https://doi.org/10.24182/2073-9885-2025-18-3-20-25

Обзорная статья / Review article
УДК 336.71:004.8

Обеспечение безопасности в банковских транзакциях при помощи искусственного интеллекта

А. А. Недбаев
Магистр
snedbaev68@yandex.ru
Кафедра экономики,
Тамбовский государственный технический университет,
Тамбов, Россия

С. П. Спиридонов
Доктор экономических наук, профессор
spiridonov_sp@bk.ru
Кафедра экономики,
Тамбовский государственный технический университет,
Тамбов, Россия

Аннотация: *В статье рассмотрены современные возможности обеспечения безопасности банковских транзакций с применением технологий искусственного интеллекта (ИИ). Проанализированы методы машинного обучения для предотвращения мошеннических действий по отношению к пользователю, а также были изучены преимущества и недостатки внедрения ИИ в банковскую сферу.*

Ключевые слова: *искусственный интеллект, банковские операции, безопасность, машинное обучение, мошенничество.*

Для цитирования: *Недбаев А.А., Спиридонов С.П. Обеспечение безопасности в банковских транзакциях при помощи искусственного интеллекта. Путеводитель предпринимателя. 2025. Т. 18. № 3. С. 20–25. https://doi.org/10.24182/2073-9885-2025-18-3-20-25.*

Enhacing security in banking transactions using artificial intelligence

A. A. Nedbaev
Masterstudent
snedbaev68@yandex.ru
Department of Economics,
Tambov State Technical University,
Tambov, Russia

S. P. Spiridonov
Dr. Sci. (Econ.), Prof.
spiridonov_sp@bk.ru
Department of Economics,
Tambov State Technical University,
Tambov, Russia

Abstract: *The paper explores modern approaches to securing banking transactions through artificial intelligence (AI) technologies. Machine learning methods for preventing fraudulent activities against users are analyzed, along with the advantages and disadvantages of implementing AI in the banking sector.*

Keywords: *artificial intelligence, banking transactions, security, machine learning, fraud.*

For citation: *Nedbaev A.A., Spiridonov S.P. Enhacing security in banking transactions using artificial intelligence. Entrepreneur's Guide. 2025. Т. 18. № 3. P. 20–25. https://doi.org/10.24182/2073-9885-2025-18-3-20-25.*

Введение

В современных реалиях банковскому сектору приходится сталкиваться с трудностями в области кибербезопасности. С каждым годом, если даже не кварталом мошенники придумывают новые способы воровства средств или же их получения обманным путем, в связи с этим требуются и новые способы защиты. Традиционные методы защиты, например, двухфакторная аутентификация, уже не в полной мере справляются с растущими угрозами как раньше. Применение искусственного интеллекта (ИИ) становится одним из ключевых факторов возможности защиты данных и денежных средств. В данной статье будут рассматриваться основные угрозы, методы их минимизации, а также преимущества и перспективы развития ИИ в банковском секторе.

Обзор методов обеспечения безопасности

Обеспечение безопасности банковских транзакций является одной из ключевых задач для любых финансовых учреждений. Существуют традиционные и современные методы обеспечения безопасности, по мере развития цифровых технологий и увеличения объема онлайн-операций традиционные методы уже не могут гарантировать такую безопасность как современные, в которых уклон идет на использование возможностей и преимуществ искусственного интеллекта [1].

К традиционным методам относят двухфакторную аутентификацию (2FA), SSL-шифрование и использование CAPTCHA.

Двухфакторная аутентификация представляет собой проверку пользователя на нескольких уровнях, как правило, это ввод пароля и одноразового кода, который отправляется владельцу аккаунта на мобильный телефон или почту. Её преимуществом служит простота внедрения и использования, а недостатками — отсутствие защиты при получении злоумышленниками доступа к обоим факторам, а также неудобен, если у пользователя в данный момент времени недоступен один из факторов аутентификации.

