

УДК 336.719
EDN: QROTEF
DOI: 10.65891/2949-1983-2026-22-3-35-37



©2026 Контент доступен по лицензии CC BY-NC 4.0
This is an open access article under the CC BY-NC 4.0 license
(https://creativecommons.org/licenses/by-nc/4.0/)

НЕЙРОСЕТЕВЫЕ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТ ДЛЯ ЗАЩИТЫ ДАННЫХ В БАНКОВСКОМ СЕКТОРЕ

ЧЕБАН Маргарита Анатольевна, кандидат экономических наук, начальник управления научных исследований
Поволжский государственный университет сервиса
445017, Россия, Тольятти, margo-555@yandex.ru

SPIN: 7921-2825
ORCID: 0009-0009-2349-4190
AuthorID: 1198832

ПОПОВ Артемий Александрович, студент-магистрант
Поволжский государственный университет сервиса
445017, Россия, Тольятти

НИКИФОРОВ Артём Юрьевич, студент-бакалавр
Поволжский государственный университет сервиса
445017, Россия, Тольятти, artem12092007tlt@gmail.com

Аннотация. В статье проводится анализ нейросетевых технологий и систем искусственного интеллекта, которые используются для защиты данных в российском банковском секторе в период с 2023 по 2025 год. Отмечено, что крупнейшие финансовые институты переходят от покупки готовых вендорских решений к созданию собственных ИИ-платформ и формируют автономный «цифровой иммунитет». На основе официальных отчетов шести коммерческих банков (Сбербанк, ВТБ, Альфа-Банк, Т-Банк, Россельхозбанк, Газпромбанк) проведено сравнение различных стратегических моделей – от тотальной автоматизации до глубокой проверки безопасности ИТ-инфраструктуры. Сделан вывод о том, что внедрение мультиагентных систем, большого количества языковых моделей (LLM) и алгоритмов машинного обучения позволяет достичь точности детекции киберугроз до 93–99 %, многократно сократить время реакции на проблему, а также минимизировать финансовые потери от мошенничества и социальной инженерии. В работе показана эффективность проактивного подхода к информационной безопасности для защиты конфиденциальных данных от угроз.

Ключевые слова: цифровой иммунитет, киберинциденты, банковский сектор, защита данных, автоматизация кибербезопасности, импортозамещение в ИТ.

© Чебан М.А., Попов А.А., Никифоров А.Ю., 2026

NEURAL NETWORK TECHNOLOGIES AS A TOOL FOR DATA PROTECTION IN THE BANKING SECTOR

CHEBAN Margarita Anatolyevna, Candidate of Economic Sciences, Head of the Scientific Research Department
Volga State University of Service

445017, Russia, Togliatti, margo-555@yandex.ru

POPOV Artemiy Aleksandrovich, Master's student
Volga State University of Service

445017, Russia, Togliatti,

NIKIFOROV Artyom Yurevich, bachelor's student
Volga State University of Service

445017, Russia, Togliatti, artem12092007tlt@gmail.com

Abstract. The article analyzes how neural network technologies and artificial intelligence systems are used to protect data in the Russian banking sector between 2023 and 2025. It is evident that major financial institutions are moving from purchasing ready-made vendor solutions to creating their own AI platforms and building an autonomous “digital immunity”. Based on official reports from six large commercial banks (Sber, VTB, Alfa-Bank, T-Bank, Rosselkhozbank, Gazprombank), a comparison was made of various strategic models – from total automation to in-depth security testing of IT infrastructure. It is evident that the implementation of multi-agent systems, a large number of language models (LLM) and machine learning algorithms makes it possible to achieve a detection accuracy of cyber threats of up to 93–99 %, significantly reduce the response time to a problem, and minimize financial losses from fraud and social engineering. The paper demonstrates the effectiveness of a proactive approach to information security for protecting confidential data from threats.

Keywords: digital immunity, cyber incidents, banking sector, data protection, cybersecurity automation, import substitution in IT.

