DOI 10.37882/2223-2966.2024.6-2.02

ВЛИЯНИЕ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА БЕЗОПАСНОСТЬ БЕЗНАЛИЧНЫХ ПЛАТЕЖЕЙ

THE IMPACT OF THE APPLICATION OF ARTIFICIAL INTELLIGENCE ON THE SECURITY OF NON-CASH PAYMENTS

D. Abdourahman

Summary. The rapid shift from cash to cashless payment methods has transformed the financial industry, creating unprecedented convenience as well as significant security concerns. In response to increasingly sophisticated cyber threats, the use of artificial intelligence (AI) in securing payment systems has become critical. The use of artificial intelligence (AI) in cashless payments has revolutionized the security of cashless payments, providing increased security and efficiency to payment processes. This article explores the profound impact of artificial intelligence on cashless payment security, focusing on its role in fraud detection, prevention and authentication techniques. However, this article also examines the transformative impact of AI on the security of payment systems, discussing its benefits, challenges and future prospects.

Keywords: artificial intelligence; cybersecurity; non-cash payments; machine learning; deep learning; natural language processing.

Абдурахман Джамал Джама
Аспирант, Финансовый Университет при Правительстве РФ, г. Москва, Россия
jamaljolevas14psg@gmail.com

Аннотация. Быстрый переход от наличных к безналичным методам оплаты изменил финансовую отрасль, создав беспрецедентное удобство, а также серьезные проблемы с безопасностью. В ответ на все более сложные киберугрозы применение искусственного интеллекта (ИИ) в обеспечении безопасности платежных систем приобрело решающее значение. Применение искусственного интеллекта (ИИ) в безналичных платежах произвело революцию в сфере безопасности безналичных платежей, обеспечив повышенную защиту и эффективность платежных процессов. В этой статье исследуется глубокое влияние искусственного интеллекта на безопасность безналичных платежей, уделяя особое внимание его роли в методах обнаружения, предотвращения и аутентификации мошенничества. Тем не менее, в этой статье также рассматривается преобразующее влияние ИИ на безопасность платежных систем, обсуждаются его преимущества, проблемы и перспективы на будущее.

Ключевые слова: искусственный интеллект, кибербезопасность, безналичные платежи, машинное обучение, глубокое обучение, обработка естественного языка.

Введение

Финансовый сектор переживает быструю трансформацию, поскольку цифровые платежные системы все чаще заменяют традиционные операции с наличными, предлагая большее удобство и эффективность. Однако этот переход также создает серьезные проблемы с безопасностью, поскольку киберпреступники разрабатывают передовые методы использования уязвимостей системы. Искусственный интеллект (ИИ) стал важнейшим решением для повышения безопасности платежной системы от этих угроз [1]. Технологии искусственного интеллекта, в частности машинное обучение и глубокое обучение, предоставляют возможности для обнаружения мошенничества в режиме реального времени, оценки рисков и проверки личности. Тем не менее, внедрение ИИ сопряжено с проблемами, такими как обеспокоенность по поводу конфиденциальности данных, проблемы с ложными срабатываниями и отрицательными результатами, а также постоянная адаптация киберпреступников. По мере развития технологии искусственного интеллекта ее роль в повышении безопасности безналичных платежей становится все более важной, обеспечивая более безопасную и устойчивую экосистему безналичных платежей.

1. Определение ИИ в контексте платежей

Искусственный интеллект (ИИ) — это отрасль информатики, ориентированная на создание систем, способных выполнять задачи, которые обычно требуют человеческого интеллекта, такие как обучение, понимание естественного языка, распознавание визуальных изображений и решение сложных проблем. Системы искусственного интеллекта используют сложные алгоритмы, которые имитируют процессы человеческого мозга для обучения, принятия решений и решения проблем. Их обучают на обширных наборах данных выявлять закономерности и тенденции, которые затем используют для принятия решений или прогнозов относительно новых данных. Этот процесс обучения, известный как машинное обучение, имеет основополагающее значение для многих приложений искусственного интеллекта, в том числе для онлайн-платежей. В контексте платежей, искусственный интеллект включает в себя использование алгоритмов машинного обучения, прогнозной аналитики, обработки естественного языка и других технологий для обработки, управления и защиты цифровых транзакций. Цель внедрения искусственного интеллекта состоит не в том, чтобы заменить вмешательство человека, а в том, чтобы усовершен-

ствовать и автоматизировать процессы, тем самым повышая эффективность и точность.