SSL-шифрование простыми словами является протоколом шифрования, который обеспечивает безопасную передачу данных между клиентом и сервером.[2] Его преимуществами являются поддержка большинством серверов и браузеров, а также конфиденциальность данных при передаче. Недостатком является уязвимость при атаках на серверы или же сами приложения.

Использование CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) — технология, которая помогает отличить человека от бота, обычно являющаяся простым тестом с вводом текста или выполнением задания.[3] Она проста во внедрении и предотвращает автоматические атаки, но создает неудобства пользователям и не защищает от сложных атак.

Современными методами обеспечения безопасности являются применение машинного обучения и обнаружение аномалий при помощи нейронных сетей.

Машинное обучение (ML) позволяет создавать модели, которые выявляют отклонение поведения пользователя от привычного ему. Они достаточно точны в работе, могут адаптироваться к новым видам атак, однако они все же могут ошибиться, например, когда пользователь обычно совершает небольшие транзакции, но однажды ему понадобилось перевести крупную сумму в другой регион, и в таком случае транзакция может быть заблокирована.

---

[1] Аликина Е. Как искусственный интеллект работает в банках: статья / Аликина Е. Frank Media, [Электронный ресурс], 2020. — URL: https://frankmedia.ru/24564 (дата обращения: 04.05.2025).

[2] Авторская трактовка.

[3] Авторская трактовка.

Обнаружение аномалий с помощью нейронных сетей используются для выявления сложных повторений в данных, они анализируют сотни и тысячи параметров транзакций. В использовании они прогнозируют будущие угрозы, опираясь на исторические данные, а также точно могут обнаружить сложные аномалии.

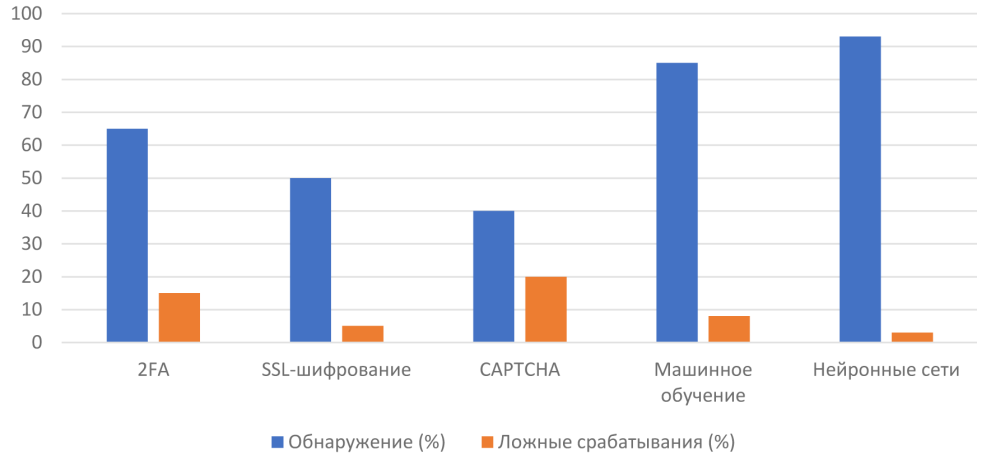

Рис. 1. Сравнение эффективности методов защиты банковских транзакций [4]

Для наглядности можно рассмотреть гистограмму, чтобы понять эффективность того или иного способа.

По сравнению с традиционными современные методы обрабатывают большие объёмы данных, они являются более гибкими к новым видам атак, у них реже происходят ложные срабатывания, к тому же они могут еще и спрогнозировать угрозы.

Основные угрозы в банковских транзакциях

Мошенники используют всё более и более изощренные методы обхода систем безопасности, а их угрозы становятся более сложными для предотвращения, поэтому банки вынуждены постоянно совершенствовать свои механизмы защиты. Следует рассмотреть основные угрозы, с которыми сейчас сталкивается банковский сектор [5].