© Cheban M.A., Popov A.A., Nikiforov A.Yu., 2026

ВВЕДЕНИЕ

Цифровая трансформация банковского сектора, сопровождающаяся быстрым ростом объемов обрабатываемой информации, превратила данные в один из ключевых стратегических активов. Финансовый сектор сегодня является одновременно локомотивом и испытательным полигоном для внедрения технологий искусственного интеллекта. Как отмечает Руслан Искяндяров, «ИИ пронизывает практически все сферы деятельности банков – от клиентских чат-ботов и голосовых помощников до сложных антифрод-систем, работающих на основе больших данных и машинного обучения» [1]. По оценке директора по инновациям Банка «Уралсиб» Дмитрия Гришина, «консолидированный экономический эффект от использования ИИ в отрасли достигает 5–7 % доходов» [1]. Есть и обратная сторона: пока банки активно внедряют цифровые технологии, они остаются

ся главной целью для хакеров. Утечка личных данных клиентов может стоить миллионы рублей, а если что-то сломается в критически важных системах, клиенты перестанут доверять всей цифровой системе. По данным Т-Банка, только в 2023 году злоумышленники пытались похитить со счетов клиентов более 21 млрд рублей [2].

В такой ситуации старые методы защиты, вроде DLP-систем с их жесткими правилами и систем, которые реагируют только на уже случившиеся атаки, не справляются с постоянно меняющимися угрозами. Их точность редко превышает 70 %, а попытки повышения за счёт ручной настройки политик ведут к большому объёму ложных срабатываний [2]. В ответ на этот вызов возникает острая необходимость перехода от реактивной защиты к проактивной и автономной.

Иллюстрацией качественного перехода на корпоративном уровне служит опыт Сбербанка, где CNN и RNN

(два основных типа искусственных нейросетей, которые используются для решения разных задач) алгоритмы обработки естественного языка (NLP) и методов математической статистики позволили повысить точность обнаружения защищаемых данных до 95–99 % и сократить время реакции на инциденты более чем в 20 раз [3]. В настоящее время мультиагентные системы на базе ИИ, внедрённые в Сбербанк, способны в автономном режиме обрабатывать до 70 % «киберинцидентов», формируя адаптивный «цифровой иммунитет». Это и определяет актуальность статьи.

МЕТОДОЛОГИЯ

Цель данного исследования – проанализировать на примере современных банковских решений и инновационных научных разработок, как банковский сектор защищает клиентов и информацию от современных угроз с использованием искусственного интеллекта.

В основе данного исследования использован метод сравнительного анализа. Основными источниками исследования послужили официальные отчеты шести крупнейших коммерческих банков (Сбербанк, ВТБ, Альфа-Банк, Т-Банк, Россельхозбанк, Газпромбанк) за период 2023–2025 гг. На первом этапе осуществлялся сбор и качественная фильтрация данных, направленная на выявление специфики применения конкретных ИИ-технологий (CNN, RNN, LLM, мультиагентные системы) для обеспечения информационной безопасности и защиты данных от современных киберугроз.

После этого весь собранный материал был перенесен в таблицу по четырем критериям: технологический стек, примеры практического внедрения, результаты и ключевые преимущества. Это позволило выявить уникальные стратегические модели защиты данных для каждого банка: от полной технологической независимости до тотальной автоматизации процессов. Заключительный этап включал сопоставление заявленных метрик эффективности (точность детекции угроз до 93–99 %, сокращение времени реакции на инциденты и достигнутый экономический эффект) для оценки устойчивости формируемого банками «цифрового иммунитета». Ограничением работы является фокус исключительно на крупнейших игроках финансового сектора, обладающих ресурсами для разработки собственных суверенных ИИ-платформ.

РЕЗУЛЬТАТЫ

Анализ российского банковского сектора показывает, что крупные игроки активно переходят от покупки готовых решений к созданию собственных ИИ-платформ. Особенно заметен тренд на формирование «цифрового иммунитета» – способности банка не просто реагировать на угрозы, а предупреждать их в автоматическом режиме [4; 5].