2. Технология искусственного интеллекта в платежах

Технология искусственного интеллекта в платежных системах сочетает в себе передовые вычислительные методы и инновационные алгоритмы для повышения безопасности, эффективности и общей функциональности [1]. Каждый из ключевых компонентов — машинное обучение, глубокое обучение, обработка естественного языка, биометрия и облачные вычисления — играет уникальную роль в совершенствовании платежных систем. Вот подробный обзор этих технологий:

2.1. Машинное обучение (МО)

Машинное обучение (МО) — это разновидность искусственного интеллекта (ИИ), которая фокусируется на разработке алгоритмов и статистических моделей, которые позволяют компьютерам выполнять задачи без явных инструкций. Обучаясь на данных, эти модели могут выявлять закономерности, принимать решения и со временем совершенствоваться с опытом. Машинное обучение имеет решающее значение для анализа больших объемов данных транзакций. Существуют различные типы машинного обучения, каждый из которых подходит для конкретных задач:

- *Контролируемое обучение (Supervised Learning)* обучает алгоритмы на маркированных наборах данных для обнаружения мошенничества путем выявления закономерностей, указывающих на подозрительную активность.
- *Обучение без учителя (Unsupervised Learning)* обнаруживает скрытые закономерности в неразмеченных данных, что важно для обнаружения аномалий и выявления необычного поведения транзакций.
- *Обучение с подкреплением (Reinforcement Learning)* улучшает процессы принятия решений посредством проб и ошибок, что полезно для динамического управления рисками, когда необходимы корректировки в реальном времени.

2.2. Глубокое обучение

Глубокое обучение расширяет возможности нейронных сетей, которые имитируют функции человеческого мозга и позволяют распознавать сложные закономерности. Сверточные нейронные сети (CNN) особенно эффективны при обработке данных изображений, что делает их ценными для распознавания лиц и других методов биометрической проверки. Рекуррентные нейронные сети (RNN) превосходно справляются с анализом последовательных данных, что имеет решающее значение для обработки естественного языка и обнаружения мошенничества в последовательностях транзакций. Эти технологии позволяют системам постоянно учиться и адаптироваться, улучшая их способность выявлять возникающие угрозы и реагировать на них.

2.3 Обработка естественного языка (NLP)

Обработка естественного языка (NLP) жизненно важна для систем искусственного интеллекта для анализа и понимания человеческого языка. Эта возможность используется для обнаружения попыток фишинга и других атак социальной инженерии путем анализа текстовых данных из электронных писем, журналов чатов и других каналов связи. Распознавание голоса, разновидность NLP, преобразует разговорную речь в текст и проверяет личность говорящего, добавляя дополнительный уровень безопасности для систем голосовых транзакций.

2.4. Биометрия

Биометрия повышает безопасность благодаря уникальным биологическим характеристикам. Системы распознавания лиц на основе искусственного интеллекта используют алгоритмы глубокого обучения для анализа черт лица и обеспечения безопасной аутентификации пользователей. Аналогичным образом, при сканировании отпечатков пальцев используются методы обработки изображений для проверки уникальных рисунков отпечатков пальцев, а при распознавании голоса анализируются голосовые характеристики для аутентификации пользователей. Эти биометрические методы обеспечивают надежную многофакторную аутентификацию, которую сложно подделать или украсть.

2.5. Облачные вычисления

Облачные вычисления поддерживают эти технологии искусственного интеллекта, предлагая необходимую вычислительную мощность и емкость хранилища для крупномасштабной обработки данных и обучения моделей искусственного интеллекта. Эта масштабируемость гарантирует, что платежные системы могут обрабатывать огромные объемы транзакций в режиме реального времени, что способствует более быстрым и эффективным процессам оплаты. Кроме того, передовые меры кибербезопасности, такие как шифрование и многофакторная аутентификация (MFA, защищают целостность и конфиденциальность данных, еще больше повышая безопасность цифровых платежных систем.