Фишинг — наиболее распространённый вид финансового мошенничества, в данном случае злоумышленник нацелен на получение конфиденциальных данных своей жертвы, например, логин, пароль, номер кредитной карты и PIN-код. Для этого создаются поддельные сайты, которые в точности повторяют официальные, отправляются сообщения со ссылками, при переходе на которые данные передаются.

Мошеннические транзакции — это операции, которые совершаются с использованием украденных данных. Для этого может быть применен тот же фишинг, скимминг (установка специального устройства на банковский аппарат, который считывает данные с магнитной полосы карт) и взлом баз данных, чтобы получить информацию о клиентах.

Атаки на банковские системы — взлом серверов и баз данных банков для получения доступа к финансовой информации. DDoS атаки — это перегрузка серверов объёмом запросов с последующим их отказом в обслуживании; взлом баз данных; внедрение вредоносного ПО.

Социальная инженерия — метод манипуляции людьми с целью получения доступа к их конфиденциальной информации. Самым ярким примером служат звонки, которые поступают якобы от сотрудников ФСБ или банка с требованием перевода средств на безопасные счета, потому что якобы в данный момент их деньгам что-то угрожает.

---

[4] https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_банках (дата обращения: 04.05.2025).

[5] Янковский Р.М. Государство и криптовалюты: проблемы регулирования. Московский государственный университет, [Электронный ресурс], 2017. — URL: http://msu.edu.ru/papers/yankovskiy/blockchain.pdf (дата обращения: 04.05.2025).

Все эти угрозы становятся всё более сложными и предоставляют всё большую опасность для пользователей, что требует от банков совершенствования своих защитных механизмов. Использование современных технологий помогает банкам не только обнаруживать, но и предотвращать угрозы, тем самым обеспечивая безопасность транзакций и данных своих клиентов.

Адаптивная многофакторная система защиты на основе искусственного интеллекта (ИИ) и блокчейна

Адаптивная аутентификация — это процесс, похожий на двухфакторную аутентификацию, но только уровень проверки пользователя зависит от уровня риска транзакции. ИИ должен проанализировать поведение пользователя, устройство, местоположение пользователя и тип транзакции для определения необходимости дополнительной аутентификации. Например, если происходит транзакция из привычного места и на знакомом устройстве, то система может ограничить пользователя однофакторной аутентификацией, а если с нового устройства, то будет запрошена дополнительная проверка [6].

Блокчейн [7] представляет собой децентрализованную цифровую технологию хранения и передачи данных, которая основана на принципах криптографии. В предлагаемой системе защиты блокчейн необходим для записи всех транзакций, чтобы обеспечить их прозрачность, это позволит отследить все операции и выявить подозрительные активности. Нельзя будет изменить данные о транзакции.

Блокчейн не имеет центрального сервера, что устраняет единую точку отказа, данные хранятся на большом количестве узлов, это делает систему более устойчивой к кибератакам, потому что при взломе одного из узлов, остальные все еще будут хранить данные. Также блокчейн может быть использован для создания децентрализованных систем аутентификации, чтобы пользователи хранили свои данные в зашифрованном виде и управлялись при помощи приватных ключей.

Благодаря прозрачности снизится риск мошеннических операций, обработка транзакций будет происходить гораздо быстрее, особенно если речь идет о международных переводах, будет упрощен аудит.

Рассчитаем эффективность внедрения данного метода защиты. Необходимо отметить, что для наглядности расчетов тарифы были усреднены и округлены.

Опираясь на данные Accenture, от мошенничества банки теряют порядка 6% от годового оборота транзакций, следовательно, для банка с оборотом в 1 млрд. $ потери составят около 60 млн. $ в год. [8] Адаптивная аутентификация снизит атаки на 55% [9], блокчейн снизит потери от мошеннических действий на 40% [10] за счёт прозрачности и отсутствия возможности изменять данные.

$$60\,\text{млн.\$} \times (1 - 0.55) \times (1 - 0.4) = 16.2\,\text{млн.\$}$$

$$60 - 16.2 = 43.8\,\text{млн.\$/год}.$$

Экономия в районе 43.8 млн.$ от уменьшения мошеннических махинаций.

