Украина);
- Кибер-Партизаны (Беларусь);
- Head Mare (Украина);
- BO Team (Украина);
- Anonymous (международное объединение).

Эти группы проводили скоординированные атаки на критически важные объекты инфраструктуры, включая банки, медиахолдинги и логистические компании. Среди наиболее громких инцидентов пострадали такие известные бренды, как RuTube, CDEK, Delivery Club, ivi и Первый канал. Эти атаки вызвали временное прекращение работы сервисов, утечку данных и потерю доверия со стороны клиентов.

Последние годы отмечены серией масштабных кибератак на российские организации, среди которых особо выделяются:

- Аэрофлот (2025) — атака украинского объединения Silent Crow и Belarus Cyber-Partisans, приведшая к отмене более 100 рейсов, сбоям в бронировании и выводу из строя около 7 тыс. серверов [7, 11];
- Винлаб (2025) — крупная атака программ-вымогателей, временно нарушившая работу более 2 тыс. магазинов [11];
- СДЭК (2024) — сбой в работе сайта и пунктов выдачи, вызванный внешним воздействием [6];
- ВГТРК (2024) — кратковременный сбой онлайн-вещания и внутренних сервисов [6].

Эти инциденты не только нанесли прямой экономический ущерб, но и проде-

монстрировали уязвимость критически важной инфраструктуры перед лицом современных киберугроз.

Значительная часть атак носила ярко выраженный политический характер. Перечисленные выше международные группировки проводят скоординированные кампании, направленные на дестабилизацию российской инфраструктуры. Политически мотивированные кибератаки становятся инструментом гибридных войн, что требует от государства принятия незамедлительных мер по укреплению цифрового суверенитета.

В ответ на указанные вызовы российское государство предприняло ряд законодательных инициатив, направленных на укрепление технологического суверенитета и информационной безопасности. Основные из них были перечислены выше.

Одной из ключевых проблем на пути к достижению полноценного цифрового суверенитета является острейший дефицит квалифицированных специалистов в области информационной безопасности. Нехватка специалистов по ИБ в России — порядка 50 тысяч человек. Не хватает экспертов, чтобы закрыть половину всех имеющихся на рынке вакансий. Особенно востребованы специалисты в ИТ-компаниях, банках и розничной торговле [15]. Дефицит объясняется несколькими причинами:

- большая часть опытных специалистов уже трудоустроена;
- выпускники вузов требуют дополнительного обучения и адаптации;
- молодые специалисты предпочитают профессии, связанные с разработкой и аналитикой, оставляя сферу кибербезопасности с меньшим интересом;
- быстрый рост потребностей рынка опережает возможности образовательной системы, которая выпускает всего 10-15 тыс. специалистов ежегодно, что покрывает лишь малую часть спроса [3, 14, 16, 19, 23].

Несмотря на имеющиеся трудности, существует позитивная динамика в увеличении числа занятых в сфере кибербезопасности. С 2016 по 2023 год количество специалистов удвоилось и достигло 110 тыс. человек. Эксперты прогнозируют дальнейший рост до 181-196 тыс. к 2027 году, хотя дефицит кадров останется значительным — около 54-65 тыс. специалистов [16, 23].

Геополитические изменения, произошедшие в 2022 году, создали абсолютно новую реальность для российских организаций, включая финансовые. Возросшая интенсивность атак, ограничение доступа к технологиям и разрыв связей с иностранными поставщиками поставили перед российским бизнесом беспрецедентные вызовы. Решение этих проблем требует срочной мобилизации ресурсов, перехода на отечественные разработки и формирования новых подходов к обеспечению кибербезопасности, способных выдержать давление внешней агрессии и сохранить устойчивость национальной финансовой системы.

Типология современных угроз типовой банковской инфраструктуры

Современные кибератаки отличаются высоким уровнем организованности, профессионализмом и разнообразием техник. Анализируя современную ситуацию в сфере кибербезопасности, эксперты выделяют ряд наиболее опасных типов атак, направленных против банков и финансовых учреждений.

1. **Фишинг и социальная инженерия**

Фишинговые атаки продолжают оставаться одним из самых распространённых способов похищения конфиденциальной информации. Преступники применяют высокотехнологичную социальную инженерию, маскируясь под официальных представителей банков и вынуждая пользователей раскрывать личные данные. Под угрозой находятся личные счета, карты и персональные данные клиентов [2, 24].

2. **Целевые атаки (Advanced Persistent Threats, APT)**

Это самые опасные и технически сложные виды атак, организованные профессиональными группами с финансированием государств или преступных синдикатов. Такие атаки нацелены на длительную скры-

тую эксплуатацию уязвимостей с целью систематического сбора ценных данных, включая исходные коды и внутреннюю документацию компаний, а также нанесения максимального ущерба [9].

3. **Программы-шпионы и вымогатели (Ransomware)**

Программные вирусы, крадущие данные или шифрующие файлы, требуют выкуп за восстановление работоспособности системы. Масштаб заражения настолько велик, что даже государственные ведомства подвергаются подобным атакам.

4. **Ботнеты и распределённые атаки отказа в обслуживании (DDoS)**

DDoS-атаки направлены на перегрузку серверов банков и сетей связи, что приводит к временной утрате доступности сервисов. Подобные атаки наносят серьёзный репутационный и экономический ущерб, вызывая недовольство клиентов и потерю конкурентоспособности [9]. Создаются ботнеты — сети заражённых компьютеров, способные генерировать мощные потоки запросов, приводящие к перегрузкам и остановке работы важнейших систем банков.

5. **Угроза искусственного интеллекта (ИИ), включая LLM и мультиагентные системы**

Совершенствование технологий искусственного интеллекта и возникновение больших языковых моделей (Large Language Models, LLM) привело к появлению новых классов угроз, представляющих особую опасность для банковской инфраструктуры. В последние годы наибольшую озабоченность вызывают две разновидности угроз:

- генеративный ИИ;
- агенты на основе LLMs;
- мультиагентные системы.

Развитие технологий ИИ открывает широкие перспективы для автоматизации процессов и повышения эффективности, но одновременно создаёт дополнительные риски. Хакеры активно осваивают технологии генеративного ИИ для создания сложных вредоносных программ, способных адаптироваться к защитным механизмам и избегать обнаружения традиционными средствами защиты, а также дипфейков и персонализированных фишинговых писем, используемых для подделывания личности сотрудников банка или клиентов.

LLM обладают огромной мощностью и широким спектром способностей, включая умение имитировать поведение людей, создавать убедительные тексты и взламывать системы с минимальным вмешательством человека. В руках злоумышленников эти технологии могут стать эффективным оружием для реализации широкомасштабных атак:

- имитация легитимных персон — подделка электронных писем, голосовых сообщений и чат-ботов, для убеждения сотрудников банков раскрыть конфиденциальную информацию;
- генерация контента, в том числе персонифицированного, для атак — агенты LLMs способны создавать качественные материалы для фишинга, социальной инженерии и дезинформации;
- автоматизация атак — атаки могут происходить в массовом масштабе, при этом агент LLM сможет точно выбирать жертвы и подбирать индивидуальные сценарии нападения.

Появились мультиагентные системы, в которых агенты скоординированно выполняют отдельную роль/функцию в рамках единой миссии, усиливая совокупную мощность атак:

- распределённая атака на систему — несколько агентов могут одновременно атаковать разные участки инфраструктуры банка, отвлекая ресурсы защиты и увеличивая шансы успеха атаки;
- совместная разведка и эксплуатация уязвимостей — мультиагенты могут параллельно искать уязвимости и совместно вырабатывать стратегию их эксплуатации;
- самообучение и адаптация — мультиагентные системы способны учиться на предыдущих действиях и адаптироваться к изменениям в инфраструктуре банка, что значительно осложняет усилия по их нейтрализации.

6. **Угроза внутреннего нарушителя (инсайды)**

Проблема инсайдерских угроз заключается в действиях сотрудников, имеющих легитимный доступ к информационным системам банка. Ранее исследования показывали, что такие нарушители занимали бóльшую долю в проводимых атаках. Недовольство персонала, халатность или корысть могут привести к серьёзным инцидентам, связанным с утечкой данных или нанесением ущерба инфраструктуре [10].

7. **Финансовые мошенничества**

Классические мошеннические схемы, такие как подделка электронных писем, фальсификация реквизитов и социальная инженерия, продолжают представлять значительную угрозу. Эксперты отмечают, что в 2025 году вероятность значительных инцидентов информационной безопасности составляет от 12% до 20%, а к 2026 году этот показатель может увеличиться до уровня выше 25% [5].

8. **Взлом API-интерфейсов**

API-интерфейсы являются неотъемлемой частью архитектуры современных банковских приложений. На совместных открытых API построены сервисы открытого банкинга (Open banking), когда банки обмениваются информацией о счетах и транзакциях, а также предоставляются сервисы сторонних организаций через поверхность банка [1]. Это позволяет клиентам в одном приложении видеть счета и балансы разных банков, а также получать услуги сторонних сервисов. Компрометация API способна привести к массовым утечкам данных и финансовым потерям, затрагивающим большое количество клиентов [21]. Актуальность данной атаки возрастает в связи с выходом финансовых организаций в облака, наращиванием взаимодействия, началом развития ИИ помощников и AI агентов, которые просто не смогут работать без открытых API.

В современном ландшафте угроз всё более доминирующую позицию занимают сложные, многогранные атаки, основанные на использовании AI, LLMs и мультиагентных систем. Эти технологии серьёзно усложняют традиционные подходы к обеспечению информационной безопасности и требуют радикально новых подходов к построению систем защиты.

Заключение

Рассмотрены основные тенденции и угрозы, влияющие на устойчивость финансовых учреждений, а также проанализированы регуляторные требования и законодательные инициативы, направленные на укрепление защиты данных и инфраструктуры банков.

Современная цифровая среда диктует необходимость выработки комплексной стратегии кибербезопасности, сочетающей технические, организационные и правовые меры. Банковская отрасль сталкивается с широким спектром угроз, начиная от традиционного фишинга и заканчивая высокоорганизованными APT-операциями, реализуемыми в реальном времени мультиагентными системами. Эффективное противостояние этим вызовам возможно только при условии тесного сотрудничества между государством, бизнесом и научным сообществом, направленного на формирование устойчивой и надёжной системы защиты национальных экономических интересов.

Представленный обзор показывает, насколько важны современные СЗИ и умение предвидеть угрозы для устойчивого функционирования банков. Основными выводами статьи являются:

- высокая степень зависимости финансовой системы от надёжности информационных сетей и коммуникаций;
- необходимость постоянного мониторинга текущих угроз и адаптации систем защиты к новым технологиям;
- рост влияния регуляторов и законодателей на политику безопасности банков.

Цифровой суверенитет является необходимым условием для сохранения национальной безопасности и независимости в условиях современных геополитических вызовов. Российская Федерация предпринимает активные шаги по укреплению тех-

нологического суверенитета, однако существующие проблемы в области кадрового обеспечения и технологической независимости требуют скорейшего разрешения.

Текущий тренд развития систем защиты должен быть направлен на кардинальное повышение эффективности борьбы с новыми поколениями угроз, вызванных появлением таких технологий, как агенты ИИ и мультиагентные атакующие системы. Сегодня количество ежедневно регистрируемых киберсобытий измеряется триллионами, и с активным внедрением агентов ИИ это число увеличится на порядки. Следовательно, новое поколение систем защиты должно уметь не только оперативно обрабатывать и анализировать миллиарды событий в реальном времени, но и выявлять скрытую корреляцию между отдельными инцидентами, происходящими в гетерогенных системах и сетях.

ЛИТЕРАТУРА

1. База знаний Открытого банкинга в России [Электронный ресурс]. URL: https://wiki.openbankingrussia.ru
2. Юдина О. Бизнес под защитой: как интернет-банк СберБизнес обеспечивает безопасность данных [Электронный ресурс]. URL: https://sberbusiness.live/publications/biznes-pod-zaschitoi-kak-internet-bank-sberbiznes-obespechivaet-bezopasnost-dannih
3. В России дичайший дефицит ИБ-специалистов. Все хорошие уже заняты, а вузы выпускают «сырых» [Электронный ресурс]. URL: https://www.cnews.ru/news/top/2025-02-04_v_rossii_dichajshchij_defitsit
4. Чернов А. В Сбере рассказали о развитии своего банкоматного сервиса [Электронный ресурс]. URL: https://www.gazeta.ru/business/news/2023/06/27/20754836.shtml
5. Пославская Ю., Буйлов М. Вероятность ИБ-инцидентов в финансовой сфере может превысить 25% [Электронный ресурс]. URL: https://www.kommersant.ru/doc/8006168
6. Ясакова Е. Винлаб, ВГТРК, СДЭК: какие ещё компании пострадали от хакерских атак [Электронный ресурс]. URL: https://hi-tech.mail.ru/review/131095-vinlab-vgtrk-sdek-kakie-eshe-kompanii-postradali-ot-hakerskih-atak/
7. Пашкова Л. Власти дали рекомендации перевозчикам после хакерской атаки на «Аэрофлот» [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/09/09/2025/68bfa9a99a794763c9f0bf05
8. Информационная безопасность в банках [Электронный ресурс]. URL: https://www.tadviser.ru/a/314707
9. Какие угрозы информационной безопасности наиболее опасны в 2025 году и как бизнесу защититься от утечек, атак и сбоев [Электронный ресурс]. URL: https://www.kt-team.ru/blog/cybersecurity-threats-2025
10. Кибератаки 2025: что нового готовят злоумышленники [Электронный ресурс]. URL: https://www.computerra.ru/312655/kiberataki-2025-chto-novogo-gotovyat-zloumyshlenniki
11. Миллионные убытки: почему от хакеров страдают даже компании-гиганты и как защитить свой бизнес от кибератак [Электронный ресурс]. URL: https://incrussia.ru/share/letnie-vzlomy-2025
12. Болотов С. Мошенники поставили рекорд по хищениям со счетов россиян в банках в 2025 году [Электронный ресурс]. URL: https://rg.ru/2026/02/16/moshenniki-postavili-rekord-po-hishcheniiam-so-schetov-rossiian-v-bankah-v-2025-godu.html?utm_referrer=https%3A%2F%2Fwww.google.com%2F
13. Заведенская А. Разъяснения к Указу Президента о дополнительных мерах по обеспечению ИБ (№ 250 от 01.05.2022) [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-250-Clarifications

14. Катковская Ю. Российский IT-рынок 2025: парадокс кадрового голода на фоне рекордной безработицы [Электронный ресурс]. URL: https://tproger.ru/articles/rossijskij-it-rynok-2025--paradoks-kadrovogo-goloda-na-fone-rekordnoj-bezraboticy
15. Быстрова Е. Рынок ИБ в 2025: нехватка кадров и рост зарплат до миллиона рублей [Электронный ресурс]. URL: https://www.anti-malware.ru/news/2025-05-27-111332/46173
16. Рынок труда в информационной безопасности в России в 2024–2027 гг.: прогнозы, проблемы и перспективы [Электронный ресурс]. URL: https://ptsecurity.com/research/analytics/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy
17. Соловьев И. Сбербанк лидирует по числу банкоматов и качеству их обслуживания [Электронный ресурс]. URL: https://www.newsinfo.ru/news/2015-09-28/bankomats/778845
18. Сбербанк удаляет ПО Citrix и переводит 150 тыс. сотрудников на российскую инфраструктуру виртуальных рабочих мест [Электронный ресурс]. URL: https://www.tadviser.ru/a/829352
19. Спрос рождает удаление [Электронный ресурс]. URL: https://www.kommersant.ru/doc/7478242
20. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента РФ от 30.03.2022 № 166 [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47688
21. Минаев И. Цифровизация в банковской сфере [Электронный ресурс]. URL: https://boostra.ru/pages/articles/tsifrovizatsiya-bankovskikh-uslug-vozmozhnosti-i-vyzovy
22. ЦОДы Сбербанка [Электронный ресурс]. URL: https://www.tadviser.ru/a/469027
23. ЦСР «Северо-Запад» и Positive Technologies представили исследование по дефициту кадров на рынке кибербезопасности РФ [Электронный ресурс]. URL: https://habr.com/ru/news/820237
24. Петрова Ю. Эксперты назвали главные киберугрозы для банков и их клиентов в 2025 году [Электронный ресурс]. URL: https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu

Cyberthreats and Banking Infrastructure Security: an Analysis in the Context of Ensuring Russia's Digital Sovereignty

Sergei Vladimirovich Lebed — Vice President for Cybersecurity at Sberbank PJSC.
E-mail: svlebed@sberbank.ru

This article examines modern cyberthreats affecting the resilience of the Russian Federa-tion's banking infrastructure in the context of ensuring the country's digital sovereignty. It analyzes an information infrastructure of large financial institutions, including server farms, ATM networks, automated workstations, network equipment, and cybersecurity systems. Par-ticular attention is paid to regulatory requirements imposed on credit institutions, including Federal Law No. 187-FZ "On the Security of Critical Information Infrastructure", Federal Law No. 161-FZ "On the National Payment System", as well as regulatory acts of the Bank of Russia. The author systematizes the main cyber risks and presents a typology of modern threats, including fishing, APT attacks, ransomware, DDoS attacks, as well as new challenges associated with the use of artificial intelligence technologies, large-scale language models, and multi-agent systems. The author concludes that a comprehensive approach to ensuring the cybersecurity of the banking sector is essential as a crucial element of Russia's digital sovereignty.