3. Преимущества внедрения искусственного интеллекта для повышения безопасности безналичных платежей

Внедрение искусственного интеллекта (ИИ) в обеспечение безопасности безналичных платежей предлагает

множество преимуществ, которые значительно повышают безопасность и эффективность цифровых транзакций. Одним из основных преимуществ являются расширенные возможности обнаружения и предотвращения мошенничества, которые обеспечивают технологии искусственного интеллекта [5]. Используя алгоритмы машинного обучения и прогнозную аналитику, искусственный интеллект (ИИ) может анализировать огромные объемы данных транзакций в режиме реального времени, чтобы выявлять подозрительные закономерности и аномалии, указывающие на мошеннические действия [9]. Такой упреждающий подход позволяет быстро принять меры по снижению потенциальных рисков и защите клиентов от мошеннических транзакций.

Еще одним важным преимуществом искусственного интеллекта (ИИ) в обеспечении безопасности безналичных платежей является улучшение методов аутентификации. Биометрическая аутентификация на основе искусственного интеллекта, такая как распознавание лиц и распознавание голоса, обеспечивает более безопасную и удобную альтернативу традиционным системам на основе паролей. Используя возможности распознавания образов ИИ, эти методы аутентификации могут точно идентифицировать людей, снижая риск несанкционированного доступа и усиливая общие меры безопасности. Более того, поведенческая биометрия на основе искусственного интеллекта анализирует взаимодействие пользователей с цифровыми интерфейсами, чтобы создать уникальные поведенческие профили для аутентификации. Отслеживая движения мыши, шаблоны набора текста, жесты на сенсорном экране и другие поведенческие сигналы, алгоритмы искусственный интеллект (ИИ) проверяют личность пользователей в режиме реального времени, не полагаясь исключительно на статические учетные данные, такие как пароли или PIN-коды [10].

Кроме того, искусственный интеллект упрощает автоматический контрольный журнал, обеспечивая подробные записи платежных процессов с отметками времени для целей аудита. Это повышает прозрачность и подотчетность финансовых операций, обеспечивая надежную основу для соблюдения требований и управления рисками [11]. Кроме того, технологии искусственного интеллекта настраивает меры безопасности на основе индивидуальных профилей пользователей, балансируя между безопасностью и удобством. Например, частые пользователи могут столкнуться с более плавным процессом аутентификации по сравнению с нечастыми пользователями. Такая персонализация помогает поддерживать высокий уровень безопасности без ущерба для удобства пользователей.

Таким образом, внедрение искусственный интеллект (ИИ) в систему безопасности безналичных платежей предлагает комплексное решение для борьбы с мошенничеством, оптимизации процессов соблюдения требований, улучшения методов аутентификации и обеспечения упреждающих мер по управлению рисками. Используя возможности технологий искусственного интеллекта, предприятия могут повысить безопасность цифровых транзакций, повысить операционную эффективность и укрепить доверие клиентов в развивающейся среде безналичных платежей.

4. Проблемы искусственного интеллекта при использовании ИИ для обеспечения безопасности безналичных платежей

Хотя искусственный интеллект (ИИ) предлагает множество преимуществ для безопасности безналичных платежей, его внедрение также создает ряд проблем, с которыми должны справиться финансовые учреждения и поставщики платежей. Эти проблемы охватывают технические, этические и эксплуатационные аспекты, создавая сложности в эффективной интеграции ИИ. Вот более детальное рассмотрение некоторых из этих препятствий:

- *Зависимость качества данных (Data Dependence)*: Эффективность искусственный интеллект (ИИ) во многом зависит от качества и количества обучающих данных. Предвзятые или неполные данные могут привести к предвзятым моделям ИИ, что приведет к неверным решениям. Например, искусственный интеллект (ИИ), обученный на наборе данных, в основном представляющем определенную демографическую группу, может с трудом выявить модели мошенничества среди недостаточно представленных демографических групп.
- *Проблемы прозрачности (Black Box Problem)*: Алгоритмы машинного обучения могут быть сложными, что затрудняет понимание того, как они приходят к решениям. Отсутствие прозрачности, часто называемое «проблемой черного ящика», вызывает обеспокоенность по поводу предвзятости и справедливости. Например, маркировка транзакций ИИ на основе данных о местоположении может непреднамеренно дискриминировать пользователей из определенных регионов.
- *Проблемы масштабируемости и интеграции (Scalability and integration challenges)*: Масштабирование решений искусственного интеллекта или их интеграция с существующими системами может оказаться дорогостоящим и трудоемким занятием для бизнеса. Например, небольшие интернет-магазины могут столкнуться с трудностями при объединении инструментов обнаружения мошенничества на основе искусственного интеллекта с существующими платежными шлюзами [2].
- *Развивающиеся угрозы (Evolving Threats)*: Мошенники постоянно адаптируют свою тактику, созда-