Традиционные международные переводы могут занимать несколько дней и взимать большую комиссию, однако при внедрении блокчейн решения перевод будет занимать секунды, а ко-

[6] Чернышова Е. Искусственный интеллект в финансах: как банки используют нейросети: статья / Чернышова Е. Газета РБК, [Электронный ресурс], 2023. — URL https://trends.rbc.ru/trends/industry/61e924349a7947761b46f2d8 (дата обращения: 04.05.2025).

[7] Авторская трактовка.

[8] Accenture. Отчет по безопасности 2023: Опережая киберугрозы в финансовом секторе, [Электронный ресурс], 2023. — URL: https://www.accenture.com/ru-ru/insights/security/cyber-resilience-financial-services (дата обращения: 05.05.2025).

[9] Accenture. Технологическое видение банковского сектора 2023: ИИ и будущее обнаружение мошенничества, [Электронный ресурс], 2023. — URL: https://www.accenture.com/ru-ru/insights/banking/technology-vision (дата обращения: 05.05.2025).

[10] Accenture. Стоимость киберпреступности в финансовых услугах, [Электронный ресурс], 2022. — URL: https://www.accenture.com/ru-ru/insights/security/cost-cybercrime-financial-services (дата обращения: 05.05.2025).

миссия составит 0.05$. Для наглядности возьмем усредненную комиссию в 50$ при традиционном способе и 10000 переводов в месяц.

$$(50 - 0.05) \times 10\,000 = 499\,500\ \$/\text{мес.}$$

$$499\,500 \times 12 = 5.994\ \text{млн.}\ \$/\text{год.}$$

Получаем экономию в размере 5.994 млн.$/год, и это без учета ускорения времени на перевод, что снизит операционные издержки банка.

В среднем банки тратят на ручной аудит до миллиона долларов, блокчейн автоматизирует верификацию клиентов и отслеживание транзакций, что составляет 70% от затрат, экономия составляет в районе 700.000$. Следует добавить стоимость внедрения системы блокчейна, которая будет составлять 200.000$/год амортизации, экономия образуется в размере 500.000$.

Усредненно традиционные методы ложно срабатывают в 15% случаях, за счёт анализа поведения ИИ снижает это до 4%, при 1 млн. транзакций в год на 100 $ – 11 млн. $/год экономии только на снижении количества ложных срабатываний.

$$499\,500 \times 12 = 5.994\ \text{млн.}\ \$/\text{год.}$$

При реализации проекта сроком 5 лет, ставки дисконтирования в 10% и первоначальных инвестициях в 5 млн. $ денежные потоки от экономии будут составлять 71.174 млн. $ в год. Это необходимо для расчета чистой приведённой стоимости.

Таблица 1

Эффективность внедрения предложенного метода за 1 год [11]

Параметр	Экономия ($)/год
Уменьшение мошенничества	43.800.000
Изменение переводов	5.994.000
Сокращение аудита	500.000
Уменьшение ложных отказов	11.000.000
Всего	61.294.000

Внедрение адаптивной аутентификации и блокчейна смогут создать долгосрочные конкурентные преимущества и сэкономить банку немалые средства.

Таким образом, блокчейн и адаптивная многофакторная аутентификация помогут обеспечить более высокий уровень защиты данных и операций пользователей, снизят потери банков от действий мошенников, клиенты получат более быстрые транзакции. Стоит отметить, что показатели, связанные с количеством операций и их стоимость были усреднены для более понятного и наглядного примера, потому что для каждого банка показатели будут варьироваться из-за разных комиссий или разного количества пользователей и операций.