Keywords: cybersecurity, banking infrastructure, digital sovereignty, cyber threats, critical information infrastructure, APT attacks, artificial intelligence, multi-agent systems, regulatory requirements, financial sector

REFERENCES

1. Baza znaniy Otkrytogo bankinga v Rossii [Electronic resource]. URL: https://wiki.openbanking-grussia.ru (in Russian).
2. Yudina O. Biznes pod zashchitoy: kak internet-bank SberBiznes obespechivaet bezopasnost dannykh [Electronic resource]. URL: https://sberbusiness.live/publications/biznes-pod-zaschitoi-kak-internet-bank-sberbiznes-obespechivaet-bezopasnost-dannih (in Russian).
3. V Rossii dichayshiy defitsit IB-spetsialistov. Vse khoroshie uzhe zanyaty, a vuzy vypuskayut «syrykh» [Electronic resource]. URL: https://www.cnews.ru/news/top/2025-02-04_v_rossii_dichajshchij_defitsit (in Russian).
4. Chernov A. V Sbere rasskazali o razvitii svoego bankomatnogo servisa [Electronic resource]. URL: https://www.gazeta.ru/business/news/2023/06/27/20754836.shtml (in Russian).
5. Poslavskaya Yu., Buylov M. Veroyatnost IB-intsidentov v finansovoy sfere mozhet prevysit 25% [Electronic resource]. URL: https://www.kommersant.ru/doc/8006168 (in Russian).
6. Yasakova E. Vinlab, VGTRK, SDEK: kakie eshche kompanii postradali ot khakerskikh atak [Electronic resource]. URL: https://hi-tech.mail.ru/review/131095-vinlab-vgtrk-sdek-kakie-eshe-kompanii-postradali-ot-hakerskih-atak/ (in Russian).
7. Pashkova L. Vlasti dali rekomendatsii perevozchikam posle khakerskoy ataki na «Aeroflot» [Electronic resource]. URL: https://www.rbc.ru/technology_and_media/09/09/2025/68bfa9a99a794763c9f0bf05 (in Russian).
8. Informatsionnaya bezopasnost v bankakh [Electronic resource]. URL: https://www.tadviser.ru/a/314707 (in Russian).
9. Kakie ugrozy informatsionnoy bezopasnosti naibolee opasny v 2025 godu i kak biznesu zashchititsya ot utechek, atak i sboev [Electronic resource]. URL: https://www.kt-team.ru/blog/cybersecurity-threats-2025 (in Russian).
10. Kiberataki 2025: chto novogo gotovyat zloumyshlenniki [Electronic resource]. URL: https://www.computerra.ru/312655/kiberataki-2025-chto-novogo-gotovyat-zloumyshlenniki (in Russian).
11. Millionnye ubytki: pochemu ot khakerov stradayut dazhe kompanii-giganty i kak zashchitit svoy biznes ot kiberatak [Electronic resource]. URL: https://incrussia.ru/share/letnie-vzlomy-2025 (in Russian).
12. Bolotov S. Moshenniki postavili rekord po khishcheniyam so schetov rossiyan v bankakh v 2025 godu [Electronic resource]. URL: https://rg.ru/2026/02/16/moshenniki-postavili-rekord-po-hishcheniiam-so-schetov-rossiian-v-bankah-v-2025-godu.html (in Russian).
13. Zavedenskaya A. Razyasneniya k Ukazu Prezidenta o dopolnitelnykh merakh po obespecheniyu IB (№ 250 ot 01.05.2022) [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-250-Clarifications (in Russian).
14. Katkovskaya Yu. Rossiyskiy IT-rynok 2025: paradoks kadrovogo goloda na fone rekordnoy bezrabotitsy [Electronic resource]. URL: https://tproger.ru/articles/rossijskij-it-rynok-2025--paradoks-kadrovogo-goloda-na-fone-rekordnoj-bezraboticy (in Russian).
15. Bystrova E. Rynok IB v 2025: nekhvatka kadrov i rost zarplat do milliona rubley [Electronic resource]. URL: https://www.anti-malware.ru/news/2025-05-27-111332/46173 (in Russian).
16. Rynok truda v informatsionnoy bezopasnosti v Rossii v 2024–2027 gg.: prognozy, problemy i perspektivy [Electronic resource]. URL: https://ptsecurity.com/research/analytics/rynok-truda-v-informaczionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy (in Russian).
17. Solovyev I. Sberbank lidiruet po chislu bankomatov i kachestvu ikh obsluzhivaniya [Electronic resource]. URL: https://www.newsinfo.ru/news/2015-09-28/bankomats/778845 (in Russian).
18. Sberbank udalyaet PO Citrix i perevodit 150 tys. sotrudnikov na rossiyskuyu infrastrukturu virtualnykh rabochikh mest [Electronic resource]. URL: https://www.tadviser.ru/a/829352 (in Russian).

19. Spros rozhdaet udalenie [Electronic resource]. URL: https://www.kommersant.ru/doc/7478242 (in Russian).
20. O merakh po obespecheniyu tekhnologicheskoy nezavisimosti i bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Ukaz Prezidenta RF ot 30.03.2022 № 166 [Electronic resource]. URL: http://www.kremlin.ru/acts/bank/47688 (in Russian).
21. Minaev I. Tsifrovizatsiya v bankovskoy sfere [Electronic resource]. URL: https://boostra.ru/pages/articles/tsifrovizatsiya-bankovskikh-uslug-vozmozhnosti-i-vyzovy (in Russian).
22. TsODy Sberbanka [Electronic resource]. URL: https://www.tadviser.ru/a/469027 (in Russian).
23. TsSR «Severo-Zapad» i Positive Technologies predstavili issledovanie po defitsitu kadrov na rynke kiberbezopasnosti RF [Electronic resource]. URL: https://habr.com/ru/news/820237 (in Russian).
24. Petrova Yu. Eksperty nazvali glavnye kiberugrozy dlya bankov i ikh klientov v 2025 godu [Electronic resource]. URL: https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu (in Russian).

Индекс УДК 004.75
Код ГРНТИ 49.33.35
DOI: 10.22204/2410-4639-2026-129-01-103-112

А.А. ИГОНИН*

Безопасный и дешёвый криптокошелёк на базе доверенной SIM-карты

В работе приведена современная классификация блокчейн сетей и узлов, а также клиентов блокчейн, выполняющих функции криптокошельков. Рассмотрен функционал аппаратного устройства электронной подписи на базе доверенной SIM-карты и возможности интеграции аппаратного устройства с различными программными криптокошельками, перечислены конкурентные преимущества подобного технического решения.

Ключевые слова: блокчейн, криптокошелёк, доверенная SIM-карта

Исходная идея использования распределённого публичного реестра или базы данных на основе технологии электронной подписи последовательной цепи блоков (далее — блокчейн) в качестве децентрализованного платёжного средства (децентрализованных финансов, DeFi) в дальнейшем привела к стремительному развитию во многих отраслях и сферах экономического взаимодействия различных хозяйствующих субъектов. В значительной мере данному росту сопутствовало создание и работа основанных на смарт-контрактах (*smart contract*) децентрализованных приложений (DApp), создаваемых разработчиками с помощью некоторого языка программирования, совместимого с той или иной блокчейн-платформой.

В настоящее время успешные примеры использования децентрализованных приложений отмечаются в сфере финансовых транзакций (автоматическое выполнение условий перевода средств, обеспечение кредитования, депозиты и прочее) [1, 2], логистике и поставках (автоматизация процессов поставок, отслеживание товаров и обеспечение выполнения условий договоров) [3], страховании (автоматическое выполнение условий страховых выплат при наступлении определённых событий) [4], процедурах токенизации активов (выпуск различных цифровых активов и управление ими) [5], игровой индустрии (управление внутриигровыми активами, правила распределения призов и наград) [6].

Разрабатывается всё больше блокчейн-решений с различными характеристика-

* **Игонин Андрей Александрович** — заместитель начальника отдела, АО «Институт точной механики и вычислительной техники им. С.А. Лебедева РАН».
E-mail: info@ipmce.ru

ми, ориентированными на разные области применения. Блокчейн-платформы развиваются и совершенствуются, предлагают новые способы организации различных бизнес-процессов, делая их более прозрачными, безопасными, децентрализованными и также, при правильной имплементации, экономически более выгодными по сравнению с классическим подходом, основанным на традиционных (фиатных) средствах платежей и клиент-серверных решениях.

С точки зрения разработчика, блокчейн модель или сеть может обладать уникальной архитектурой и собственным фреймворком (эталонный клиент блокчейн), а может быть так называемым клоном некоторой существующей блокчейн-платформы с различными внесёнными изменениями в протокол сети. Первый вариант принято называть **нативным** (*native*) блокчейном или блокчейном на собственных решениях, а второй — **форком** (*fork*) исходного блокчейна. При этом также принято различать так называемые «мягкие» форки (*softfork*) и «жёсткие» форки (*hardfork*). «Мягкий» форк является полностью совместимым с исходной версией протокола блокчейн, и внесённые изменения технически всегда возможно отменить. «Жёсткий» форк несовместим с исходным кодом как минимум в части майнинга криптовалюты. Как следствие, «жёсткий» форк приводит к созданию новой криптовалюты, неспособной работать в одной сети с оригиналом.

По отношению совместимости (возможности кроссплатформенных взаимодействий) все блокчейн-платформы можно разделить на классы эквивалентности. Определение совместимости различных блокчейн требует проведения анализа их протоколов по следующим направлениям:

- стандарты токенов;
- механизмы консенсуса;
- смарт-контракты;
- протоколы обмена данными при взаимодействии узлов.

Все блокчейн сети также принято подразделять на два основных типа, получивших своё наименование по аналогии с ключами ассиметричных криптосистем:

- **открытый** (публичный) блокчейн;
- **закрытый** (приватный) блокчейн.

Своеобразным мостом между Пользователями и протоколом блокчейн сети выступает **блокчейн клиент** — программное обеспечение и/или физическое устройство, которое позволяет «подключаться» к сети блокчейн. Примеры эталонных блокчейн клиентов: Geth для сети Ethereum [7], Bitcoin Core для сети Bitcoin [8].

Приходящая на смену клиент-серверной модели Web2.0 новая форма цифровой инфраструктуры Web3.0 [9], где основной акцент сделан на децентрализации, прозрачности и пользовательском контроле, предполагает использование вычислительной модели взаимодействия блокчейн, в которой данные и приложения защищаются не различными централизованными посредниками, а децентрализованной сетью [10].

Узлами или нодами блокчейн принято называть устройства блокчейн сети, которые в совокупности отвечают за хранение копий распределённого реестра блокчейн, проверку транзакций и общение компонентов сети друг с другом. Данные узлы представляют собой «строительные кирпичи» архитектуры блокчейн, и от степени их защищённости зависит безопасность децентрализованных приложений и самой сети в целом.

С точки зрения протокола в различных блокчейн сетях могут быть реализованы и одновременно сосуществовать разные типы узлов. При этом в зависимости от практической реализации их функциональные характеристики могут пересекаться. Однако общепринятой является следующая классификация узлов блокчейн сети:

1. **Полные ноды или суперноды (*full nodes, supernodes*)**

Суперноды хранят полную копию всей цепи блоков блокчейн, а также участвуют в проверке и подтверждении (валидации)

транзакций, обеспечивают следующий функционал:

- проверка транзакций на соответствие правилам блокчейн сети (проверка электронных подписей, «двойных трат» кошельков и прочих условий);
- распространение информации о новых блоках транзакций по всей блокчейн сети, обеспечение синхронизации блокчейн для всех участников;
- поддержка безопасности путём участия в алгоритме консенсуса и голосовании о валидности новых блоков транзакций, обеспечение защиты блокчейн сети от различных атак и некорректных данных.

2. **Архивные ноды**

Архивные ноды хранят не только текущее состояние блокчейн, но и всю историю изменений. В отличие от полных нод обладают урезанным функционалом. Используются для запроса исторических данных, а также для восстановления состояния сети на любой момент времени. Как правило, имеют высокие требования к аппаратному обеспечению.

3. **Лёгкие ноды (*light nodes*)**

Лёгкие ноды вместо полной копии всего реестра блокчейн хранят только заголовки блоков. В отличие от полных нод обладают урезанным функционалом. Другие особенности:

- рассчитаны для использования в устройствах с ограниченными ресурсами, например, для абонентских терминалов;
- могут использоваться для проведения транзакций и проверки их состояния без необходимости загружать весь реестр блокчейн.

4. **Валидаторы (*validators*)**

Основной функционал нод-валидаторов заключается в проверке и подтверждении (валидации) транзакций, а именно:

- поддержание консенсуса блокчейн сети: валидаторы согласовываются между собой относительно состояния блокчейн сети и правильности транзакций, предлагая или голосуя за включение конкретных транзакций в блокчейн сеть;
- проверка транзакций: валидаторы проверяют каждую транзакцию на соответствие правилам протокола и на наличие достаточного количества средств для её осуществления, отклоняя при этом недопустимые транзакции и блокируя попытки мошенничества;
- формирование новых блоков: в некоторых блокчейн сетях валидаторы также отвечают за создание новых блоков, содержащих недавно проведённые транзакции.

В узком смысле валидаторами называют производителей блоков с алгоритмом консенсуса Proof of Stake.

5. **Майнинговые ноды или производители блоков (*mining nodes, block producer nodes*)**

Основной функционал майнинговых нод заключается в формировании и добавлении новых блоков в блокчейн сеть. Майнинговые ноды используют специализированное аппаратное обеспечение и потребляют значительное количество электрической энергии. В узком смысле майнинговыми нодами называют производителей блоков с алгоритмом консенсуса Proof of Work.

6. **Узлы Remote Procedure Call или провайдеры (*RPC nodes*)**

Основной функционал узлов RPC заключается в обеспечении доступа к сети блокчейн для различных клиентов сети блокчейн. Узлы RPC часто используются теми, кто не имеет или не может запустить свою собственную суперноду или лёгкую ноду. Любой Пользователь при подключении своего клиента блокчейн через провайдера неявно доверяет его честности, поскольку никакой работы по самопроверке не проводится. Данные узлы также именуются RPC-провайдерами, в частности провайдерами криптокошельков.

Отметим, что по своей сути блокчейн сеть предназначена для обслуживания конечных Пользователей, поэтому важной частью технологии блокчейн являются клиенты блокчейн, которые принято обозначать термином криптокошельки (*wallets*).

Криптокошелёк — это программное обеспечение и/или физическое устройство, которое позволяет Пользователям одновременно взаимодействовать с различными блокчейн сетями, предоставляя доступ к криптовалютам, хранящимся в сетях путём выполнения транзакций.

В отличие от узлов, которые выполняют функции хранения копии распределённого реестра блокчейн, проверки криптовалютных транзакций и общения между собой, криптокошельки обеспечивают хранение криптографических ключей Пользователей, подписание, отправку и получение транзакций, а также мониторинг баланса и истории транзакций.

Криптографические ключи Пользователей, хранящиеся в криптокошельках, предоставляют собой пары закрытых и открытых ассиметричных ключей, выработанных согласно заданным стандартам протоколов сетей блокчейн с использованием, как правило, алгоритмов ассиметричной криптографии на группе точек эллиптических кривых. Закрытые ключи необходимы для формирования электронной подписи (ЭП) транзакций Пользователя, открытые — для идентификации Пользователя в сетях блокчейн и проверки ЭП транзакций.

С точки зрения формы существования криптокошельки подразделяются на:

- **программные** (обладают только цифровой формой);
- **аппаратные** (представляются в виде физического носителя (например, USB-токен));
- **бумажные** (документ, на котором напечатан закрытый ключ (как правило, в виде QR-кода)).

Если рассматривать криптокошелёк как средство хранения криптографических ключей, необходимое владельцам криптовалют для доступа к различным сетям блокчейн и управления своими криптовалютами, то все криптокошельки можно разделить на следующие группы.

Горячие криптокошельки существуют только в цифровой форме, постоянно подключены к сети, доступ к средствам Пользователей можно получить через браузер или мобильное приложение. Такие криптокошельки удобны для быстрых транзакций, но уязвимы для различных угроз информационной безопасности.

Примеры: MetaMask [11], Coinbase Wallet, Exodus.

Холодные (жёсткие) криптокошельки для доступа к средствам не требуют прямого подключения к сети, для хранения криптовалют используются в автономном режиме. Подразделяются на аппаратные холодные кошельки (подключаются к сети опосредовано, только когда нужно осуществить транзакцию) и бумажные холодные кошельки (зачастую используются как резервные копии аппаратного или программного криптокошелька). Считаются более безопасными с точки зрения получения доступа к закрытым ключам Пользователей.

Примеры: Ledger [12], Trezor, KeyStone.

Как горячие, так и холодные криптокошельки относятся к так называемым **некастодиальным** криптокошелькам. В отличие от них существуют также **кастодиальные** криптокошельки (*custodial wallet*) — для которых управление ключами доверено третьей стороне, например, криптовалютной бирже или специализированному сервису.

Основным удобством кастодиальных кошельков является невозможность утраты доступа к нему вследствие потери Пользователем пароля, ключа или seed-фразы. Однако платой за это является полная зависимость и прозрачность Пользователей для третьей стороны.

Использование горячих кошельков оправдано для совершения повседневных транзакций, а основной капитал следует хранить на холодных кошельках.

Криптокошельки можно также классифицировать по степени их автономности и способу взаимодействия с сетью блокчейн:

- **Толстый криптокошелёк или полноценный клиент** предназначен для проверки всей истории транзакций блокчейна (каждая транзакция каждого

Пользователя за всё время существования блокчейна начиная с блока генезиса). Фактически толстый кошелёк является супернодой с добавлением функционала криптокошелька Пользователя. Опционально, полноценные клиенты могут также хранить подтверждённые ранее транзакции и предоставлять данные другим программам блокчейна. Полноценный клиент использует значительные компьютерные ресурсы, но при этом он обеспечивает пользователям полную автономность.

- **Тонкий криптокошелёк или облегчённый клиент (клиент с упрощённой проверкой платежей, *Simplified-Payment-Verification*, SPV)** подключается к какому-либо узлу сети (например, узлу RPC) для получения и отправки информации о транзакциях, но в то же время обеспечивает локальное хранение пользовательского секретного ключа криптокошелька, частичную проверку получаемых транзакций и независимое создание исходящих транзакций.
- **API-криптокошелёк или сторонний API-клиент** предназначен для взаимодействия с сетью блокчейн через систему API сторонних разработчиков, а не путём прямого подключения. Такой криптокошелёк может храниться у Пользователя или на сторонних серверах, но при этом будет полностью доверять удалённому серверу, который будет передавать ему точную информацию и обеспечивать его конфиденциальность и анонимность.