вая угрозу для систем искусственного интеллекта. Хотя искусственный интеллект (ИИ) может учиться на прошлых попытках, могут возникнуть новые схемы мошенничества, к которым ИИ плохо подготовлен. Чтобы опережать эту постоянную эволюцию, необходимо постоянное совершенствование и адаптация моделей ИИ.

- *Уязвимости безопасности (Security Vulnerabilities)*: Сами системы искусственного интеллекта могут быть уязвимы для атак, особенно если хакеры манипулируют обучающими данными или используют слабости алгоритмов. Надежные меры кибербезопасности необходимы для защиты систем безопасности на базе искусственного интеллекта.
- *Нормативная неопределенность (Regulatory Landscape)*: Нормативно-правовая база, связанная с ИИ в финансах, все еще развивается, что приводит к неопределенности в отношении конфиденциальности данных, ответственности за решения, принимаемые ИИ, и соблюдения правил. Четкие инструкции и надзор имеют решающее значение для обеспечения ответственного внедрения ИИ в безналичных платежах [12].

5. Будущее искусственного интеллекта в обеспечении безопасности безналичных платежей

Среда безналичных платежей постоянно развивается, и искусственный интеллект может взять на себя более важную роль в обеспечении безопасности будущих транзакций. Вот краткий обзор того, что может быть в будущем:

— *Непрерывное обучение и адаптация (Continuous Learning and Adaptation)*. Модели искусственного интеллекта будут развиваться, чтобы постоянно учиться, быстро адаптируясь к новым тактикам мошенничества и возникающим угрозам в режиме реального времени. Эта адаптация будет включать интеграцию различных источников данных, таких как тенденции в социальных сетях или новостные события в реальном времени, чтобы опережать развивающиеся преступные схемы.

— *Объяснимый ИИ (Explainable AI)*. Прозрачность принятия решений с помощью ИИ будет иметь приоритет, а достижения в области объяснимого ИИ (XAI) позволят глубже понять, как ИИ приходит к своим выводам. Такая прозрачность уменьшит предвзятость и повысит доверие к системе, что необходимо для соблюдения нормативных требований и укрепления доверия потребителей [13].

— *Мультимодальная аутентификация (Multimodal Authentication)*. Помимо поведенческой биометрии, ИИ будет интегрировать дополнительные факторы, такие как распознавание голоса или лица, для еще более надежной аутентификации. Такой многогранный подход создаст уровни безопасности, что сделает несанкционированный доступ все более затруднительным.

— *Федеративное обучение (Federated Learning)*. Проблемы конфиденциальности данных будут решаться с помощью методов федеративного обучения, что позволит обучать модели ИИ на децентрализованных наборах данных без ущерба для конфиденциальной информации пользователей. Такой совместный подход улучшит модели безопасности, сохраняя при этом конфиденциальность пользователей.

— *Автономное реагирование на угрозы (Autonomous Threat Response)*. Искусственный интеллект (ИИ) будет все более автономно реагировать на потенциальные угрозы безопасности при безналичных платежах, быстро изолируя и нейтрализуя подозрительные действия. Такой упреждающий подход сведет к минимуму последствия мошенничества и нарушений безопасности, повысив устойчивость платежных систем.

— *Устойчивость квантовых вычислений (Quantum Computing Resilience)*. По мере появления квантовых вычислений ИИ будет играть решающую роль в разработке методов шифрования, устойчивых к квантовым угрозам. Алгоритмы искусственного интеллекта будут способствовать созданию квантовоустойчивых криптографических методов, обеспечивающих постоянную безопасность безналичных платежей на фоне развития технологических возможностей.