Таблица 1. Используемые ИИ в коммерческих банках
Table 1. AI technologies used in commercial banks

Банк	Используемые ИИ-технологии	Конкретные примеры внедрения	Ключевые преимущества и результаты
Сбербанк	Суверенный генеративный ИИ, LLM (GigaChat), мультиагентные системы, компьютерное зрение (CNN, RNN), NLP	Платформа GigaChat, ИИ-системы, «цифровой иммунитет», обработка естественного языка для документов	Полный контроль над шлом обучения ИИ (Pre-train) обеспечивает устойчивость и суверенитет [3]. Точность обнаружения угроз до 99 %, автоматическое отражение до 70 % инцидентов [4].
ВТБ	Собственные ИИ-алгоритмы для кибербезопасности, анализ социально-демографических данных	Системы защиты от социальной инженерии, транзакций, выявления атак	Эффективный переход от вендорских решений к собственной разработке (key import substitution), выявление нетипичного поведения клиента в реальном времени [6; 7].
Альфа-Банк	Генеративный ИИ (GenAI), технология Deep Research, LLM (GPT-OSS-120B)	Платформа AlfiGen (аналитик на базе ИИ), внутренние ассистенты	Автоматизация рутинной аналитики, являясь «сней работ» аналитиков. Технологии позволяют самостоятельно собирать и проверять данные, готовя структурированные отчеты за 15–20 минут [8; 9].
Т-Банк	Искусственный интеллект для скрининга, автоматический анализ данных из интернета	Автоматическая оценка ТСП при овербординге к эквайрингу, антифрод-платформа	Точность проверок достигает 93 % (отличный показатель для рисков мошенничества). «Бесшовный» овербординг (автоматическое подключение) для 99 % клиентов [10].
Россельхозбанк	MLOps-платформа RAISA (Lakehouse, Airflow), модели прогнозирования, LLM	Система управления остатками наличных (касса банкомата), скрининг кредитных конвейеры	Экономический эффект от оптимизации операционной деятельности подтвержден цифрами (~700 млн руб. в год). Платформа объединяет более 3000 сотрудников (от дата-сайентистов до аналитиков) [11].
Газпромбанк	LLM для статического и динамического анализа кода (DevSecOps), детекция аномалий	Проверка безопасности приложений, защита API, мониторинг пользовательского поведения	Сокращение времени на анализ уязвимостей за счет фильтрации ложных срабатываний. Формирование безопасных сценариев проверки инфраструктуры [12].

По данным таблицы 1 отметим, что используется ИИ в каждом коммерческом банке по-разному. Сбербанк, как огромный завод, который делает всё сам, имеет собственный большой генеративный ИИ (GigaChat). Самое главное – это полный контроль над процессом обучения, чтобы не зависеть от иностранных программ. ВТБ, в отличие от Сбербанка, использует стратегию целенаправленного импортозамещения, сконцентрировавшись на безопасности и отказе от чужих решений. Альфа-Банк активно применяет передовые языковые модели, что позволяет ему выполнять задачи, ранее занимавшие у живых аналитиков несколько дней, всего за 15–20 минут. Это показывает, что ИИ стал незаменимым помощником. В Т-БАНК большая часть предпринимателей работают через эквайринг автоматически. И при этом система с огромной вероятностью выявляет различия в управлении потоками и персоналом. АО «Россельхозбанк» создал платформу RAISA для 3000 сотрудников – от аналитиков до экспертов кибербезопасности. Общая среда для финансового моделирования и прогнозирования загрузки банкоматов сэкономила около 700 млн рублей. ПАО «Газпромбанк» использует ИИ для автоматической проверки кода на уязвимости и фильтрации ложных срабатываний. Это позволило ускорить процессы обеспечения кибербезопасности, минимизируя участие программистов.

Таким образом, ПАО «Сбербанк» реализует принцип полной технологической независимости, Т-Банк делает ставку на максимальную скорость процессов и тотальную автоматизацию без участия человека, Банк «Альфа-Банк» ориентирован на поддержку рутинных когнитивных операций, ВТБ и Газпромбанк акцентируют усилия на разработке «интеллектуальной охраны» и систем киберзащиты, создаваемых собственными силами, без использования внешних коммерческих решений.

ВЫВОДЫ

Проведённый анализ использования нейросетевых технологий в российском банковском секторе за 2023–2025 гг. позволяет утверждать, что отрасль совершила качественный переход от реактивной защиты информации к проактивному формированию «цифрового иммунитета». Традиционные DLP-решения и статические правила уступают место мультиагентным системам, большим языковым моделям (LLM) и генеративному ИИ, которые демонстрируют точность детекции киберугроз на уровне 93–99 % и сокращают время реагирования на инциденты в десятки раз.