В зависимости от среды функционирования криптокошельки также можно условно разделить на следующие категории:

- **Десктопный криптокошелёк** является исторически первым типом криптокошелька. Именно такой криптокошелёк обычно разрабатывается в качестве эталонного варианта. Многие Пользователи работают с десктопными криптокошельками по причине предлагаемых ими «богатых» возможностей, автономности и управляемости. Однако работа в распространённых операционных системах связана с известными недостатками в плане обеспечения безопасности, поскольку данная среда функционирования часто оказывается плохо настроенной и незащищённой.
- **Мобильный криптокошелёк** в настоящее время можно назвать наиболее распространённым типом криптокошелька. Эти приложения работают в операционных системах абонентских терминалов или планшетов, и зачастую представляют собой оптимальный выбор для начинающих Пользователей. Многие из этих кошельков рассчитаны в основном на простоту и удобство использования, но есть и полнофункциональные мобильные кошельки для опытных Пользователей. Чтобы не загружать и не хранить большие объёмы данных, многие мобильные кошельки получают информацию с удалённых узлов. Это снижает уровень анонимности, поскольку позволяет третьим лицам получать сведения о пользовательских адресах и балансах. Также обладает недостатками десктопного криптокошелька.
- **Веб криптокошелёк**. Доступ к вебкошелькам открывается через браузер, а сам криптокошелёк находится на сервере стороннего сервиса. Большинство подобных систем лишают Пользователей контроля над своими ключами в обмен на простоту использования. Однако некоторые из этих сервисов используют клиентский код, запускаемый в браузере, что даёт возможность сохранить контроль над ключами блокчейна в руках владельца, хотя его зависимость от сервиса всё равно ставит конфиденциальность под угрозу.
- **Аппаратные устройства подписи или аппаратные криптокошельки** представляют собой, как было указано ранее, оборудование для хранения ключей и подписания транзакций с помощью специализированного аппаратного и микропрограммного обеспечения. Обычно они подключаются к десктоп-

ному, мобильному или веб-кошельку через USB-кабель, беспроводной интерфейс (NFC) или камеру для работы с QR-кодами. Поскольку все операции с криптовалютами выполняются исключительно внутри специализированного оборудования, такие кошельки менее уязвимы для различных типов атак.

Стоит отметить, что подавляющая часть блокчейн-сообщества в качестве криптокошельков в основном использует «удобные» решения, основанные на плагинах, интегрируемых в различные браузеры. Криптографические ключи в таких криптокошельках содержатся в криптоконтейнерах, стойкость которых основывается на сложности пароля Пользователя. Кроме того, в момент формирования ЭП для хэш-значения транзакции криптографические ключи считываются в оперативную память среды функционирования в явном или маскированном виде, и, как следствие, могут быть перехвачены хакерскими программами.

В последнее время «медийной» критике также подвергается практика использования изготовленных известными производителями аппаратных и бумажных криптокошельков. Опасения вызывает возможная реализация угроз внутреннего нарушителя на производстве данных устройств и носителей информации, особенно в свете наличия спроса на персональные или учётные данные покупателей, а также предложения таких сведений в даркнете.

В связи с чем предлагается к рассмотрению модель, обладающая удобством использования программного криптокошелька, наряду с безопасностью классического аппаратного криптокошелька на основе USB-токена, но превосходящая его с точки зрения обеспечения анонимности, а также итоговой стоимости приобретения устройства.

Далее подробно рассмотрим вопросы обеспечения безопасности реализации криптокошелька на базе SIM-карты.

Под программным обеспечением (ПО) криптоядра SIM-карты будем понимать специальное программное обеспечение (СПО), предназначенное для исполнения на аппаратном средстве среды функционирования (АС СФ), представленном микросхемной картой (МК).

Под SIM-картой будем понимать МК HUADA CIU98M25 с предустановленным в неё ПО криптоядра.

Основное предназначение криптоядра SIM-карты заключается в обеспечении аутентификации в ядре сети подвижной радиосвязи согласно рекомендации по стандартизации Р 1323565.1.003-2024, а также взаимодействии с различными электронными Сервисами, использующими возможности ЭП Владельцев SIM-карт (например, сервисами электронного документооборота), и устройствами IoT на основе поддерживаемых SIM-картой криптографических функций хэширования, шифрования, имитозащиты, проверки и формирования ЭП.

Программное обеспечение среды функционирования SIM-карты содержит:

1) операционную систему (ОС) оператора сети подвижной радиосвязи (далее — ОСПРС), предоставляющую основной функционал для абонентского терминала;
2) динамическую библиотеку (ДБ) коммерческих организаций, предоставляющую дополнительный функционал, отсутствующий в ОС, для абонентского терминала.

МК, на которой функционирует ПО криптоядра, оснащена 32-разрядным процессором SC000 архитектуры ARM v6-M, который поддерживает два режима работы: привилегированный и непривилегированный.

Привилегированный режим процессора доступен только для ПО криптоядра. ПО СФ (как ОС, так и ДБ) доступен только непривилегированный режим процессора.

ПО криптоядра предоставляет ОС и ДБ ограниченный и управляемый доступ к операциям записи и стирания в энергонезависимой памяти МК.

Для изоляции ресурсов памяти МК, используемых ПО криптоядра, от ПО СФ применяется модуль защиты памяти (memory protect unit, MPU). Более подробно, при

подаче питания (или сигнала сброса) на МК происходит передача управления ОС. Перед передачей управления ПО криптоядра включает MPU и настраивает его таким образом, что ОС не имеет доступа (ни на запись, ни на чтение) к областям памяти (энергонезависимой и оперативной), используемым ПО криптоядра. Также ОС не имеет доступа к областям памяти, используемым ДБ.

При каждом вызове ОС функций ДБ происходит перехват управления и передача его ДБ. После перехвата управления и перед его передачей ПО криптоядра перенастраивает MPU таким образом, что ДБ не имеет доступа (ни на запись, ни на чтение) к областям памяти (энергонезависимой и оперативной), используемым ПО криптоядра. Также ДБ не имеет доступа к областям памяти, используемым ОС.

Поскольку ОС и ДБ выполняются в непривилегированном режиме процессора, они не могут выключить или перенастроить MPU.

Для доступа к аппаратным функциям МК используется специальная область адресного пространства МК, доступная только ПО криптоядра. Изоляция (на чтение и на запись) данной области адресного пространства от ПО СФ также осуществляется при помощи MPU.

Получая управление, ОС или ДБ не имеют доступа (ни на запись, ни на чтение) к специальной области адресного пространства, используемого для управления аппаратными функциями МК. Также они не могут изменить настройки доступа MPU, поскольку выполняются в непривилегированном режиме процессора.

Таким образом, с точки зрения возможности извлечения ключевой информации непредусмотренным разработчиками ДБ способом обеспечивается аналогичный криптоядру уровень безопасности, который соответствует требованиям, предъявляемым к СКЗИ по классу КС3. А с учётом того, что формирование ключевой информации для нужд ДБ будет выполняться криптоядром SIM-карты на основе верифицированных безопасных криптографических алгоритмов с использованием принципа диверсификации источников случайных последовательностей (передача в защищённом виде в криптоядро SIM-карты на этапе её производства и эксплуатации нескольких случайных последовательностей в процессе взаимодействия с независимыми СКЗИ), можно утверждать, что SIM-карта с предустановленной ДБ будет представлять собой доверенное, высоконадёжное и недорогое аппаратное устройство подписи криптокошелька, предназначенное для массового использования.

Более того, разработчики ДБ могут предусмотреть поддержку широкого спектра криптовалют за счёт реализации различных схем ЭП:

- RSA,
- Schnorr,
- ElGamal (включая ГОСТ, ECDSA, KCDSA, EDS, SM2),

использующих вычисления как в кольцах вычетов, так в различных эллиптических кривых (ЭК), например:

- NIST,
- SECP,
- BrainPool.

Кроме того, разработчики ДБ могут предусмотреть поддержку расширенного функционала криптокошельков за счёт реализации правил различных протоколов блокчейн. Например, стандартов:

- Bitcoin Improvement Proposals (BIP-32) [13],
- BIP-39,
- BIP-44 и других.

При этом единственным естественным ограничением для реализации всего вышеперечисленного будет являться только размер flash-памяти, выделяемый в доверенной SIM-карте под нужды ДБ.

Предполагаемые сценарии взаимодействия доверенной SIM-карты и клиента блокчейн существенно зависят от наличия того или иного транспортного канала связи между ними. Например, возможна реализация не слишком удобного для Пользователей решения, связанного с извлечением

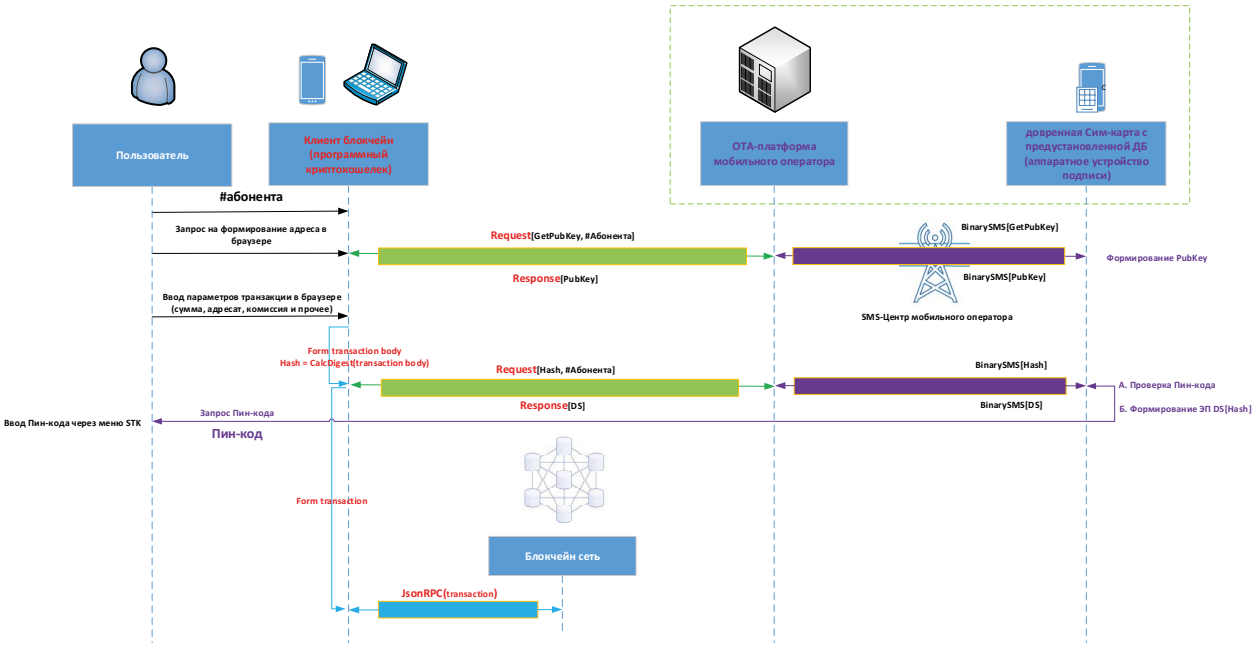


Рис. 1. *Сценарии взаимодействия Владельца доверенной SIM-карты с криптокошельком с использованием ОТА платформы ОСПРС*

доверенной SIM-карты из абонентского терминала и помещением её в специальный считыватель, соединённый с ПК.

Для приёма и передачи команд взаимодействия также возможно использование беспроводных каналов связи. На рис. 1 представлен универсальный сценарий взаимодействия с задействованием инфраструктуры ОСПРС. Универсальность обеспечивается инвариантностью относительно используемой ОС абонентского терминала.

Минимальный функционал, который должна обеспечивать ДБ доверенной SIM-карты:

- формирование и хранение ключей ЭП;
- ответ на запрос получения ключей проверки ЭП;
- ответ на запрос подписания хэш-значения транзакций.

Стоит отметить, что в рамках предложенного сценария обеспечивается только безопасность использования ключей ЭП, но не гарантируется, что Пользователь будет подписывать именно ту самую транзакцию, которая отображается на экране планшета, абонентского терминала или монитора ПК, поскольку за это отвечает выбранный Пользователем программный криптокошелёк, который потенциально может содержать уязвимости либо может использоваться в потенциально небезопасной среде.

Для решения данной проблемы существует возможность усложнения сценария взаимодействия с добавлением следующих участников:

- клиент блокчейн (Сервис) на базе АПК HSM, напрямую взаимодействующий с доверенной SIM-картой и выполняющий доверенное вычисление хэш-значений транзакций;
- специальное устройство с возможностью доверенного ввода и отображения информации (trusted monitor).

Таким образом, конкурентными преимуществами имплементации предложенной модели являются:

- повышение уровня безопасности использования ключей ЭП за счёт защищённого от НСД доверенного компонента SIM-карты;
- выполнение генерации ключей ЭП с использованием встроенных верифицированных безопасных криптографических алгоритмов, реализующих принцип диверсификации источников случайных последовательностей: на ос-

нове передаваемых в защищённом виде в доверенную SIM-карту на этапе её производства и эксплуатации случайных последовательностей в процессе взаимодействия с независимыми СКЗИ класса не ниже КС3.

ЛИТЕРАТУРА

1. Сотниченко Е.А., Ахмед Н.И., Баранова Е.В. Использование блокчейн-технологий в экономическом секторе: потенциал и будущее направление // Прогрессивная экономика. 2025. № 10. С. 299–321. DOI: 10.54861/27131211_2025_10_209.
2. Китанин С.С., Чемерис О.С., Прокопов М.А. Внедрение блокчейн-технологий в финансовом секторе экономики // Экономика, предпринимательство и право. 2025. Т. 15. № 4. С. 2963–2976. DOI: 10.18334/epp.15.4.122927.
3. Фальченко О.Д., Стремоусова Е.Г. Оценка эффективности внедрения технологии блокчейн для оптимизации транспортной логистики // Национальные интересы: приоритеты и безопасность. 2025. № 8 (449). С. 182–203. DOI: 10.24891/mmlieq.
4. Асяева Э.А. Блокчейн-технологии в страховании: перспективы и ограничения // НИР. Экономика фирмы. 2025. Т. 14. № 4. С. 60–64. DOI: 10.12737/2306-627X-2025-14-4-60-64.
5. Андрюшин С.А. Токенизация реальных активов: классификация, платформы, приложения, возможности и проблемы развития // Russian Journal of Economics and Law. 2024. Т. 18. № 1. С. 88–104. DOI: 10.21202/2782-2923.2024.1.88-104.
6. Смоликова Т.М. Блокчейн-революция в играх: формирование новой культуры цифрового взаимодействия // Sciences of Europe. 2024. № 145. С. 21–27. DOI: 10.5281/zenodo.129094601.
7. go-ethereum: Official Go implementation of the Ethereum protocol [Электронный ресурс]. URL: https://geth.ethereum.org
8. Bitcoin Core [Электронный ресурс]. URL: https://bitcoincore.org
9. Web3 в большом бизнесе: тренды, теория и практика [Электронный ресурс]. URL: https://sber.pro/publication/web3-v-bolshom-biznese-trendi-teoriya-i-praktika
10. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. 2008. URL: https://bitcoin.org/bitcoin.pdf
11. MetaMask [Электронный ресурс]. URL: https://metamask.io
12. LEDGER [Электронный ресурс]. URL: https://ledger.com
13. BIPs (Bitcoin Improvement Proposals) [Электронный ресурс]. URL: https://bips.xyz

Secure and Cheap Crypto Wallet Based on a Trusted SIM Card

Andrey Aleksandrovich Igonin — Deputy Head of the Department, IPMCE "Institute of Precision Mechanics and Computer Engineering named after S.A. Lebedev RAS".
E-mail: info@ipmce.ru

The article provides a modern classification of blockchain networks and nodes, as well as blockchain clients that perform the functions of crypto-wallets. The functionality of an elec-tronic signature hardware device based on a trusted SIM card and the possibilities of inte-grating the hardware device with various software crypto-wallets are considered, and the competitive advantages of such a technical solution are listed.