Будущее искусственного интеллекта в сфере безопасности безналичных платежей является многообещающим. Решая текущие проблемы и способствуя инновациям, ИИ может стать краеугольным камнем безопасного и бесперебойного платежного процесса. Поскольку протоколы искусственного интеллекта и безопасности продолжают развиваться, мы можем предвидеть будущее, в котором безналичные транзакции будут не только удобны, но и очень устойчивы к мошенничеству.

Заключение

В заключение, применение искусственного интеллекта (ИИ) в безналичных платежах представляет собой палку о двух концах. Хотя ИИ предлагает значительные преимущества в обнаружении мошенничества, оценке рисков и аутентификации пользователей, он также создает новые проблемы безопасности. В этой статье исследовано многогранное влияние ИИ на безопасность безналичных платежей. Мы видели, как ИИ может анализировать огромные объемы данных в режиме реального времени, чтобы выявлять мошеннические транзакции, персонализировать методы аутентификации для повышения безопасности и оптимизировать безопасные про-

цессы оплаты. Однако потенциальные уязвимости, такие как утечка данных, предвзятость модели и возможность состязательных атак на модели ИИ, требуют тщательного рассмотрения.

В дальнейшем сбалансированный подход имеет решающее значение. Чтобы обеспечить постоянную безопасность безналичных транзакций, необходимо создать надежные системы безопасности наряду с интеграцией искусственного интеллекта. Это включает в себя внедрение надежных методов шифрования данных, регулярную проверку моделей ИИ на предмет предвзятости и разработку стратегий для смягчения состязательных атак. Постоянное сотрудничество между финансовыми учреждениями, поставщиками технологий и регулирующими органами имеет важное значение для построения безопасного будущего для безналичных платежей на основе искусственного интеллекта. Признавая как преимущества, так и риски, мы можем использовать возможности искусственного интеллекта для создания более безопасной и эффективной экосистемы безналичных платежей.

ЛИТЕРАТУРА

1. Ахматова, Д.Р. Влияние ИИ-решений на финансовый сектор: прогнозирование будущих изменений / Д.Р. Ахматова // Вестник экономических и социологических исследований. — 2023. — № 2. — С. 4–10. — EDN GLFZTF.
2. Туркина Д.Е. Три ключевые проблемы внедрения искусственного интеллекта в российских банках на современном этапе развития экономики // Инновации и инвестиции. — 2018. — № 12. — С. 335–336.
3. Звягин, Л.С. Технологии искусственного интеллекта в банковском и финансовом секторах / Л.С. Звягин // Мягкие измерения и вычисления. — 2022. — Т. 56, № 7— 1. — С. 5–18.
4. Саламова, А.А. Роль искусственного интеллекта в финансах / А.А. Саламова, И.Е. Федоровская, И.И. Васильев // Финансовые рынки и банки. — 2023. — № 1. — С. 63–68.
5. Бердышев А.В. Искусственный интеллект как технологическая основа развития банков // Вестник университета. — М., 2018. — № 5. — С. 91–94.
6. Digalaki E. The impact of artificial intelligence in the banking sector & how AI is being used in 2021 // Business Insider. — 2021. — 13.01. — URL: https://www.businessinsider.com/ai-in-banking-report (дата обращения: 15.02.2024).
7. Milana, C., & Ashta, A. Artificial intelligence techniques in finance and financial markets: a survey of the literature. Strategic Change, 30(3) pp. 189–209. (2021).
8. S. Deepalakshmi, Impact of Artificial Intelligence in E-payments (2018).
9. «Enhancing Payment Security Using Artificial Intelligence and Machine Learning» by Manish Bapna, et al. (2020).
10. «Anomaly Detection for Payment Fraud using Deep Learning» by Chih-Cheng Chen, et al. (2019).
11. «AI-powered Risk Assessment in Payment Systems: A Survey of Techniques and Applications» by Feng Liu, et al. (2022).
12. «Security and Privacy Challenges of AI-powered Payment Systems» by Xinxin Li, et al. (2021).
13. «Explainable AI for Fraud Detection in Payments» by Arvind Narayanan, et al. (2020).

Журнал «Современная наука: актуальные проблемы теории и практики»