Исследование показало, что крупнейшие банки (Сбербанк, ВТБ, Альфа-Банк, Т-Банк, Россельхозбанк, Газпромбанк) последовательно отказываются от покупных вендорских решений в пользу собственных суверенных ИИ-платформ. Финансовые учреждения выбирают индивидуальные пути внедрения искусственного интеллекта. Варианты контроля за ИИ могут очень сильно различаться от полной автоматизации до тотального контроля.

Эволюция в сфере киберзащиты за последние несколько лет показала возможности российского банковского сектора быстро и точно менять «классические» методы обнаружения на точную нейтрализацию большого количества киберинцидентов, исключая участие человека. Это позволило сократить финансовые потери, которые были связаны с мошенническими действиями, что являлось очень важной статьёй потерь, особенно во время экономической нестабильности. Проблемой в настоящее время является новизна и, вследствие, дороговизна технологии, она доступна только самым крупным банкам, которые могут позволить выделить бюджеты соответствующего уровня на развитие и внедрение.

Нейросетевые технологии зарекомендовали себя одним из стратегически важным инструментом для обеспечения безопасности данных в российском банковском секторе. В будущем «цифровой иммунитет» будет укрепляться в основном внедрением LLM-агентов на

средние и малые финансовые организации, а также федеративного обучения, которое даст возможность обрабатывать конфиденциальные данные без необходимости их хранения.

СПИСОК ЛИТЕРАТУРЫ

1. Как искусственный интеллект изменил работу банков и финансовых организаций [Электронный ресурс] IQ Media. – 2024. – 18 декабря. – URL: <https://iq-media.ru/news/4593>
2. Кибермошенники украли почти 16 млрд рублей у россиян в 2023 году [Электронный ресурс] Forbes. – 2024. – 13 февраля. – URL: <https://www.forbes.ru/finansy/506131-kibermosenniki-ukrali-pochti-16-mlrd-rublej-u-rossiyan-v-2023-godu>
3. ИИ на страже банковских данных [Электронный ресурс] СберБанк. – URL: https://www.sberbank.ru/ru/person/kibrary/experts/ii_na_strazhe_bankovskih_dannyh_2
4. Политика допустимого использования ИИ-сервисов ПАО Сбербанк [Электронный ресурс] СберБанк. – URL: <https://developers.sber.ru/docs/ru/policies/gigachat-agreement/permisible-use-ai>
5. В Сбере объяснили зачем делают суверенный ИИ [Электронный ресурс] ТКС.PV. – 2026. – 24 марта. – URL: <https://www.tks.ru/politics/2026/03/24/0005/>
6. Альфа-Банк запустил ИИ-технологию «глубокого исследования» для бизнес-аналитики [Электронный ресурс] Bankinform.ru. – 2026. – 28 января. – URL: <https://bankinform.ru/news/140458>
7. Как выстроить гибкий и быстрый онбординг [Электронный ресурс] PlusWorld.ru. – 2026. – 15 апреля. – URL: <https://plusworld.ru/articles/71422/>
8. Смирнов Н. РСХБ: ИИ и аналитика на единой платформе [Электронный ресурс] Открытые системы. СУБД. – 2026. – 2 апреля. – URL: <https://osp.ru/articles/2026/0402/13060648>
9. Банки внедряют ИИ-алгоритмы для защиты от мошенников [Электронный ресурс] ГТРК «Волгоград-ТРВ». – 2026. – URL: <https://volgograd-trv.ru/news/obschestvo/101596-banki-vnedrajut-ii-algoritmy-dlja-zaschity-ot-moshennikov.html>
10. В России ИИ сможет собирать и анализировать информацию [Электронный ресурс] IT Russia. – 2026. – 28 января. – URL: <https://itrussia.media/ru/article/v-rossii-ii-smozhet-sobirat-i-analizirovat-inform-28-01-2026>
11. Газпромбанк Tech. Блог [Электронный ресурс]. – URL: <https://www.gazprombank.tech/blog/1467/>
12. Николаева, М. О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации / М. О. Николаева // Мониторинг. Образование. Безопасность. – 2023. – № 1(1). – С. 51–57. – EDN IOIQDI.
13. Метод приоритизации рисков информационной безопасности для реагирования на инциденты информационной безопасности / А. К. Амренов, А. М. Нурушева, Д. К. Токсеит, Н. Горанин // Труды университета. – 2025. – № 2(99). – С. 364–370. – DOI 10.52209/1609-1825_2025_2_364. – EDN WKUDAY.