Keywords: blockchain, crypto-wallet, trusted SIM card

REFERENCES

1. Sotnichenko E.A., Akhmed N.I., Baranova E.V. Ispolzovanie blokcheyn-tekhnologiy v ekonomicheskom sektore: potentsial i budushchee napravlenie // Progressivnaya ekonomika. 2025. № 10. S. 299–321. DOI: 10.54861/27131211_2025_10_209 (in Russian).
2. Kitanin S.S., Chemeris O.S., Prokopov M.A. Vnedrenie blokcheyn-tekhnologiy v finansovom sektore ekonomiki // Ekonomika, predprinimatelstvo i pravo. 2025. T. 15. № 4. S. 2963–2976. DOI: 10.18334/epp.15.4.122927. (in Russian)
3. Falchenko O.D., Stremousova E.G. Otsenka effektivnosti vnedreniya tekhnologii blokcheyn dlya optimizatsii transportnoy logistiki // Natsionalnye interesy: prioritety i bezopasnost. 2025. № 8 (449). S. 182–203. DOI: 10.24891/mmlieq (in Russian).
4. Asyaeva E.A. Blokcheyn-tekhnologii v strakhovanii: perspektivy i ogranicheniya // NIR. Ekonomika firmy. 2025. T. 14. № 4. S. 60–64. DOI: 10.12737/2306-627X-2025-14-4-60-64 (in Russian).
5. Andryushin S.A. Tokenizatsiya realnykh aktivov: klassifikatsiya, platformy, prilozheniya, vozmozhnosti i problemy razvitiya // Russian Journal of Economics and Law. 2024. T. 18. № 1. S. 88–104. DOI: 10.21202/2782-2923.2024.1.88-104 (in Russian).
6. Smolikova T.M. Blokcheyn-revolyutsiya v igrakh: formirovanie novoy kultury tsifrovogo vzaimodeystviya // Sciences of Europe. 2024. № 145. S. 21–27. DOI: 10.5281/zenodo.129094601 (in Russian).
7. go-ethereum: Official Go implementation of the Ethereum protocol [Electronic resource]. URL: https://geth.ethereum.org
8. Bitcoin Core [Electronic resource]. URL: https://bitcoincore.org
9. Web3 v bolshom biznese: trendy, teoriya i praktika [Electronic resource]. URL: https://sber.pro/publication/web3-v-bolshom-biznese-trendi-teoriya-i-praktika (in Russian)
10. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. 2008. URL: https://bitcoin.org/bitcoin.pdf
11. MetaMask [Electronic resource]. URL: https://metamask.io
12. LEDGER [Electronic resource]. URL: https://ledger.com
13. BIPs (Bitcoin Improvement Proposals) [Electronic resource]. URL: https://bips.xyz

Image

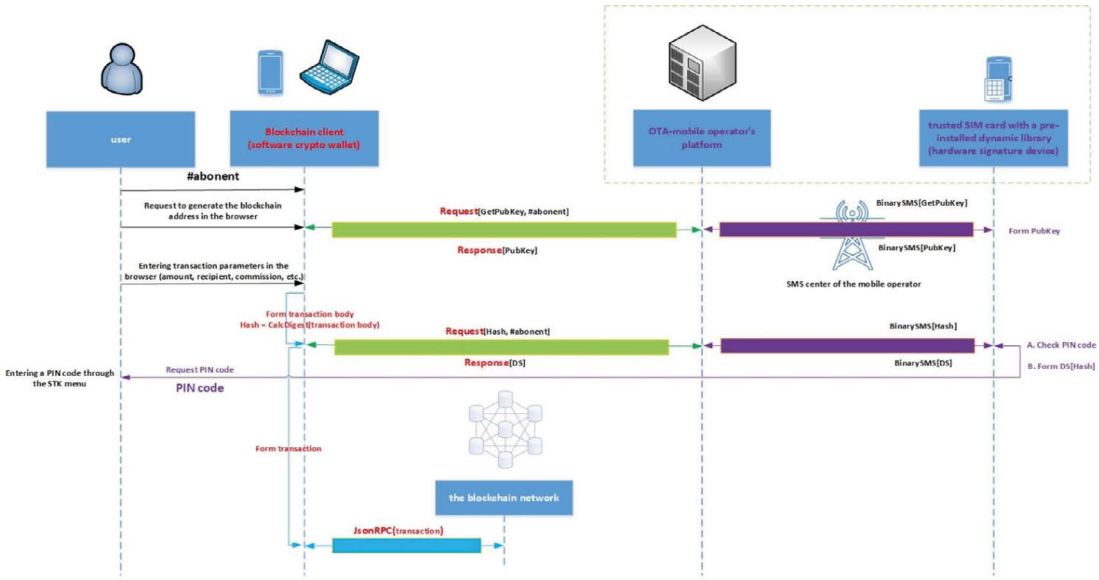


Fig. 1. *Scenarios for the interaction of a trusted SIM-card owner with a crypto wallet using the OTA-mobile operator's platform*

Индекс УДК 336.7:004.8
Код ГРНТИ 06.73.55
DOI: 10.22204/2410-4639-2026-129-01-113-126

Е.В. САМОХОДКИН,
А.А. САМОХОДКИНА*

Доверие к системам искусственного интеллекта как условие цифрового суверенитета в финансовом секторе

В данной работе исследуется доверие к системам искусственного интеллекта в финансовом секторе как условие цифрового суверенитета. Цель исследования состоит в теоретико-аналитическом обосновании того, каким образом доверие формируется на индивидуально-поведенческом и институциональном уровнях и при каких условиях оно становится фактором суверенно ориентированного развития финансовой цифровой среды. Методологическая основа включает социотехнический, институциональный и системный подходы, а также анализ, синтез и сравнительное обобщение научной литературы. Показано, что доверие не сводится ни к пользовательской лояльности, ни к технической эффективности алгоритма; оно возникает на пересечении объяснимости, подотчётности, управления модельным риском, контроля над данными и инфраструктурной автономии. Обосновано, что в условиях непрозрачности и внешних технологических зависимостей доверие приобретает суррогатный характер и не способствует укреплению цифрового суверенитета.

Ключевые слова: искусственный интеллект, доверие к искусственному интеллекту, цифровой суверенитет, финансовый сектор, объяснимый искусственный интеллект, модельный риск, социотехническая инфраструктура

Введение

В последние годы в финансовом секторе фиксируется ускоренная институционализация алгоритмических решений: машинно-обучаемые модели всё чаще встраиваются в кредитование, комплаенс-контуры, антифрод, клиентскую аналитику, инвестиционное консультирование, вследствие чего доверие к данным системам начинает функционировать как

* **Самоходкин Евгений Вячеславович** — аспирант кафедры социологии, психологии управления и истории, ФГБОУ ВО «Государственный университет управления».
E-mail: rodentforme@gmail.com
Самоходкина Алиса Андреевна — аспирант кафедры социологии, психологии управления и истории ФГБОУ ВО «Государственный университет управления».
E-mail: alisaelzon@gmail.com

предпосылка легитимного использования, устойчивого масштабирования, общественного принятия в условиях растущего общественного и научного интереса к искусственному интеллекту (ИИ) [1, 2]. При этом в междисциплинарной литературе доверие к ИИ трактуется как готовность субъектов полагаться на выводы системы, делегируя часть когнитивной работы и принимая связанные риски, что в финансовой сфере приобретает повышенную остроту из-за высокой цены ошибок, асимметрии информации, потенциальных каскадных эффектов на уровне рынков [3]. В российских исследованиях влияние ИИ на финансовый сектор также описывается как амбивалентное: одновременно расширяется инструментальный потенциал управления рисками и усиливается уязвимость к новым классам технологических, правовых, этических неопределённостей, влияющих на доверительный контур взаимодействия «клиент — организация — регулятор» [4, 5].

Данная проблематика встраивается в более широкую рамку цифрового суверенитета, поскольку финансовая инфраструктура, будучи критической для экономической безопасности, оказывается зависимой от данных, вычислительных мощностей, программных стеков, облачных архитектур, поставщиков моделей, режимов трансграничной передачи информации, а значит — от внешних правил, стандартов, юрисдикций, технологических траекторий [6]. В зарубежной политэкономической и правовой аналитике цифровой суверенитет описывается как стремление к восстановлению контроля над цифровым пространством через регуляторные, инфраструктурные и институциональные механизмы, при этом ключевым объектом такого контроля становится именно способность управлять цифровыми зависимостями и их рисковым профилем [7]. В отечественной научной дискуссии цифровой суверенитет, как правило, связывается с контролем над данными, цифровыми технологиями и инфраструктурой, а также с задачей минимизации внешней технологической зависимости, что для финансового сектора означает необходимость согласования инноваций с требованиями безопасности и правовой определённости [8].

Внутри данной рамки доверие к системам ИИ выступает необходимой предпосылкой суверенизации: когда решения модели не поддаются верификации, а причины вывода остаются непрозрачными, контроль подменяется верой в корректность поставщика или в «самоочевидность» результата, что противоречит логике суверенного управления критическими цифровыми активами [9, 10]. Исследования по финансовой объяснимости показывают, что даже при наличии высоких показателей точности дефицит интерпретируемости порождает регуляторное напряжение, снижает организационную готовность к внедрению, осложняет внутренние процедуры аудита и постфактум-разбирательств по спорным кейсам [11, 12]. В прикладной финансовой литературе объяснимый ИИ (XAI, eXplainable Artificial Intelligence — совокупность моделей, процедур и инструментов, с помощью которых обеспечивается интерпретируемое представление результата работы системы) описывается не только как набор методов интерпретации, но и как средство обоснования решения, позволяющее снижать доверительный разрыв между алгоритмической рациональностью и институциональной ответственностью финансовой организации [13]. В российских работах по объяснимости кредитного скоринга акцентируется, что прозрачность модели рассматривается как функциональное требование, поскольку устойчивость и интерпретируемость напрямую связаны с возможностью обоснования кредитных решений и снижением конфликтности взаимодействия с клиентом [14].

Даже при достижении приемлемой объяснимости сохраняется слой управленческой проблематики, связанный с управлением модельным риском: машинно-обучаемые методы, будучи более гибкими и часто более точными, создают новые

формы неопределённости для валидации, мониторинга, сопоставления качества модели и связанных с риском издержек, что в финансовых организациях трансформирует традиционные контуры управления модельным риском (model risk management) [15, 16]. В систематических обзорах подчёркивается, что расширение применения машинного обучения в управлении банковскими рисками сопровождается ростом сложности моделей, повышением требований к данным, появлением уязвимостей, связанных с переносимостью результатов и корректностью обобщения, вследствие чего доверие становится зависимым от зрелости процедур контроля жизненного цикла модели [17]. Дополнительно в исследованиях финансового риск-менеджмента указывается, что практики алгоритмического аудита и объяснимости рассматриваются как инфраструктурные компоненты «доверенной» финансовой аналитики, а не как факультативные меры коммуникации [18]. В российской академической периодике риски внедрения ИИ в банковском секторе также связываются с недостаточной прозрачностью решений и с организационными ограничениями контроля, что усиливает разрыв между технологическим внедрением и институциональным доверием [19].

В итоге проблематика доверия к системам ИИ в финансовом секторе может быть описана как многослойная: техническая объяснимость, модельный риск, справедливость и недискриминация, организационная подотчётность, управляемость данных, суверенность инфраструктуры — данные пласты взаимно усиливают друг друга, формируя эффект критического ограничения, при котором провал в одном измерении обесценивает усилия в других. Следовательно, в рамках данной работы проблематика темы задаётся не вопросом «доверять или не доверять» ИИ как технологии, а вопросом о том, каким образом доверие конструируется как проверяемое, институционально закреплённое свойство социотехнической системы, обеспечивая цифровой суверенитет финансового сектора в условиях ускоренной алгоритмизации.

Методология исследования

Методология исследования носит междисциплинарный характер и основана на сочетании социотехнического, институционального и системного подходов, что позволяет рассматривать доверие к системам ИИ в финансовом секторе одновременно как поведенческий, организационный и инфраструктурный феномен. В качестве основных методов используются анализ и синтез научной литературы, сравнительный анализ российских и зарубежных исследований, а также концептуальное обобщение, направленное на выявление взаимосвязи между объяснимостью, подотчётностью, управлением модельным риском, контролем над данными и цифровым суверенитетом.

Объектом исследования выступают общественные отношения, организационные практики и инфраструктурные процессы, складывающиеся в ходе внедрения и использования систем ИИ в финансовом секторе в условиях цифровой трансформации. Предметом исследования являются механизмы формирования доверия к системам ИИ как к индивидуально воспринимаемому и институционально обеспечиваемому свойству социотехнической инфраструктуры финансового сектора, а также связь данных механизмов с обеспечением цифрового суверенитета.

Цель исследования состоит в теоретико-аналитическом обосновании того, каким образом доверие к системам ИИ в финансовом секторе формируется на поведенческом и институциональном уровнях и при каких условиях данное доверие становится фактором укрепления цифрового суверенитета.

Ограничения исследования могут быть сформулированы следующим образом:

1. Данная работа носит теоретико-аналитический характер и не включает самостоятельную эмпирическую проверку выдвигаемых положений на материале опросов, интервью, кейс-стади

либо экспериментальных данных. Вследствие данного обстоятельства выводы ориентированы прежде всего на концептуальное обобщение и интерпретацию научной литературы.

2. Исследование ограничено финансовым сектором, поскольку именно в данной сфере доверие к ИИ приобретает особую значимость вследствие высокой цены ошибки, чувствительности данных, регуляторной плотности и системной значимости цифровой инфраструктуры. Соответственно, полученные выводы не претендуют на автоматическое распространение на иные отрасли без дополнительной адаптации.
3. Источниковая база ограничена академическими статьями, научными публикациями и исследовательскими работами, тогда как отраслевые отчёты, консалтинговые обзоры, корпоративные документы и иные непроверенные по академическим стандартам материалы в исследовательскую рамку не включаются. Данное ограничение повышает научную строгость, однако одновременно сужает спектр прикладных наблюдений.

Методологическая рамка данной работы выстроена таким образом, чтобы обеспечить согласованное рассмотрение доверия к ИИ в финансовом секторе сразу в нескольких взаимосвязанных плоскостях — поведенческой, институциональной, инфраструктурной и суверенной.

Доверие как индивидуально-поведенческая готовность к принятию решений, сгенерированных искусственным интеллектом

Доверие на данном уровне целесообразно интерпретировать как готовность субъекта допустить алгоритм в контур собственного выбора, признать его рекомендации релевантными и, в предельном случае, скорректировать под них финансовое поведение. Данная трактовка подтверждается банковской эмпирикой: в исследовании принятия ИИ в банковских сервисах отношение к технологии оказалось наиболее сильным непосредственным предиктором намерения использования ($\beta = 0.574$), тогда как воспринимаемое доверие сохранило самостоятельное положительное влияние на поведенческое намерение ($\beta = 0.135$) [20]. В исследованиях robo-advisory (цифровой сервис, который с опорой на алгоритмы и/или модели машинного обучения формирует персонализированные финансовые рекомендации) сходная логика воспроизводится на иной выборке: начальный уровень доверия формируется не только ожидаемой функциональной полезностью, но и предрасположенностью к доверию, воспринимаемой способностью системы оправдать ожидания, социальным влиянием, организационной поддержкой и ценностным восприятием сервиса, тогда как цифровая неграмотность и сложность финтех-решений способны ослаблять доверительный импульс уже на входе [21]. Отсюда следует, что индивидуальная готовность принимать решения, сгенерированные ИИ, обусловливается не одной лишь точностью алгоритма; она возникает в точке пересечения технологических характеристик, пользовательской компетентности и институционального контекста, в котором цифровой выбор воспринимается как допустимый и безопасный.

При этом доверие в финансовой среде носит неоднородный характер, поскольку включает когнитивный, аффективный и социальный компоненты, по-разному влияющие на согласие с машинной рекомендацией. В исследовании сектора BFSI (Banking, Financial Services and Insurance — банковский, финансовый и страховой сектор) было показано, что намерение использовать ИИ как средство поддержки решения определяется аффективным и когнитивным доверием, тогда как делегирование решения цифровому агенту требует дополнительно социального доверия, то есть признания допустимости самой формы алгоритмического посредничества [22]. Экспериментальные исследования финансового консультирования демонстрируют

ещё более существенную деталь: пользователи чаще следуют совету романтического партнёра, чем автономного ИИ-советника, а связь между источником совета и готовностью ему следовать опосредуется одновременно когнитивным и аффективным доверием, причём последнее действует сильнее; вместе с тем антропоморфизация robo-advisor и гибридная схема «человек с ИИ-поддержкой» заметно снижают выраженность AI aversion (алгоритмическая неприязнь / избегание ИИ — это наблюдаемая в экспериментах и полевых исследованиях тенденция реже следовать рекомендациям алгоритма или отказываться от делегирования, особенно после обнаружения ошибки или при наличии риска, даже когда объективно алгоритм в среднем не хуже человека) [23]. Аналитически данное обстоятельство принципиально важно для темы цифрового суверенитета: если готовность принять ИИ-решение возрастает за счёт реляционного оформления интерфейса и эмоционального смягчения восприятия, то доверие начинает опираться не столько на проверяемость и контроль, сколько на поведенческую архитектуру убеждения, а значит, может быть институционально хрупким и манипулятивно уязвимым.

Доверие к ИИ в финансах не является статическим состоянием; оно развивается во времени, переживает фазы усиления, шока и частичного восстановления. В динамическом исследовании взаимодействия человека с ИИ-финансовым консультантом было установлено, что пользователи первоначально демонстрируют algorithmic appreciation (алгоритмическое предпочтение — эмпирически фиксируемая тенденция пользователей придавать рекомендациям/оценкам алгоритма больший вес, чем сопоставимым рекомендациям человека), однако единичная ошибка вызывает существенное падение доверия ($\eta^2 = 0.141$), после чего качественно выстроенные объяснения способны не только восстановить, но и усилить доверительный уровень по сравнению с исходной точкой; дополнительно было показано, что финансовая грамотность усиливает чувствительность к ошибке и одновременно повышает способность к восстановлению доверия после объяснения [24]. Следовательно, индивидуально-поведенческое доверие не тождественно максимальной готовности делегировать выбор машине; напротив, оно ближе к калиброванной готовности, в которой сохраняется способность к критической дистанции, а данная способность непосредственно соотносится с автономией субъекта — одной из фундаментальных предпосылок цифрового суверенитета.

При этом авторы исходят из того, что методологически недостаточно рассматривать доверие к системам ИИ лишь как следствие эмоциональной приемлемости интерфейса либо пользовательской привычки к взаимодействию с цифровым сервисом. Подобная редукция чрезмерно упрощает сам предмет анализа, поскольку в финансовом секторе доверие формируется не на уровне поверхностного впечатления от удобства, а в пространстве более сложной оценки — насколько алгоритмическое решение является понятным, насколько оно поддаётся интерпретации, в какой мере сохраняется возможность соотнести его логику с характером конкретной финансовой ситуации. Именно поэтому доверие к ИИ должно рассматриваться не как эмоциональная реакция на технологическую новизну, а как результат осмысленного соотнесения функциональной эффективности, прозрачности, безопасности и пределов допустимой алгоритмической автономии.

В данной связи особую значимость приобретает вопрос объяснимости. Если пользователь сталкивается с решением, логика которого для него принципиально закрыта, доверие оказывается лишённым когнитивного основания и начинает опираться либо на вынужденное принятие, либо на репутационный капитал организации, либо на инерцию цифрового поведения. Однако подобная конфигурация является внутренне неустойчивой, поскольку в ситуации финансового риска одного символического авторитета недостаточно. Для

того чтобы готовность принять решение, сгенерированное ИИ, приобрела устойчивый характер, требуется не абстрактная прозрачность как декларация, а содержательная объяснимость, позволяющая понять, почему система пришла именно к данному выводу, где пролегают границы применимости рекомендации, каким образом учитывается персональный риск-профиль и в какой степени пользователь сохраняет возможность влиять на дальнейшую траекторию решения.