Заключение

В статье показано, что применение ИИ значительно повышает уровень безопасности банковских транзакций и данных клиентов. Предложенная система защиты поможет обеспечить прозрачную модель проведения банковских операций и сохранить данные клиентов в безопасности. Значительно повышается эффективность работы банков путем автоматизации процессов, улучшения обнаружения мошенничества, появления новых персональных услуг и работы клиентского сервиса. Все это позволяет не только увеличить конкурентоспособность, но и сэкономить большие денежные суммы, что увеличивает прибыльность. Банковскому сектору необходимо делать акцент на внедрении искусственного интеллекта в свою деятельность.

[11] Расчеты авторов.

Список литературы

1. Янковский Р.М. Государство и криптовалюты: проблемы регулирования. Московский государственный университет [Электронный ресурс], 2017. – URL: http://msu.edu.ru/papers/yankovskiy/blockchain.pdf (дата обращения: 04.05.2025).
2. Аликина Е. Как искусственный интеллект работает в банках: статья / Аликина Е. Frank Media, [Электронный ресурс] 2020. – URL: https://frankmedia.ru/24564 (дата обращения: 04.05.2025).
3. Чернышова Е. Искусственный интеллект в финансах: как банки используют нейросети: статья / Чернышова Е. Газета РБК, [Электронный ресурс]. 2023. – URL: https://trends.rbc.ru/trends/industry/61e924349a7947761b46f2d8 (дата обращения: 04.05.2025).
4. https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_банках (дата обращения: 04.05.2025).
5. Accenture. Отчет по безопасности 2023: Опережая киберугрозы в финансовом секторе [Электронный ресурс]. 2023. – URL: https://www.accenture.com/ru-ru/insights/security/cyber-resilience-financial-services (дата обращения: 05.05.2025).
6. Accenture**.** Технологическое видение банковского сектора 2023: ИИ и будущее обнаружения мошенничества [Электронный ресурс]. 2023. – URL: https://www.accenture.com/ru-ru/insights/banking/technology-vision (дата обращения: 05.05.2025).
7. Accenture. Стоимость киберпреступности в финансовых услугах [Электронный ресурс]. 2022. – URL: https://www.accenture.com/ru-ru/insights/security/cost-cybercrime-financial-services (дата обращения: 05.05.2025).

References

1. Yankovsky, R.M. The state and cryptocurrencies: Problems of regulation. Moscow State University. 2017 URL: http://msu.edu.ru/papers/yankovskiy/blockchain.pdf (date of access: 04.05.2025) – Text: electronic.
2. Alikina, E. How artificial intelligence works in banks. Frank Media. 2020. – URL: https://frankmedia.ru/24564 (date of access: 04.05.2025) – Text: electronic.
3. Chernyshova, E. Artificial intelligence in finance: How banks use neural networks, RBK Newspaper. 2023. – URL: https://trends.rbc.ru/trends/industry/61e924349a7947761b46f2d8 (date of access: 04.05.2025) – Text: electronic.
4. https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_банках (date of access: 04.05.2025) – Text: electronic.
5. Accenture. Security Report 2023: Staying Ahead of Cyber Threats in the Financial Sector. 2023. – URL: https://www.accenture.com/ru-ru/insights/security/cyber-resilience-financial-services (date of access: 05.05.2025). – Text: electronic.
6. Accenture. Banking Technology Vision 2023: AI and the Future of Fraud Detection. 2023. – URL: https://www.accenture.com/ru-ru/insights/banking/technology-vision (date of access: 05.05.2025) – Text: electronic.
7. Accenture. *The Cost of Cybercrime in Financial Services.* 2022. – URL: https://www.accenture.com/ru-ru/insights/security/cost-cybercrime-financial-services. (date of access: 05.05.2025) – Text: electronic.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.

Authors' contribution: All authors have made an equivalent contribution to the preparation of the article for publication.

Авторы заявляют об отсутствии конфликта интересов.

The authors declare that there is no conflict of interest.

Статья поступила в редакцию 24.05.2025; одобрена после рецензирования 17.06.2025; принята к публикации 20.06.2025.

The article was submitted 24.05.2025; approved after reviewing 17.06.2025; accepted for publication 20.06.2025.