REFERENCES

1. How artificial intelligence has changed the work of banks and financial organizations [Electronic resource] IQ Media. – 2024. – December 18. – URL: <https://iq-media.ru/news/4593>
2. Cybercriminals stole almost 16 billion rubles from Russians in 2023 [Electronic resource] Forbes. – 2024. – February 13. – URL: <https://www.forbes.ru/finansy/506131-kibermosenniki-ukrali-pochti-16-mlrd-rublej-u-rossiyan-v-2023-godu>
3. AI on guard of banking data [Electronic resource] SberBank. – URL: https://www.sberbank.ru/ru/person/library/experts/ii_na_strazhe_bankovskih_dannyh_2
4. Policy on Permissible Use of AI Services of PJSC Sberbank [Electronic resource] Sberbank. – URL: <https://developers.sber.ru/docs/ru/policies/gigachat-agreement/permisible-use-ai>
5. Sber explained why they are developing sovereign AI [Electronic resource] TKSRU. – 2026. – March 24. – URL: <https://www.tks.ru/politics/2026/03/24/0005/>
6. Alfa-Bank launched AI technology for “deep research” for business analytics [Electronic resource] Bankinform.ru. – 2026. – January 28. – URL: <https://bankinform.ru/news/140458>
7. How to build flexible and fast onboarding [Electronic resource] PlusWorld.ru. – 2026. – April 15. – URL: <https://plusworld.ru/articles/71422/>
8. Smirnov N. RSHB: AI and analytics on a single platform [Electronic resource] Open Systems. DBMS. – 2026. – April 2. – URL: <https://osp.ru/articles/2026/0402/13060648>
9. Banks are implementing AI algorithms to protect against fraudsters [Electronic resource] GTRK “Volgograd-TRV”. – 2026. – URL: <https://volgograd-trv.ru/news/obschestvo/101596-banki-vnedrajut-ii-algoritmy-dlja-zaschity-ot-moshennikov.html>
10. In Russia, AI will be able to collect and analyze information [Electronic resource] IT Russia. – 2026. – January 28. – URL: <https://itrussia.media/ru/article/v-rossii-ii-smozhet-sobirat-i-analizirovat-inform-28-01-2026>
11. Gazprombank Tech. Blog [Electronic resource]. – URL: <https://www.gazprombank.tech/blog/1467/>
12. Nikolaeva, M. O. Information Security: The Current State of the Problem of Information Security and Information Protection / M. O. Nikolaeva // Monitoring. Education. Safety. – 2023. – No. 1(1). – Pp. 51–57. – EDN IOIQDI.
13. Method for prioritizing information security risks to respond

to information security incidents / A. K. Amrenov, A. M. Nurusheva, D. K. Tokseit, N. Goranin // Proceedings of the University. – 2025. – No. 2(99). – Pp. 364–370. – DOI 10.52209/1609-1825_2025_2_364. – EDN WKUDAY.

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Заявленный вклад авторов:

Чебан М. А. – постановка проблемы, разработка методики исследования, формулирование выводов, научное редактирование.

Попов А. А. – группировка банков, анализ отраслевых отчетов, анализ направлений применения ИИ, оформление библиографии.

Никифоров А. Ю. – сбор и обработка статистических данных, подготовка таблиц, работа с нормативными источниками.

Интерпретация результатов и формулирование выводов выполнены авторами совместно.

The stated contribution of the authors:

Cheban M. A. – problem definition, development of research methodology, formulation of conclusions, scientific editing.

Popov A. A. – grouping of banks, analysis of industry reports, analysis of AI application areas, compilation of the bibliography.

Nikiforov A. Yu. – collection and processing of statistical data, preparation of tables, and work with regulatory sources.

The interpretation of the results and the formulation of the conclusions were carried out jointly by the authors.

Received date: 09.09.2026

Approved date: 24.09.2026

Accepted date: 29.09.2026