Вместе с тем и сама объяснимость не должна мыслиться упрощённо. Формальное раскрытие участия ИИ в принятии решения ещё не гарантирует усиления доверия. Напротив, подобное раскрытие может производить обратный эффект, если оно не сопровождается понятной для пользователя интерпретацией смысла алгоритмической обработки. Иначе говоря, доверие подрывается не столько самим фактом участия ИИ, сколько отсутствием ясности относительно его роли, компетенции и ограничений. Отсюда вытекает важное аналитическое следствие: для индивидуально-поведенческой готовности принципиально значима такая форма раскрытия, при которой снимается неопределённость относительно оснований решения, условий использования данных и возможностей оспаривания результата.

Данное обстоятельство позволяет перейти к более широкому пониманию доверия как многосоставной конструкции. В финансовом секторе пользователь фактически имеет дело не с изолированным алгоритмом, а с комплексной социотехнической конфигурацией, включающей данные, модель, интерфейс, процедуры верификации, нормативные ограничения, внутренний контроль, механизмы ответственности. Поэтому доверие к ИИ не исчерпывается убеждённостью в математической корректности модели. Оно включает доверие к качеству исходных данных, к корректности их обработки, к устойчивости алгоритма за пределами обучающей выборки, к способности организации выявлять ошибки, к наличию институциональных фильтров, не допускающих произвольной цифровой власти над пользователем. В данном смысле объяснимость выступает существенным, но не единственным элементом доверительной архитектуры.

Логика дальнейшего рассуждения подводит к необходимости учёта человекоориентированного измерения. Индивидуальная готовность принять решение, сгенерированное ИИ, возникает, как представляется, не в условиях полной замены субъекта машиной, а там, где сохраняется представление о контролируемости цифрового инструмента. Когда алгоритм встроен в контур, допускающий проверку, корректировку, человеческое вмешательство и институциональную ответственность, доверие приобретает более рациональную и, следовательно, более устойчивую форму. Если же система воспринимается как автономный и недоступный пересмотру механизм, пользовательская готовность к принятию её рекомендаций становится либо вынужденной, либо ситуативной, либо основанной на неосведомлённости. Для финансовой сферы, где цена ошибки может быть значительной, подобная зависимость имеет принципиальное значение.

Именно на данном уровне проблематика доверия начинает непосредственно сопрягаться с цифровым суверенитетом. Поведенческое доверие пользователя не возникает в нормативном вакууме — оно является производным от того, каким образом организован контроль над данными, инфраструктурой и цифровыми посредниками. Если данные циркулируют по непрозрачным маршрутам, если вычислительная логика решения вынесена за пределы доступного контроля, если критически значимые компоненты финансовой цифровой среды зависят от внешних поставщиков и закрытых технологических стеков, доверие теряет суверенное основание. В таком случае пользователь может демонстрировать внешнюю готовность следовать алгоритмическому выводу, однако данная готовность будет опираться не на институционально обеспеченную

уверенность, а на структурную асимметрию — на невозможность проверить, понять и оспорить решение.

Следовательно, в контексте цифрового суверенитета доверие должно интерпретироваться как переживаемое пользователем выражение более глубокой архитектурной упорядоченности. Безопасность, понятность, оспоримость, контролируемость, ограниченность алгоритмической автономии — данные свойства приобретают не только прикладное, но и суверенное значение. Чем выше способность финансовой системы гарантировать субъекту доступное понимание принципов работы ИИ, защиту данных, процедурную справедливость и наличие реальных каналов пересмотра решения, тем в большей степени индивидуально-поведенческое доверие перестаёт быть психологической случайностью и превращается в социально и институционально обоснованную готовность к использованию алгоритмических инструментов.

При данном подходе становится очевидным, что доверие к решениям, сгенерированным ИИ, не может быть понято как спонтанная лояльность цифровой инновации. Оно складывается в результате сложной калибровки между воспринимаемой компетентностью системы, качеством объяснений, режимом обращения с данными, степенью человеческого контроля и субъективной способностью пользователя удерживать автономную позицию в ситуации алгоритмического воздействия. Чем в большей мере пользователь понимает, кто контролирует данные, каким образом проверяется модель, где проходят границы автоматизации и каким способом может быть оспорен результат, тем выше вероятность формирования доверия, совместимого с логикой цифрового суверенитета.

Таким образом, индивидуально-поведенческая готовность к принятию решений, сгенерированных ИИ, должна рассматриваться не как частный поведенческий эффект цифровизации, а как стратегически значимый индикатор состояния финансовой цифровой среды. Там, где доверие опирается на содержательную объяснимость, институциональную подотчётность и контролируемость инфраструктуры, оно способствует укреплению суверенной модели развития. Там же, где оно формируется на основе непрозрачности, интерфейсного удобства и скрытых цифровых зависимостей, возникает лишь видимость доверия, лишённая устойчивого нормативного и технологического основания.

Доверие как институционально обеспеченное свойство социотехнической инфраструктуры

В рамках анализа доверия к системам ИИ в финансовом секторе продуктивным представляется смещение оптики с индивидуального восприятия на институциональную среду, поскольку в высокорисковых цифровых контурах доверие формируется не столько в сознании пользователя, сколько в архитектуре проверки, подотчётности и управляемости алгоритмического решения. В российской академической дискуссии данная логика выражена предельно отчётливо: доверие к ИИ связывается с качеством знаний и данных, границами применимости модели, процедурами валидации и верификации, объяснимостью вывода и ролью человека в принятии окончательного решения, вследствие чего доверенным может считаться лишь такой ИИ, который является подотчётным, надёжным и объяснимым [25].

Данная постановка особенно значима для финансового сектора, где алгоритмическая система включается не в нейтральную информационную среду, а в инфраструктуру распределения доступа к капиталу, оценки кредитоспособности, обнаружения мошенничества и управления рисками. Поэтому институциональное доверие не может выводиться из одной лишь предиктивной эффективности: обзор объяснимого ИИ в финансовой сфере показывает, что в финансовой сфере доверительность решений непосредственно увязывается с прозрачностью, способностью интерпретировать ошибки, подот-

чётностью и корректным выбором объяснительных инструментов, причём сами объяснения подлежат оценке по критериям правдоподобия и добросовестности, иначе возрастает риск ложной уверенности в корректности модели [11]. В той же логике показывается, что внедрение машинного обучения в кредитный скоринг действительно повышает прогностическую результативность, однако одновременно производит новые формы модельного риска, прежде всего в плоскости надзорной валидации, технологической прозрачности и проверяемости модели, а неопределённость относительно того, каким образом данные риски будут оцениваться регулятором, уже сама по себе способна тормозить инновацию [16]. Из данного обстоятельства следует принципиальный вывод: доверие к ИИ в финансах возникает там, где организация способна доказуемо показать, почему ему можно доверять, где проходят пределы его применимости и каким образом устраняются институциональные последствия ошибки.

Вместе с тем доверие как свойство социотехнической инфраструктуры не исчерпывается внутренними процедурами банка либо финтех-платформы, поскольку в высокорисковых контурах оно носит распределённый характер. В исследовании, посвящённом управлению высокорисковыми системами ИИ, выполненном на материале здравоохранения и кредитного скоринга, подчёркивается, что кредитный скоринг представляет собой сеть взаимодействующих акторов — финансовых организаций, кредитных бюро, разработчиков, регуляторов и пользователей, вследствие чего формирование доверия не может быть локализовано в одной точке; на уровне поставщика решения оно требует тестирования, валидации, постоянного мониторинга, прозрачности и механизмов оспаривания решений, на институциональном уровне — доверия к регулирующим органам и установленным ими стандартам, на общественном уровне — уверенности в справедливости цифрового порядка в целом [26]. Более того, в данной работе специально подчёркивается, что пользователи должны быть способны адекватно оценивать степень надёжности и допустимые пределы доверия к ИИ-системам, иначе формируются режимы избыточного доверия или недостаточного доверия, в равной мере деструктивные для высокорисковых сфер. Следовательно, институционально обеспеченное доверие предполагает не просто наличие регуляции, а наличие такой регуляции и такой организационной практики, которые делают доверительные свойства системы наблюдаемыми, проверяемыми и поддающимися калибровке для всех участников инфраструктуры.

С позиций цифрового суверенитета данная проблематика углубляется, поскольку институциональное доверие к ИИ оказывается неотделимым от контроля над данными, цифровой инфраструктурой и внешними технологическими зависимостями. В российской научной литературе цифровой суверенитет определяется через способность государства контролировать собственные цифровые данные, информацию, технологии и инфраструктуру, обеспечивая безопасность, конфиденциальность, киберустойчивость и относительную независимость от внешних поставщиков, причём в структуру цифрового пространства прямо включаются данные, информационные системы, сети, инфраструктура, нормы регулирования и механизмы управления [8]. В результате доверие к ИИ-системе в финансовом секторе не может быть признано институционально зрелым, если критически важные контуры хранения, обработки и интерпретации данных вынесены в непрозрачные внешние юрисдикции, а внутренний субъект управления не обладает полнотой контроля над жизненным циклом модели.

Зарубежные исследования суверенитета финансовых данных подтверждают данную логику уже на уровне систематического обзора. В работе, выполненной по протоколу PRISMA на материале 52 исследований, показано, что страны и регио-

ны существенно расходятся в подходах к регулированию ИИ и обеспечению суверенитета финансовых данных; при этом из 13 выявленных методов обеспечения суверенитета данных лишь 5 прямо адресуют вопросы безопасности, хотя именно безопасность признаётся наиболее значимым компонентом. Одновременно подчёркивается необходимость формирования устойчивой и согласованной нормативно-правовой рамки, способной совместить доверие, защиту частной жизни и автономию данных в финансовом секторе [27]. Там же фиксируется, что возрастающая опора финансовых систем на цифровые процессы усиливает риски, связанные с защитой частной жизни, регуляторной согласованностью, алгоритмическими смещениями, отравлением данных и состязательными атаками, вследствие чего без надлежащего надзора и защитных рамок ИИ в финансах способен подрывать доверие, справедливость и соблюдение законодательства о суверенитете данных. В аналитическом плане это означает следующее: цифровой суверенитет не является внешним политико-правовым фоном для доверия к ИИ; напротив, он выступает его инфраструктурной предпосылкой, поскольку именно контроль над данными и платформами делает возможными подлинную проверку модели, эффективный аудит и реальную подотчётность.

Тем самым доверие как институционально обеспеченное свойство социотехнической инфраструктуры должно пониматься как результат согласованного действия нескольких взаимосвязанных контуров: верифицируемости модели, прозрачности её поведения, распределения ответственности между участниками, наличия процедур обжалования, устойчивости цифровой инфраструктуры и суверенного контроля над данными. В логике цифрового суверенитета доверие приобретает качество стратегического критерия: если финансовая организация и регулирующая среда способны не только использовать ИИ, но и управлять его рисками, контролировать инфраструктурные зависимости, локализовать ответственность и обеспечивать автономию данных, тогда доверие становится институциональным ресурсом суверенного развития; если же алгоритмическая система встроена в непрозрачные, внешне управляемые и слабо оспоримые контуры, тогда речь идёт не о доверии в строгом смысле, а о вынужденной зависимости, маскируемой под цифровую эффективность.

Заключение

Проведённое исследование позволило установить, что доверие к системам ИИ в финансовом секторе не может быть сведено ни к субъективной расположенности пользователя к цифровым сервисам, ни к формальному соответствию алгоритма заданным техническим параметрам. В рамках данной работы было показано, что доверие представляет собой многослойную и институционально опосредованную конструкцию, формирующуюся на пересечении индивидуального восприятия, организационных механизмов контроля, нормативной архитектуры, качества данных и инфраструктурной автономии. Вследствие данного обстоятельства доверие следует интерпретировать не как внешнее сопровождение цифровой трансформации, а как одно из её базовых условий, от которого зависит возможность легитимного, устойчивого и суверенно ориентированного внедрения ИИ в финансовые процессы.

В ходе анализа было выявлено, что на индивидуально-поведенческом уровне доверие выражается в готовности субъекта принять алгоритмически сгенерированное решение в контур собственного выбора, однако данная готовность не является простой реакцией на удобство интерфейса либо на технологическую новизну. Напротив, она определяется более сложной конфигурацией факторов, включающей воспринимаемую компетентность системы, содержательную объяснимость, понятность границ применимости модели, защищённость данных, возможность сохранения

человеческого контроля и процедурную оспоримость результата. Тем самым было обосновано, что доверие к ИИ в финансовой сфере должно рассматриваться как калиброванная готовность к взаимодействию с алгоритмической системой, а не как безусловное делегирование ей решения. Данная калибровка особенно значима в условиях цифрового суверенитета, поскольку именно она позволяет сохранить субъектную автономию в ситуации возрастающей алгоритмизации финансового поведения.

Одновременно было показано, что ограничение анализа только поведенческим измерением доверия является методологически недостаточным. Доверие в высокорисковых цифровых контурах возникает и воспроизводится в границах социотехнической инфраструктуры, где решающую роль начинают играть процедуры валидации и верификации моделей, качество управления модельным риском, прозрачность логики вывода, распределение ответственности между участниками, механизмы надзора, обжалования и аудита. При данном подходе доверие предстаёт как институционально обеспеченное свойство системы, а его наличие определяется не декларацией надёжности, а способностью финансовой организации и регулирующей среды доказуемо подтверждать корректность, подотчётность и управляемость алгоритмического решения. Из данного вывода следует, что доверие не может быть признано устойчивым, если оно не поддержано зрелыми организационными и правовыми механизмами контроля.

Особое значение в рамках проведённого исследования приобрела связка доверия и цифрового суверенитета. Было установлено, что доверие к ИИ в финансовом секторе утрачивает устойчивое основание в тех случаях, когда критически значимые контуры хранения, обработки и интерпретации данных оказываются вынесенными в непрозрачные внешние юрисдикции, когда жизненный цикл модели не поддаётся полноценному внутреннему контролю, а инфраструктурные зависимости маскируются под технологическую эффективность. Следовательно, цифровой суверенитет должен рассматриваться не как внешний политико-правовой фон, а как инфраструктурная предпосылка доверия. Именно контроль над данными, вычислительными ресурсами, цифровыми платформами, регуляторными рамками и процедурами ответственности создаёт условия, при которых доверие становится не иллюзией надёжности, а подтверждаемым свойством финансовой цифровой среды.

В результате было обосновано, что доверие к системам ИИ в финансовом секторе имеет двойственную природу. С одной стороны, оно проявляется как индивидуально-поведенческая готовность субъекта признать алгоритмическую рекомендацию допустимой и значимой для собственного выбора. С другой стороны, оно формируется как институционально закреплённое качество социотехнической инфраструктуры, обеспечиваемое прозрачностью, подотчётностью, управляемостью рисков, процедурной справедливостью и суверенным контролем над данными и технологическими зависимостями. Данные измерения не противостоят друг другу, а образуют единую конструкцию: без институциональной обеспеченности поведенческое доверие становится хрупким и манипулятивно уязвимым, тогда как без пользовательской готовности даже наиболее развитая инфраструктура не приобретает полноценной социальной легитимности.

Тем самым основная исследовательская идея получает подтверждение: в условиях ускоренной алгоритмизации финансового сектора доверие к ИИ должно пониматься как проверяемое, институционально сконструированное и нормативно насыщенное свойство цифровой среды, выступающее необходимым условием цифрового суверенитета. Чем выше степень объяснимости, подотчётности, контролируемости и инфраструктурной автономии финансовых ИИ-систем, тем более вероятным становится формирование доверия, совместимого с задачами устойчивого и безопасного разви-

тия. И наоборот, там, где алгоритмические решения встроены в непрозрачные, внешне зависимые и слабо оспоримые контуры, возникает не доверие в строгом смысле, а лишь его функциональный суррогат, не укрепляющий, а размывающий суверенные основания финансовой цифровизации.

Итак, по итогам проведённой работы представляется возможным заключить, что доверие к системам ИИ в финансовом секторе должно рассматриваться как стратегический ресурс, от состояния которого зависит не только эффективность конкретных цифровых решений, но и способность финансовой системы сохранять управляемость, автономию и институциональную устойчивость в условиях технологической трансформации. Именно в данной плоскости доверие перестаёт быть вторичным социально-психологическим эффектом и превращается в одну из центральных категорий анализа цифрового суверенитета.

ЛИТЕРАТУРА

1. Ridzuan N.N., Masri M., Anshari M., Fitriyani N.L., Syafrudin M. AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility // Information. 2024. Vol. 15, No. 8. Art. 432. DOI: 10.3390/info15080432.
2. Samokhodkin E.V., Elzon A.A. Analysis of the Relationship Between Scientific Interest and Publication Dynamics on Artificial Intelligence in the Russian Federation (2020–2024) // Scientific and Technical Information Processing. 2025. Vol. 52, No. 2. P. 152. DOI: 10.3103/S0147688225700182.
3. Afroogh S., Akbari A., Malone E., Kargar M., Alambeigi H. Trust in AI: Progress, Challenges, and Future Directions // Humanit. Soc. Sci. Commun. 2024. Vol. 11. Art. 1568. DOI: 10.1057/s41599-024-04044-8.
4. Samokhodkin E.V., Elzon A.A. Social Threats of Artificial Intelligence: Classification and Risk Assessment // Scientific and Technical Information Processing. 2025. Vol. 52, No. 3. P. 263. DOI: 10.3103/S0147688225700674.
5. Кузин М. А. Оценка влияния развития искусственного интеллекта на финансовый сектор экономики // Вестник евразийской науки. 2023. Т. 15, № s4. Art. 31FAVN423.
6. Rodriguez Pita P., Perez-Martinez J., Urueña López A. From Concept to Method: A Framework for Measuring Digital Sovereignty // SSRN. 2025. DOI: 10.2139/ssrn.5683701.
7. Farrand B., Farrand Carrapico H. Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity // European Security. 2022. Vol. 31, No. 3. P. 435. DOI: 10.1080/09662839.2022.2102896.
8. Авдийский В.И., Иванов А.В., Царегородцев А.В. Взаимосвязь цифрового суверенитета и цифрового пространства: новые вызовы и перспективы // Вестник евразийской науки. 2024. Т. 16, № s3. Art. 21FAVN324.
9. Balasubramaniam N., Kauppinen M., Rannisto A., Hiekkanen K., Kujala S. Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements // Information and Software Technology. 2023. Vol. 159. Art. 107197. DOI: 10.1016/j.infsof.2023.107197.
10. Timokhovich A.N., Samokhodkin E.V., Elzon A.A. Classification of Epistemological Threats Posed by Artificial Intelligence // Scientific and Technical Information Processing. 2025. Vol. 52, No. 4. P. 318. DOI: 10.3103/S0147688225700741.
11. Yeo W.J., Van Der Heever W., Mao R., Cambria E., Satapathy R., Mengaldo G. A Comprehensive Review on Financial Explainable AI // Artif. Intell. Rev. 2025. Vol. 58. Art. 189. DOI: 10.1007/s10462-024-11077-7.
12. Кантаев Н.К. Перспективы использования методов машинного обучения для оценки кредитных рисков // Вестник евразийской науки. 2025. Т. 17, № s2. Art. 70FAVN225.
13. Weber P., Carl K. V., Hinz O. Applications of Explainable Artificial Intelligence in Finance — a Systematic Review of Finance, Information Systems, and Computer Science Literature // Manag. Rev. Q. 2024. Vol. 74, No. 2. P. 867. DOI: 10.1007/s11301-023-00320-0.
14. Якубин А. Я. Искусственный интеллект в кредитном скоринге: разработка, обучение и применение модели // Молодой учёный. 2025. № 19 (570). С. 33-35.

15. Самоходкин Е. В., Эльзон А. А. Подходы к формализации нормативного поведения автономных интеллектуальных агентов // Искусственный интеллект и принятие решений. 2025. № 4. С. 35. DOI: 10.14357/20718594250403.
16. Alonso Robisco A., Carbó Martínez J. M. Measuring the Model Risk-Adjusted Performance of Machine Learning Algorithms in Credit Default Prediction // Financial Innovation. 2022. Vol. 8. Art. 70. DOI: 10.1186/s40854-022-00366-1.
17. Heß V.L., Damásio B. Machine Learning in Banking Risk Management: Mapping a Decade of Evolution // International Journal of Information Management Data Insights. 2025. Vol. 5, No. 1. Art. 100324. DOI: 10.1016/j.jjimei.2025.100324.
18. Fritz-Morgenthal S., Hein B., Papenbrock J. Financial Risk Management and Explainable, Trustworthy, Responsible AI // Front. Artif. Intell. 2022. Vol. 5. Art. 779799. DOI: 10.3389/frai.2022.779799.
19. Гозгешев Э.А. Искусственный интеллект в банковском секторе: возможности и риски // Вестник евразийской науки. 2024. Т. 16, № s6. Art. 49FAVN624.
20. Byambaa O., Yondon C., Rentsen E., Darkhijav B., Rahman M. An Empirical Examination of the Adoption of Artificial Intelligence in Banking Services: the Case of Mongolia // Futur. Bus. J. 2025. Vol. 11, No. 1. Art. 76. DOI: 10.1186/s43093-025-00504-y.
21. Bashir Z., Farooq S., Iqbal M.S., Aamir M. The Role of Trust in Financial Robo-Advisory Adoption: A Case of Young Retail Investors in Pakistan // Sustainable Futures. 2025. Vol. 9. Art. 100538. DOI: 10.1016/j.sftr.2025.100538.
22. Pathak A., Bansal V. AI as Decision Aid or Delegated Agent: The Effects of Trust Dimensions on the Adoption of AI Digital Agents // Computers in Human Behavior: Artificial Humans. 2024. Vol. 2, No. 2. Art. 100094. DOI: 10.1016/j.chbah.2024.100094.
23. Hermann E., Alberhasky M. The Trusted Partner for Financial Decision Making: Romantic Partner or AI? // Computers in Human Behavior. 2026. Vol. 177. Art. 108877. DOI: 10.1016/j.chb.2025.108877.
24. Han J., Ko D. Trust Formation, Error Impact, and Repair in Human-AI Financial Advisory: A Dynamic Behavioral Analysis // Behav. Sci. 2025. Vol. 15, No. 10. Art. 1370. DOI: 10.3390/bs15101370.
25. Кобринский Б.А. Доверие к технологиям искусственного интеллекта // Искусственный интеллект и принятие решений. 2024. № 3. С. 3–17. DOI: 10.14357/20718594240301.
26. Bartsch S., Behn O., Benlian A., Brownsword R. [et al.] Governance of High-Risk AI Systems in Healthcare and Credit Scoring // Business & Information Systems Engineering. 2025. Vol. 67, No. 4. P. 563. DOI: 10.1007/s12599-025-00944-4.
27. Patil A., Mishra B., Chockalingam S., Misra S., Kvalvik P. Securing Financial Systems Through Data Sovereignty: a Systematic Review of Approaches and Regulations // Int. J. Inf. Secur. 2025. Vol. 24. Art. 159. DOI: 10.1007/s10207-025-01074-4.

Trust in Artificial Intelligence Systems as a Condition for Digital Sovereignty in the Financial Sector

Evgeniy Vyacheslavovich Samokhodkin — Postgraduate Student, Department of Sociology, Management Psychology and History, State University of Management.
E-mail: rodentforme@gmail.com

Alisa Andreevna Samokhodkina — Postgraduate Student, Department of Sociology, Management Psychology and History, State University of Management.
E-mail: alisaelzon@gmail.com

This paper examines trust in artificial intelligence systems in the financial sector as a condition of digital sovereignty. The study aims to provide a theoretical and analytical explanation of how trust is formed at the individual-behavioral and institutional levels and under what conditions it becomes a factor of sovereignty-oriented development of the financial digital environ-

ment. The methodological framework combines socio-technical, institutional, and systemic approaches, as well as analysis, synthesis, and comparative generalization of academic literature. It is demonstrated that trust cannot be reduced either to user loyalty or to the technical efficiency of an algorithm; rather, it emerges at the intersection of explainability, accountability, model risk management, data control, and infrastructural autonomy. It is argued that under conditions of opacity and external technological dependencies, trust becomes surrogate in nature and does not contribute to the strengthening of digital sovereignty.

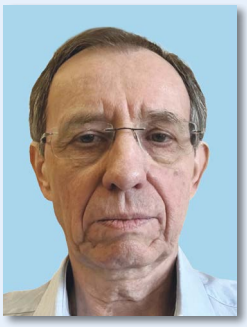
Keywords: artificial intelligence, trust in artificial intelligence, digital sovereignty, financial sector, explainable artificial intelligence, model risk, socio-technical infrastructure

REFERENCES

1. Ridzuan N.N., Masri M., Anshari M., Fitriyani N.L., Syafrudin M. AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility // Information. 2024. Vol. 15, No. 8. Art. 432. DOI: 10.3390/info15080432.
2. Samokhodkin E.V., Elzon A.A. Analysis of the Relationship Between Scientific Interest and Publication Dynamics on Artificial Intelligence in the Russian Federation (2020–2024) // Scientific and Technical Information Processing. 2025. Vol. 52, No. 2. P. 152. DOI: 10.3103/S0147688225700182.
3. Afroogh S., Akbari A., Malone E., Kargar M., Alambeigi H. Trust in AI: Progress, Challenges, and Future Directions // Humanit. Soc. Sci. Commun. 2024. Vol. 11. Art. 1568. DOI: 10.1057/s41599-024-04044-8.
4. Samokhodkin E.V., Elzon A.A. Social Threats of Artificial Intelligence: Classification and Risk Assessment // Scientific and Technical Information Processing. 2025. Vol. 52, No. 3. P. 263. DOI: 10.3103/S0147688225700674.
5. Kuzin M.A. Otsenka vliyaniya razvitiya iskusstvennogo intellekta na finansovyy sektor ekonomiki // Vestnik evraziyskoy nauki. 2023. T. 15, № s4. Art. 31FAVN423 (in Russian).
6. Rodriguez Pita P., Perez-Martinez J., Urueña López A. From Concept to Method: A Framework for Measuring Digital Sovereignty // SSRN. 2025. DOI: 10.2139/ssrn.5683701.
7. Farrand B., Farrand Carrapico H. Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity // European Security. 2022. Vol. 31, No. 3. P. 435. DOI: 10.1080/09662839.2022.2102896.
8. Avdiyskiy V.I., Ivanov A.V., Tsaregorodtsev A.V. Vzaimosvyaz tsifrovogo suvereniteta i tsifrovogo prostranstva: novye vyzovy i perspektivy // Vestnik evraziyskoy nauki. 2024. T. 16, № s3. Art. 21FAVN324 (in Russian).
9. Balasubramaniam N., Kauppinen M., Rannisto A., Hiekkanen K., Kujala S. Transparency and Explainability of AI Systems: From Ethical Guidelines to Requirements // Information and Software Technology. 2023. Vol. 159. Art. 107197. DOI: 10.1016/j.infsof.2023.107197.
10. Timokhovich A.N., Samokhodkin E.V., Elzon A.A. Classification of Epistemological Threats Posed by Artificial Intelligence // Scientific and Technical Information Processing. 2025. Vol. 52, No. 4. P. 318. DOI: 10.3103/S0147688225700741.
11. Yeo W.J., Van Der Heever W., Mao R., Cambria E., Satapathy R., Mengaldo G. A Comprehensive Review on Financial Explainable AI // Artif. Intell. Rev. 2025. Vol. 58. Art. 189. DOI: 10.1007/s10462-024-11077-7.
12. Kantaev N.K. Perspektivy ispolzovaniya metodov mashinnogo obucheniya dlya otsenki kreditnykh riskov // Vestnik evraziyskoy nauki. 2025. T. 17, № s2. Art. 70FAVN225 (in Russian).
13. Weber P., Carl K.V., Hinz O. Applications of Explainable Artificial Intelligence in Finance — a Systematic Review of Finance, Information Systems, and Computer Science Literature // Manag. Rev. Q. 2024. Vol. 74, No. 2. P. 867. DOI: 10.1007/s11301-023-00320-0.

14. Yakubin A.Ya. Iskusstvennyy intellekt v kreditnom skoringe: razrabotka, obuchenie i primenenie modeli // Molodoy uchenyy. 2025. № 19 (570). S. 33–35 (in Russian).
15. Samokhodkin E.V., Elzon A.A. Podkhody k formalizatsii normativnogo povedeniya avtonomnykh intellektualnykh agentov // Iskusstvennyy intellekt i prinyatie resheniy. 2025. № 4. S. 35. DOI: 10.14357/20718594250403 (in Russian).
16. Alonso Robisco A., Carbó Martínez J.M. Measuring the Model Risk-Adjusted Performance of Machine Learning Algorithms in Credit Default Prediction // Financial Innovation. 2022. Vol. 8. Art. 70. DOI: 10.1186/s40854-022-00366-1.
17. Heß V.L., Damásio B. Machine Learning in Banking Risk Management: Mapping a Decade of Evolution // International Journal of Information Management Data Insights. 2025. Vol. 5, No. 1. Art. 100324. DOI: 10.1016/j.jjimei.2025.100324.
18. Fritz-Morgenthal S., Hein B., Papenbrock J. Financial Risk Management and Explainable, Trustworthy, Responsible AI // Front. Artif. Intell. 2022. Vol. 5. Art. 779799. DOI: 10.3389/frai.2022.779799.
19. Gozgeshev E.A. Iskusstvennyy intellekt v bankovskom sektore: vozmozhnosti i riski // Vestnik evraziyskoy nauki. 2024. T. 16, № s6. Art. 49FAVN624 (in Russian).
20. Byambaa O., Yondon C., Rentsen E., Darkhijav B., Rahman M. An Empirical Examination of the Adoption of Artificial Intelligence in Banking Services: the Case of Mongolia // Futur. Bus. J. 2025. Vol. 11, No. 1. Art. 76. DOI: 10.1186/s43093-025-00504-y.
21. Bashir Z., Farooq S., Iqbal M.S., Aamir M. The Role of Trust in Financial Robo-Advisory Adoption: A Case of Young Retail Investors in Pakistan // Sustainable Futures. 2025. Vol. 9. Art. 100538. DOI: 10.1016/j.sftr.2025.100538.
22. Pathak A., Bansal V. AI as Decision Aid or Delegated Agent: The Effects of Trust Dimensions on the Adoption of AI Digital Agents // Computers in Human Behavior: Artificial Humans. 2024. Vol. 2, No. 2. Art. 100094. DOI: 10.1016/j.chbah.2024.100094.
23. Hermann E., Alberhasky M. The Trusted Partner for Financial Decision Making: Romantic Partner or AI? // Computers in Human Behavior. 2026. Vol. 177. Art. 108877. DOI: 10.1016/j.chb.2025.108877.
24. Han J., Ko D. Trust Formation, Error Impact, and Repair in Human-AI Financial Advisory: A Dynamic Behavioral Analysis // Behav. Sci. 2025. Vol. 15, No. 10. Art. 1370. DOI: 10.3390/bs15101370.
25. Kobrinskiy B.A. Doverie k tekhnologiyam iskusstvennogo intellekta // Iskusstvennyy intellekt i prinyatie resheniy. 2024. № 3. S. 3–17. DOI: 10.14357/20718594240301 (in Russian).
26. Bartsch S., Behn O., Benlian A., Brownsword R. [et al.] Governance of High-Risk AI Systems in Healthcare and Credit Scoring // Business & Information Systems Engineering. 2025. Vol. 67, No. 4. P. 563. DOI: 10.1007/s12599-025-00944-4.
27. Patil A., Mishra B., Chockalingam S., Misra S., Kvalvik P. Securing Financial Systems Through Data Sovereignty: a Systematic Review of Approaches and Regulations // Int. J. Inf. Secur. 2025. Vol. 24. Art. 159. DOI: 10.1007/s10207-025-01074-4.

Индекс УДК 004.94:007:517:519.6
Код ГРНТИ 16.01.29, 19.01, 27.35, 28.19.27, 34.17.03
DOI: 10.22204/2410-4639-2026-129-01-127-135



А.А. ЕГОРОВ,
М.А. ЕГОРОВА*

Модель распространения информации в обществе: учёт влияния современных масс-медиа**

В статье исследована динамическая модель распространения информации в некотором обществе. Рассмотренная модель учитывает влияние средств масс-медиа на распространение информации в данном обществе. Представлены результаты теоретического анализа и компьютерного моделирования. Дано описание некоторых случаев, демонстрирующих особенности поведения рассматриваемой модельной общественной системы при вариации управляющих параметров. Проанализирован важный случай, когда информация и энтропия измеряются на одном уровне рецепции, т.е. на сенсорном уровне (органами зрения и/или слуха). Показано, что в энтропийной шкале информация «стоит» достаточно дёшево. Приведены численные оценки величины полной информации в битах и в единицах энтропийной шкалы для короткого и длинного сообщений. Анализ полученных в настоящей статье результатов позволил установить области изменения параметров системы и соотношение между ними, при которых происходит как переход от стационарного к периодическому, а затем к хаотическому поведению системы, так и последующий переход — от хаотического к стационарному или периодическому поведению. Отмечена важная роль в этих процессах бифуркаций удвоения периода. Кратко рассмотрена проблема корректности задач рассеяния, возникающих при исследовании распространения информации в обществе. Рекомендовано делать поиск устойчивого приближённого решения подобных задач на множестве функций, интегрируемых по модулю в квадрате. В заключении отмечена возросшая роль Интернета среди других электронных средств массовой информации.

Ключевые слова: информация, энтропия, система, общество, масс-медиа, лингвистика, математическая модель, бифуркация, рецепция, компьютерное моделирование

* **Егоров Александр Алексеевич** — доктор физико-математических наук, внештатный профессор-консультант, Российский университет дружбы народов им. П. Лумумбы.
E-mail: alexandr_egorov@mail.ru
Егорова Майя Александровна — кандидат политических наук, доцент, кафедра иностранных языков факультета гуманитарных и социальных наук Российского университета дружбы народов им. П. Лумумбы.
E-mail: egorova-ma@rudn.ru

** Работа выполнена при частичной поддержке «Программы стратегического академического лидерства РУДН».

Введение

В общем случае модель распространения информации в некотором обществе может быть описана, например, некоторой системой дифференциальных или интегро-дифференциальных уравнений, поскольку поведение моделируемой системы существенно определяется предыдущими состояниями системы. Тем не менее, исследование более простых моделей позволяет получить результаты, допускающие достаточно простую наглядную интерпретацию, особенно в случае анализа бифуркационных явлений, связанных с качественным изменением поведения исследуемой системы [1].

Под «*информацией*» будем понимать любые сведения и данные, отражающие свойства объектов в природных, социальных и технических системах и передаваемые звуковым, графическим или иным способом без применения или с применением технических средств [2]. В более узком смысле «*информация*» — содержание сообщения, рассматриваемое в процессе его передачи, восприятия и использования, уменьшающее неопределённость в выборе различных возможностей [1, 2]. При рассмотрении сообщений в лингвистике проводится анализ «*лингвистической информацией*», например, семантики (определяет соотношение между словами и их значениями) и грамматики (правила, выражающие общие синтаксические свойства слов и групп слов, позволяющие производить и/или описывать правильные предложения языка) некоторого языка.

«*Бифуркация*» (от латинского bifurcus — раздвоенный) — появление нового качества в поведении динамической системы при малом изменении её параметров [1, 3]. Если при перестройке объекта он не изменяется во времени, то вместо термина бифуркация можно использовать термин «*катастрофа*» [3]. При бифуркации происходит перестройка характера движения исследуемой системы, например, физической, химической, биологической или социальной. Предметом теории катастроф является изучение зависимости качественной природы решений уравнений от значений параметров, входящих в данные уравнения.

Пуанкаре в своих работах показал, что нередко требуется только ограниченный объём информации, причём качественного характера, который и представляет основной интерес при изучении конкретных объектов и описывающих их систем уравнений [3]. С этой точки зрения исследование полного набора решений уравнений, описывающих исследуемый объект, является препятствием для понимания качественных изменений в поведении решений уравнений и, как следствие, в поведении изучаемого объекта. При этом наиболее важным является понимание того, как качественно меняется поведение изучаемой системы при изменении описывающих её (управляющих) параметров.

Бифуркации происходят в точках бифуркации (критические точки); при этих значениях параметров системы она меняет своё поведение — происходит качественное изменение свойств системы. Если состояние системы можно описать некоторой потенциальной функцией, то в бифуркационном множестве происходит переход из одного локального минимума (устойчивое состояние системы) в другой, т.е. фазовый переход.

Полученные в работе оригинальные результаты дают возможность по-новому взглянуть на развитие общества в свете развития современных информационных технологий. А также предлагают новые инновационные подходы к исследованию явления передачи и распространения различной информации в сложных социальных системах.

Материалы и методы

Динамическая модель распространения некоторой информации I в обществе может быть описана следующим нелинейным уравнением [1]:

$$I_{n+1} = \left[aI_n \left(M - I_n \right) + b\left(M - I_n \right)^2 \right] \lambda, \quad (1)$$

где $n = 1, 2 \ldots$ ($n = 1$ соответствует первому «измерению», т.е. I_1 — начальное значение

данной информации, например, в начальный момент времени t_1); a — коэффициент, характеризующий распространение информации при контактах «незнающих» со «знающими» данную информацию I_n; b — коэффициент, который будет характеризовать вклад преимущественно электронных средств массовой информации (действует только на «незнающих» лиц); M — максимальное значение информации; λ — параметр задачи, который в соответствии с теорией катастроф [3] может быть назван управляющим параметром. Уравнение (1) позволяет исследовать зависимость информации, как от времени, так и от величин a, b, M, λ.

Преобразуем уравнение (1) очевидным образом к виду:

$$y = \lambda_a x(1-x) + \lambda_b (1-x)^2, \qquad (2)$$

где сделана замена переменных: $y=I_{n+1}/M$, $x=I_n/M$; $\lambda_a=aM\lambda$, $\lambda_b=bM\lambda$, — новые управляющие параметры системы; $0 \le x \le 1$.

Результаты аналитического исследования уравнения (2) можно свести к следующему. Предельные значения функции y:

$$\lim_{x\to 0} y = \lambda_b, \lim_{\substack{x\to 0 \\ b\to 0}} y = 0, \lim_{x\to 1} y = 0. \qquad (3)$$

Экстремум функции $y(x)$:

$$y_{\max} = \left[\frac{\lambda_a^2}{4(\lambda_a-\lambda_b)}\right] \begin{cases} > 0, \lambda_a > \lambda_b; \\ < 0, \lambda_a < \lambda_b. \end{cases} \qquad (4)$$

наблюдается при значении $x = x_m$:

$$x_m = \begin{cases} \dfrac{\lambda_a - 2\lambda_b}{2(\lambda_a-\lambda_b)} > 0, \lambda_a > 2\lambda_b; \\ \dfrac{2\lambda_b - \lambda_a}{2(\lambda_b-\lambda_a)} > 0, \lambda_a < 2\lambda_b. \end{cases} \qquad (5)$$

При этом:

$$\lim_{\lambda_a\to\lambda_b}(y_{\max}) \to \begin{cases} +\infty, \lambda_a > \lambda_b; \\ -\infty, \lambda_a < \lambda_b. \end{cases} \qquad (6)$$

Простой анализ показывает, что выпуклость графика функции $y(x)$ направлена вверх при $\lambda_b < \lambda_a$ и — вниз при $\lambda_a < \lambda_b$. Поскольку информация является положительно определённой величиной ($I \ge 0$ по определению [4]), случай $y < 0$ подробно не исследуется.

Учитывая положительную определённость информации $I \ge 0$ [4], можем определить информацию так:

$$I \propto |\Psi|^2, \qquad (7)$$

где Ψ — волновая функция, которая по определению является комплекснозначной величиной, т.е. содержит действительную и мнимую части. В (7) функция Ψ зависит от пространственных переменных ($r = r(x, y, z)$) и времени (t), т.е. $\Psi = \Psi(r;t)$.

При заданном направлении распространения информационной волны функция Ψ является решением дифференциального уравнения второго порядка

$$c^2 \frac{\partial^2 \Psi(z;t)}{\partial z^2} - \frac{\partial^2 \Psi(z;t)}{\partial t^2} = 0. \qquad (8)$$

Данное уравнение гиперболического типа описывает математические модели различных реальных процессов в физических, биологических и социальных системах. В одномерном уравнении (8) пространственная координата (ось z) направлена вдоль направления распространения потока информации; c — скорость распространения волны.

Решение $\Psi(z;t)$ волнового уравнения известно и даётся формулой Даламбера:

$$\Psi(z;t) = \frac{U(z-ct)+U(z+ct)}{2} + \frac{1}{2b}\int_{z-ct}^{z+ct} \phi(x)\,dx. \qquad (9)$$

При поиске решения (9) учитывается, что $\Psi(z;0) = U(x)$, $\Psi_t(z;0) = \varphi(x)$, b — некоторая константа (см., например, [7]). Решение (9) ищется в виде функции непрерывной в некоторой замкнутой области. Следовательно, мы ограничиваем класс искомых функций набором достаточно гладких функций $\Psi(z;t)_m$, где $m = 1, 2, \ldots M$ ($M < \infty$).

Подчеркнём, что волновой процесс распространения информации может сопровождаться также диффузией информации в окрестности сегментов общества, куда доходят волны данной информации.

Важно отметить, что при непрерывном изменении управляющих параметров системы может реализоваться случай $\lambda_a < \lambda_b$, когда функция y терпит разрыв, оставаясь в пространстве управляющих параметров положительной при $\lambda_b < \lambda_a$ ($y_{max} \to +\infty$) и отрицательной при $\lambda_a < \lambda_b$ ($y_{max} \to -\infty$). Этот случай может быть проанализирован, если информация I и энтропия S (информационная энтропия [4]) измеряются на одном уровне рецепции (восприятия; например, зрительная или слуховая рецепция; см. подробнее ниже), когда выполняется закон сохранения [5]:

$$I + S = const. \qquad (10)$$

Эквивалентность информации I (в битах, т.е. двоичных единицах) и энтропии S (в Дж/К) подобна [4, 5] эквивалентности массы m и энергии E в известной формуле Эйнштейна: $E = m \cdot c^2$, где c — скорость света. При таком подходе 1 бит информации I эквивалентен величине $k \ln 2 \approx 10^{-22}$ Дж/К (очень маленькая термодинамическая величина), где $k = 1{,}38 \cdot 10^{-23}$ Дж/К — постоянная Больцмана, $\ln 2 \approx 0{,}6931$. Следовательно, в энтропийной шкале информация I «стоит достаточно дёшево». Так, при флуктуациях идеального газа (некоторый модельный объект) в заданном объёме прирост информации I на 1 бит требует затрат энергии (т.е. совершения работы) при заданной температуре $T = 300$ K (около 27ºC), равной величине $kT \ln 2 \approx 3 \cdot 10^{-20}$ Дж. Это естественно нижняя оценка затрат энергии на получение 1 бита информации.

Регистрация информации, т.е. *рецепция*, осуществляется людьми (участниками рассматриваемого процесса распространения информации в обществе) на сенсорном уровне (органами зрения, слуха, обоняния, вкуса, электро-, термо- и другими рецепторами). Передаваемые далее сигналы обрабатываются в разных частях нервной системы, и в итоге в её высших отделах (мозг) формируется ответная реакция организма человека на принятую информацию.

При возрастании I убывает S и наоборот (обе величины I и S измеряются в одинаковых единицах и имеют макроскопический смысл). Как видно при учёте закона сохранения (10), энтропия S становится, в сущности, мерой *недостатка информации* о рассматриваемой системе. Таким образом, резкое (скачком) убывание y вызовет скачок энтропии S в системе. Как следствие, резко возрастёт недостаток информации об исследуемой системе, т.е. о состоянии общества. С другой стороны, информационная энтропия совпадает с термодинамической энтропией [5]. Отсюда следует реальный физический смысл информации I, который можно сформулировать так: за полученную информацию I надо «платить» увеличением энтропии S рассматриваемой системы. Таким образом, любое измерение влечёт за собой возрастание энтропии S исследуемой системы, например — окружающей среды (понимаемой здесь в достаточно широком смысле этого слова).

Следовательно, при $\lambda_a < \lambda_b$ в системе нет информации I в традиционном её понимании (её нельзя использовать в обычном смысле), это фактически энтропия S. Применительно к исходной постановке задачи можно сказать, что если официальные каналы информации (электронные и другие масс-медиа, например, Интернет и телевидение) преобладают над общественными (т.е. в случае, когда $\lambda_b < \lambda_a$), то, как ни покажется странным, информации в системе (обществе) не становится больше.

Этот случай можно проинтерпретировать так: в обществе наблюдается рост дезинформации, т.е. манипулирование общественным сознанием преобладает над процессами получения достоверной информации. И в предельном случае — недостаток (правдивой) информации в обществе бесконечен, несмотря на кажущийся её избыток.

Эта проблема может иметь серьёзные последствия, например, при социологических исследованиях, когда такие известные методы исследования как опросы в различных социальных или так называемых «фокус группах» могут приводить как минимум к неправильной интерпретации полученных результатов. Особенно в тех случаях, когда те или иные группы участвующих в социологических опросах получают информацию (в результате становятся «знающими») об окружающем их мире (обществе) и происходящих в нём процессах лишь из узкого круга определённых источников информации, например, только из радио, газет, журналов или телевидения. Особенно некорректно, например, говорить о рейтингах в условиях доминирования и тем более монополии на информацию в обществе одной партии или организации.

Результаты

Приведём краткое описание некоторых результатов, полученных в процессе компьютерного моделирования процессов распространения информации в некотором обществе, где присутствуют как официальные каналы информации (электронные и др. масс-медиа, например, Интернет и телевидение), так и общественные неформальные, например, различные социальные сети общения.

В численных расчётах уравнение (2) было приведено к виду (8), удобному при численных расчётах на дискретном множестве значений переменной x_n:

$$x_{n+1} = \lambda_a x_n (1 - x_n) + \lambda_b (1 - x_n)^2, \qquad (11)$$

где величина $n = 1, 2, \ldots$ ограничена сверху главным образом точностью и скоростью расчётов на компьютере.

Отметим несколько наиболее интересных случаев, описывающих поведение рассматриваемой модельной общественной системы при вариации управляющих параметров λ_a и λ_b.

При $\lambda_a = 3$ и $\lambda_b = 0{,}3$ функция $y(x)$ имеет максимум $y_{max} \approx 0{,}83$ при $x = x_{max} \approx 0{,}44$. При увеличении параметра $\lambda_a \in (0,4)$ в системе наблюдаются следующие закономерности. При $\lambda_a < 1$ $y(x) \to 0$ (итерации x_{n+1} (т.е. информация I_n) сходятся к окрестности точки 0 — устойчивая неподвижная точка).

При дальнейшем росте управляющего параметра λ_a происходит бифуркация, а вновь появившаяся точка становится устойчивой (итерированные значения информации стремятся к некоторой постоянной величине, т.е. динамический режим становится стационарным или имеет период, равный единице).

Дальнейшее увеличение параметра λ_a снова приводит к изменению системы: происходит бифуркация удвоения периода (неподвижная точка расщепляется, и I_n осциллирует между двумя значениями, образующими устойчивый аттрактор с периодом 2). В этом случае отображение (11) имеет устойчивый цикл с периодом 2: S^2. При дальнейшем увеличении параметра λ_a возникают циклы S^2, S^4, S^6, S^8, S^{10}, ..., S^{64} и т.д. Можно построить функцию $y = f(f(x))$, которая пересекается с прямой $y = x$ в точках, принадлежащих рассматриваемому циклу (они и определяют данный цикл).

Дальнейший рост управляющего параметра λ_a позволяет наблюдать переход системы в хаотический режим: непериодический, стохастический процесс возникает как предел всё более сложных структур (циклов S^{2^p}, где $p = 0,1,2,\ldots$).

Таким образом, хаос возникает как предел сверхсложной организации. Наконец, при некотором значении управляющего параметра $\lambda_a < \lambda_\infty$ отображение (11) даёт уже совершенно непериодическую последовательность x_{n+1}. Между порядком и хаосом наблюдается глубокая внутренняя связь. Подобные закономерности существуют в любых системах, где наблюдаются последовательности бифуркаций удвоения периода [1, 3, 6].

Анализ полученных в настоящей работе зависимостей позволяет установить области изменения параметров системы и соотношения между ними, при которых происходит как переход от стационарного

к периодическому, а затем к хаотическому поведению системы, так и последующий переход — от хаотического к стационарному или периодическому поведению. Исследование особенностей фазовых переходов применительно к рассмотренной модели распространения информации в современном обществе как некоторой диссипативной (динамической) системы выходит далеко за рамки настоящей работы и требует во многом междисциплинарного подхода.

Проблема корректности задач рассеяния при исследовании проблемы распространения информации в обществе

В общем случае волновое распространение информации сопровождается процессами её рассеяния и диффузии в окрестности общественных сфер, куда доходят волны распространяющейся информации. Следовательно, надо кратко затронуть проблемы корректности задач рассеяния информации в лингвистическом сообществе.

Важно отметить, что необходимо различать корректно и некорректно поставленные задачи (см., например, [7]). Задача называется *корректно поставленной*, если выполняются следующие требования: 1) её решение существует; 2) это решение определяется однозначно; 3) решение непрерывно зависит от входных данных, т.е. малым изменениям входных данных соответствуют малые изменения в решении задачи (свойство устойчивости решения). Задачи, которые не удовлетворяют указанным требованиям, называются *некорректно поставленными*.

Доказательство *существования решения* поставленных задач при наличии различного рода помех основывается на существовании регуляризирующих операторов для интегральных уравнений (см., например, [7]).

Единственность приближённого решения при наличии помех основана на использовании регуляризирующего оператора. При точных входных данных решение сформулированной проблемы распространения информации существует и оно единственное.

Поиск *устойчивого решения* проблемы возможен, например, на множестве функций, интегрируемых по модулю в квадрате L_2. При этом в качестве приближённого решения обычно берётся наиболее гладкое из возможных в L_2 решений $\{\mathrm{I}(z)\}_s$ (s = 0,1,2,...). Это означает, что конечен интеграл:

$$\int \left|I\left(z\right)\right|^2 dz < +\infty, \qquad (12)$$

где интеграл (12) определён на конечном отрезке z. Интервал определения информации $I(z)$ ограничен естественным образом направлением, вдоль которого происходит распространение потока информации.

В рассматриваемом случае уклонение искомого приближённого решения $I(z)_s$ от точного решения $I(z)$ оценивается в метрике L_2 по формуле:

$$l = \left(\int \left|I\left(z\right) - I\left(z\right)_s\right|^2 dz\right)^{1/2}. \qquad (13)$$

Использование процедуры регуляризации сводится к достижению минимума невязки: $l \to 0$. Важно подчеркнуть, что компьютерная реализация этих методов требует в первую очередь построения адекватной математической модели рассматриваемого явления создания, передачи и распространения информации в обществе, а затем разработки эффективных вычислительных алгоритмов. Более подробный анализ этих проблем выходит за рамки настоящей статьи (см., например, [7]).

Выводы. Заключение

В настоящей статье проведено исследование динамической модели распространения информации в обществе. Рассмотренная модель учитывает влияние важнейших средств массовой информации на распространение информации в данном обществе.

Приведём несколько вполне очевидных выводов. При определённых значениях управляющих параметров можно полу-

чить достаточно протяжённые области хаоса, а при других — узкие области хаоса быстро сменяются узкими областями стационарного или периодического поведения.

Анализ полученных результатов показал, что существует такое соотношение управляющих параметров, при котором две составляющие процесса распространения информации (общество как совокупность граждан, различных гражданских институтов и государство в лице государственных (в первую очередь — электронных) средств массовой информации) могут оказывать взаимно регуляризирующее действие. Данный процесс регуляризации будет приводить, по сути, к определённому сглаживанию сложных процессов взаимодействия (эффекты саморегуляции) различных составляющих современного информационного общества как динамической открытой системы.

Заметим, что при анализе процесса распространения информации в обществе с точки зрения лингвистики, необходимо уделять внимание в первую очередь лингвистическим особенностям используемых языков, особенно в полилингвистических обществах, где кроме одного общегосударственного языка могут использоваться другие национальные языки или диалекты. В странах, где какая-то часть населения сохраняет билингвизм, эти аспекты могут приобрести критически важные особенности, как в процессах распространения информации в различных слоях общества, так и в особенностях исследования этих процессов.

В последние десятилетия всё возрастающую роль среди электронных средств массовой информации (телевидение, Интернет, радио) начинает играть Интернет. Более того, его роль в процессах распространения информации в обществе будет со временем только возрастать. Это обуславливает необходимость и более того — потребность учитывать двум взаимосвязанным элементам процесса распространения информации (общество и государство) данную объективную реальность в своей повседневной деятельности. Поскольку только распространение достоверной информации способно, при правильной организации этого процесса, стать одним из важных факторов стабилизации и гармонизации разнообразных и во многом противоречивых процессов динамично развивающегося современного открытого демократического общества.

Приложение

Для численных оценок величины информации можно использовать известную в теории информации формулу для полной информации I_s, содержащейся в некотором сообщении:

$$I_S = p \log_2 \mathrm{K}\,, \qquad (14)$$

где p — общее число символов в сообщении или длина сообщения (непрерывный сигнал заменён дискретной последовательностью отсчётов); K — число различных символов используемого алфавита.

При распространении некоторого короткого сообщения длиной $p = 150$, в котором алфавит состоит из 25 символов, в соответствии с формулой (14) имеем значение $I_s \approx 697$ бит (двоичные единицы или бит информации), при некотором фиксированном заданном начальном значении информации. В энтропийной шкале та же самая информация эквивалентна примерно $7 \cdot 10^{-20}$ Дж/К.

При распространении более продолжительного сообщения длиной $p = 3000$, в котором алфавит состоит из 30 символов, аналогично получаем значение $I_s \approx 14720$ бит. В этом случае информация в энтропийной шкале эквивалентна примерно $1{,}5 \cdot 10^{-18}$ Дж/К. Видно, что в рассмотренных здесь случаях при возрастании длины сообщения в 20 раз, величина передаваемой информации возрастает примерно в 21 раз. Такое незначительное отличие обусловлено медленным изменением логарифмической функции в формуле (14). Действительно, при фиксированном значе-

нии p возрастание числа различных символов алфавита от 20 до 30 приводит к росту информации всего лишь в 1,1 раза, а при их росте от 5 до 30 приводит к росту информации примерно в 2,1 раза. Только при существенном увеличении числа символов алфавита с 5 до 550 информация возрастает примерно в 4 раза.

ЛИТЕРАТУРА

1. Егоров А.А., Егорова М.А. О моделях распространения лингвистической информации в языковом сообществе // Тез. докл. XXI-й Всерос. конф. «Теоретические основы конструирования численных алгоритмов и решение задач математической физики», 5–11 сентября 2016 г., Новороссийск, Абрау-Дюрсо. М.: ИПМ им. М.В. Келдыша РАН, 2016. С. 82–83.
2. Физическая энциклопедия / гл. ред. А.М. Прохоров. Т. 2. М.: Сов. энциклопедия, 1990. 704 с.
3. Гилмор Р. Прикладная теория катастроф: в двух книгах. Кн. 1. М.: Мир, 1984. 350 с.
4. Яглом А.М., Яглом И.М. Вероятность и информация. М.: Наука, 1973. 512 с.
5. Волькенштейн М.В. Биофизика. М.: Наука, 1981. 576 с.
6. Компьютеры и нелинейные явления: информатика и современное естествознание / авт. предисл. А.А. Самарский. М.: Наука, 1988. 192 с.
7. Арсенин В.Я. Методы математической физики и специальные функции. М.: Наука, 1974. 432 с.

A Model of Information Spreading in Society: Taking into Account the Influence of Modern Mass Media

Aleksandr Alekseyevich Egorov — Dr.Sc. (Doctor of Sciences in Physical and Mathematical Sciences), Visiting Professor-consultant (Consulting Professor), Peoples' Friendship University of Russia named after Patrice Lumumba.
E-mail: alexandr_egorov@mail.ru

Maia Aleksandrovna Egorova — Candidate of Political Sciences, Associate Professor, Department of Foreign Languages of the Faculty of Humanities and Social Sciences of Peoples' Friendship University of Russia named after Patrice Lumumba.
E-mail: egorova-ma@rudn.ru

This article examines a dynamic model of information spreading in a given society. The model takes into account the influence of mass media on information's propagation in this society. The results of theoretical analysis and computer modeling are presented. Several cases are described, demonstrating the behavioral characteristics of the model social system under consideration when varying control parameters. An important case is analyzed where information and entropy are measured at the same level of perception, i.e., at the sensory level (by the organs of vision and/or hearing). It is shown that on the entropy scale, information is relatively cheap. Numerical estimates of the total information in bits and in units of the entropy scale are provided for short and long messages. The analysis of the results obtained in this article made it possible to establish the areas of change in the system parameters and the relationship between them, in which both the transition from stationary to periodic and then to chaotic behavior of the system occurs, and the subsequent transition from chaotic to stationary or periodic behavior take place. The important role of period-doubling bifurcations in these processes is noted. The problem of the well-posedness of scattering problems arising in the study of information dissemination in society is briefly considered. It is recommended to search for stable approximate solutions to such problems on a set of square-integrated functions. The conclusion notes the growing role of the internet among other electronic media.

Keywords: information, entropy, system, society, mass media, linguistics, mathematical model, bifurcation, reception, computer modeling

REFERENCES

1. Egorov A.A., Egorova M.A. O modelyakh rasprostraneniya lingvisticheskoy informatsii v yazykovom soobshchestve // Tez. dokl. XXI-y Vseros. konf. «Teoreticheskie osnovy konstruirovaniya chislennykh algoritmov i reshenie zadach matematicheskoy fiziki», 5–11 sentyabrya 2016 g., Novorossiysk, Abrau-Dyurso. M.: IPM im. M.V. Keldysha RAN, 2016. S. 82–83. (in Russian)
2. Fizicheskaya entsiklopediya / gl. red. A.M. Prokhorov. T. 2. M.: Sov. entsiklopediya, 1990. 704 s. (in Russian).
3. Gilmor R. Prikladnaya teoriya katastrof: v dvukh knigakh. Kn. 1. M.: Mir, 1984. 350 s. (in Russian).
4. Yaglom A.M., Yaglom I.M. Veroyatnost i informatsiya. M.: Nauka, 1973. 512 s. (in Russian).
5. Volkenshteyn M.V. Biofizika. M.: Nauka, 1981. 576 s. (in Russian).
6. Kompyutery i nelineynye yavleniya: informatika i sovremennoe estestvoznanie / avt. predisl. A.A. Samarskiy. M.: Nauka, 1988. 192 s. (in Russian).
7. Arsenin V.Ya. Metody matematicheskoy fiziki i spetsialnye funktsii. M.: Nauka, 1974. 432 s. (in Russian).

Индекс УДК 004.896
Код ГРНТИ 28.23.11
DOI: 10.22204/2410-4639-2026-129-01-136-139

И.А. ШЕРЕМЕТ*

Большие языковые модели и их влияние на интеллектуальный потенциал человечества

Рассматриваются сферы применения больших языковых моделей и присущие им принципиальные недостатки. Анализируются негативные последствия их массового внедрения.

Ключевые слова: большая языковая модель, генеративный искусственный интеллект, чат-бот, датацентр

Большая языковая модель (Large Language Model, LLM) — это нейроимитатор разговорного общения (чат-бот), использующий для имитации постоянно пополняемую базу текстов на естественном языке и реализующий генерацию ответов чат-бота на обращения пользователя посредством последовательного подбора каждого следующего слова, согласующегося с несколькими предшествующими словами, из какого-либо из этих текстов. С 2022 года, когда американским стартапом OpenAI во главе с Сэмом Альтманом началась агрессивная рекламная кампания по продвижению нейроимитатора ChatGPT (Generative Pretrained Transformer), большие языковые модели стали фактором планетарного масштаба. Суммарная аудитория различных версий ChatGPT составляет порядка 800 миллионов человек, что позволяет говорить о влиянии нейроимитаторов на интеллектуальный потенциал всего человечества и требует максимально глубокого и ответственного анализа возможных последствий массового внедрения LLM.

Не подлежит сомнению то обстоятельство, что чат-боты способны приносить определённую пользу при решении различных практических задач. В первую очередь речь идёт о быстром формировании правдоподобных текстовых, аудио и видео документов (в последних двух случаях применяются являющиеся развитием LLM большие мультимодальные модели — Large Multimodal Model, LMM) по любому требуемому вопросу, что особенно ценно при необходимости подготовки материалов на малознакомые темы. Изначально неочевидным полезным применением LMM является создание языковой среды для разговорного общения в процессе обучения иностранному

* **Шеремет Игорь Анатольевич** — академик РАН, профессор, доктор технических наук, главный научный сотрудник Геофизического центра РАН.
E-mail: i.sheremet@gcras.ru

языку. Сложно найти испанца, вьетнамца или араба, который беседовал бы с вами ни о чём по 2–3 часа в день. А для чат-бота, обученного на текстах или аудиограммах на соответствующем языке, это, разумеется, не проблема. В последнее время существенно расширилась сфера применения LLM за счёт областей, где алгоритмический аппарат LLM используется для накопления и генерации последовательностей таких первичных лексических единиц — токенов, — которые кодируют не лексемы и словоформы, как в базовой идеологии больших языковых моделей, а события либо другие концепты. К таким областям относятся медицина (накопление последовательностей симптомов болезней и использование накопленной базы данных для предсказания их возможного развития по результатам наблюдения за пациентами), кибербезопасность (накопление последовательностей проявлений кибератак и использование накопленной базы данных для предсказания их возможного развития по результатам мониторинга проявлений в защитном периметре сети) и ряд других.

При этом, однако, массовое применение чат-ботов выявило целый ряд принципиальных недостатков LLM:

- генерация бессмысленных ответов («галлюцинаций») в силу отсутствия в технологии LLM средств распознавания смысла накапливаемых текстов и контроля смысла ответов, генерируемых нейроимитатором;
- генерация «токсичных» ответов и фейков вследствие возможности бесконтрольного поступления в базу данных нейроимитатора текстов любого содержания (в том числе целенаправленного «отравления» этой базы данных недостоверными, ложными и злонамеренно искажёнными сведениями);
- генерация однообразных и бесполезных ответов на любые запросы по причине засорения базы данных нейроимитатора текстами, сгенерированными им в ходе его длительной эксплуатации; и т.п.

(В компетентных обзорах по тематике LLM число таких серьёзных недостатков уже более десяти).

Проявившиеся в процессе массового применения чат-ботов очевидная примитивность LLM и реальное несоответствие заявленным в ходе пиар-кампании по её продвижению интеллектуальным возможностям (упомянутая кампания получила в прессе название «рекламный балаган Альтмана») поставили на повестку дня вопрос верификации больших языковых моделей и оценки их перспектив в научном, технологическом и экономическом контексте.

В прогнозе на 2024 год специалисты ведущих аналитических центров (Gartner, MIT и др.), видимо, находясь под влиянием упомянутого «балагана», поставили «генеративный искусственный интеллект» (GenAI), ассоциирующийся с нейроимитаторами, на первое место среди наиболее перспективных направлений научно-технологического развития (это, кстати, само по себе вызывает вопросы относительно качества форсайтов указанных аналитических центров). При этом в прогнозе на 2026 год GenAI как такового в указанной десятке уже нет. Он если и упоминается, то при описании других технологий как возможно применяемая внутри них составная часть.

Что касается технологического аспекта, то датацентры, создаваемые для реализации и эксплуатации нейроимитаторов, состоят из запредельного количества процессоров для накопления и ассоциативной обработки баз данных объёмами в триллионы токенов. При этом NVidia, производитель графических процессоров для строящихся и функционирующих датацентров, стал самой дорогой компанией в истории с капитализацией 5 трлн.$. Потребление электроэнергии датацентрами исчисляется гигаваттами, что в свете сказанного не удивительно. В частности, обработка запроса к ChatGPT требует в 10 раз больше электроэнергии, чем обработка запроса к Google. М. Цукербергом финансируется создание датацентра с энергопотреблением 5 гигаватт. И. Маском анонсировано массовое приме-

нение ядерных реакторов для энергоснабжения датацентров. При этом стоимость электроэнергии для потребителей, проживающих на территориях, прилегающих к датацентрам, возрастает в 2–3 раза. Здесь уместно заметить, что энергопотребление человеческого мозга составляет 20–21 ватт.

И наконец, экономика. 95% решений в области ИИ отклоняются корпоративными заказчиками [1]. OpenAI до настоящего времени убыточен, и его среднеквартальный убыток по состоянию на 1 октября 2025 года составляет 11,5 млрд. долларов, хотя капитализация этого громкого стартапа по разным оценкам составляет 0,5–1 триллион долларов. Инвесторами заготовлено порядка 35 триллионов долларов для превращения их в гораздо большую сумму посредством финансирования технологий искусственного интеллекта, которые в их сознании прочно ассоциируются с LLM. Всё это в совокупности указывает на возникновение «пузыря», который в обозримом будущем может лопнуть, превратив в убытки все средства, которые были инвестированы в инфраструктуру больших языковых моделей. Устойчивого и массово используемого «интеллектуального суперсервиса», который обеспечил бы перманентный приток значимых платежей от его пользователей и возврат вложений в упомянутую инфраструктуру, в обозримой перспективе не просматривается [2]. Выручка OpenAI за первое полугодие 2025 года составила всего 4,5 млрд долларов. Вот как прокомментировал происходящее сам С.Альтман 21 августа 2025 года в интервью агентству Bloomberg, говоря о «пузыре ИИ»: «Находимся ли мы в фазе, когда инвесторы в целом чрезмерно воодушевлены ИИ? По моему мнению, да» [3]. Дж. Безос 4 октября 2025 года подтвердил эту оценку: «Это своего рода промышленный пузырь» [4]. В начале ноября 2025 года П. Тиль, один из наиболее эффективных инвесторов в высокие технологии, продал свою долю в NVidia, что было воспринято многими аналитиками как сигнал о том, что пузырь ИИ начал лопаться. 23 ноября 2025 года С. Альтман разослал сотрудникам OpenAI циркулярное письмо, в котором признал, что компания столкнулась со сложными экономическими условиями и потеряла технологические преимущества. По его оценкам, выручка OpenAI в 2026 году может упасть до 5–10 процентов относительно 2025 года.

Что бы ни происходило на рынке высоких технологий, следует иметь в виду, что массовое распространение чат-ботов несёт целый ряд весьма негативных последствий [5]. В первую очередь, речь идёт о депрофессионализации и интеллектуальной деградации человечества.

Нейроимитаторы превратили процесс обучения в его имитацию. По некоторым оценкам, 87 процентов российских школьников используют ChatGPT и его аналоги для подготовки домашних заданий, не приобретая при этом ни знаний, ни навыков, ради которых обучение и организуется. Аналогичным образом поступают и многие студенты, и соискатели учёных степеней в области гуманитарных наук. Всё это в конечном итоге ведёт к распространению имитократии как власти людей-фейков, обладающих всеми необходимыми внешними атрибутами образованности, кроме самих знаний. В условиях ультрасложной техносферы это неминуемо ведёт к принятию такими людьми неверных управленческих решений, результатом которых может стать разрушение целых сегментов критических инфраструктур с массовой гибелью людей. Некритичное использование LLM-подобных технологий при разработке и проектировании различных технических систем, программных средств, устройств и изделий микроэлектроники сопряжено со снижением уровня ответственности разработчиков за некачественные технические решения, которые, в свою очередь, чреваты возрастанием рисков техногенных катастроф [6].

Обобщая сказанное, следует отметить, что массовое применение генеративного ИИ чревато целым рядом негативных последствий, что требует от нас высочайшей ответственности и осторожности при принятии решений о направлениях развития искусственного интеллекта в России.

ЛИТЕРАТУРА

1. Инициативы в области ИИ терпят неудачу в 95% случаев – мы находимся на грани кризиса, о котором никто не говорит [Электронный ресурс]. URL: https://aftershock.news/?q=node/1568189
2. Ilya Sutskever, Yann LeCun and the End of «Just Add GPUs» [Электронный ресурс]. URL: https://www.abzglobal.net/web-development-blog/ilya-sutskever-yann-lecun-and-the-end-of-just-add-gpus
3. Почему растут опасения по поводу пузыря ИИ стоимостью в триллион долларов [Электронный ресурс]. URL: https://www.profinance.ru/news2/2025/12/01/chw0-pochemu-rastut-opaseniya-po-povodu-puzyrya-ii-stoimostyu-v-trillion-dollarov.html
4. Джефф Безос: ИИ – это «промышленный пузырь», но он поможет человечеству [Электронный ресурс]. URL: https://3dnews.ru/1130265/dgeff-bezos-ii-eto-promishlenniy-puzir-no-on-pomoget-chelovechestvu/
5. Между генерированием слов и деланием дел – большая разница. Китай близок к победе в гонке за мировое технологическое превосходство [Электронный ресурс] // Малоизвестное интересное. Нояб. 2025. URL: https://dzen.ru/a/aTHI8j5pxhe-Ygsh
6. Шеремет И. А. Что ждёт мировую отрасль ИИ в 2026–2030 годах // Business Information Security Journal. 2026. № 1 (60). С. 72.

Large Language Models and Their Impact on the Intellectual Potential of Humanity

Igor Anatolyevich Sheremet – Full member of RAS, Professor, Doctor of engineering science, Chief scientist of the Ge-ophisical Center of RAS.
E-mail: i.sheremet@gcras.ru

Large Language Models areas of application and LLMs fundamental drawbacks are con-sidered. Negative consequences of LLMs wide dissemination are analyzed.

Keywords: Large Language Model, generative artificial intelligence, chat bot, datacenter

REFERENCES

1. Initsiativy v oblasti II terpyat neudachu v 95% sluchaev – my nakhodimsya na grani krizisa, o kotorom nikto ne govorit [Electronic resource]. URL: https://aftershock.news/?q=node/1568189 (in Russian).
2. Ilya Sutskever, Yann LeCun and the End of "Just Add GPUs" [Electronic resource]. URL: https://www.abzglobal.net/web-development-blog/ilya-sutskever-yann-lecun-and-the-end-of-just-add-gpus
3. Pochemu rastut opaseniya po povodu puzyrya II stoimostyu v trillion dollarov [Electronic resource]. URL: https://www.profinance.ru/news2/2025/12/01/chw0-pochemu-rastut-opaseniya-po-povodu-puzyrya-ii-stoimostyu-v-trillion-dollarov.html (in Russian).
4. Dzheff Bezos: II – eto «promyshlennyy puzyr», no on pomozhet chelovechestvu [Electronic resource]. URL: https://3dnews.ru/1130265/dgeff-bezos-ii-eto-promishlenniy-puzir-no-on-pomoget-chelovechestvu/ (in Russian).
5. Mezhdu generirovaniyem slov i delaniyem del – bolshaya raznitsa. Kitay blizok k pobede v gonke za mirovoe tekhnologicheskoe prevoskhodstvo [Electronic resource] // Maloizvestnoe interesnoe. Noyab. 2025. URL: https://dzen.ru/a/aTHI8j5pxhe-Ygsh (in Russian).
6. Sheremet I.A. Chto zhdet mirovuyu otrasl II v 2026–2030 godakh // Business Information Security Journal. 2026. № 1 (60). S. 72 (in Russian).

Вестник Российского фонда фундаментальных исследований

2026, № 1 (129)

Адрес редакции: 119991, Москва, Ленинский пр-т, д. 32а
Тел.: +7 (499) 995-16-05
E-mail: pressa@rcsi.science
https://rcsi.science

Подписано в печать 03.06.2026. Формат 60×90 1/8.
Усл. печ. л. 17,5. Печать офсетная. Бумага мелованная.
Тираж 300 экз. Заказ № 381311/1

Отпечатано в типографии ООО «Вива-Стар».
107023, г. Москва, ул. Электрозаводская, д. 20, стр. 3