ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ/ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

DOI: https://doi.org/10.60797/COMP.2025.6.1

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ СЛУЧАЕВ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Обзор

Алдохина Д.В.[1, *]

[1] Южный Федеральный Университет, Таганрог, Российская Федерация

* Корреспондирующий автор (aldokhina[at]sfedu.ru)

Аннотация

В данной статье рассматриваются современные методы применения искусственного интеллекта и машинного обучения для выявления и предотвращения финансового мошенничества. В условиях роста объема транзакций традиционные методы анализа становятся менее эффективными, что требует внедрения новых решений. Особое внимание уделяется алгоритмам классификации и методам обнаружения аномалий, которые позволяют выявлять подозрительные операции. Рассматриваются сложности, связанные с разметкой данных, и перспективные подходы, включающие в себя обучение для анализа последовательностей транзакций и текстовой информации. В перспективе развитие технологий, таких как графовые нейронные сети, генеративно-состязательные сети, мультимодальный анализ предиктивная аналитика, позволит повысить точность детектирования и перейти к проактивному противодействию мошенничеству.

Ключевые слова: искусственный интеллект, машинное обучение, финансовое мошенничество, обнаружение аномалий, глубокое обучение, предиктивная аналитика.

APPLICATION OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING METHODS TO DETECT FINANCIAL FRAUD

Review article

Aldokhina D.V.[1, *]

[1] Southern Federal University, Taganrog, Russian Federation

* Corresponding author (aldokhina[at]sfedu.ru)

Abstract

This article examines modern methods of applying artificial intelligence and machine learning to detect and prevent financial fraud. With the growing volume of transactions, traditional methods of analysis are becoming less effective, which requires the introduction of new solutions. Special attention is paid to classification algorithms and anomaly detection methods, which allow to identify suspicious transactions. Challenges associated with data markup and promising approaches that incorporate learning to analyse transaction sequences and textual information are discussed. In the future, advances in technologies such as graph neural networks, generative adversarial networks, and multimodal analysis predictive analytics will improve detection accuracy and allow to move towards proactive fraud countermeasures.

Keywords: artificial intelligence, machine learning, financial fraud, anomaly detection, deep learning, predictive analytics.

Введение

Применение искусственного интеллекта и машинного обучения для выявления случаев финансового мошенничества становится все более актуальным в современной жизни, когда объемы транзакций значительно увеличиваются, а традиционные методы анализа уже не справляются с нагрузкой. Финансовое мошенничество принимает различные формы, включая мошенничество с банковскими картами, кредитное мошенничество, отмывание денег, фишинг и другие схемы, которые требуют инновационных подходов к его обнаружению и предотвращению.

Алгоритмы классификации

Одним из главных преимуществ машинного обучения является его способность анализировать огромные массивы данных в режиме реального времени и выявлять аномалии, которые могут указывать на мошенническую активность. Для прогнозирования вероятности мошеннической транзакции можно применить алгоритмы классификации, обучив модель на исторических данных. Разделение типов мошенничества возможно с помощью двух подходов: бинарной и многоклассовой классификации. Алгоритмы, такие как логистическая регрессия, метод опорных векторов (SVM) и случайный лес (Random Forest), позволяют автоматически маркировать подозрительные транзакции. Для обнаружения ранее неизвестных схем мошенничества применяются методы поиска аномалий, включая «Isolation Forest» и автоэнкодеры, которые способны находить отклонения от нормальных паттернов поведения [1].

Для обучения этих алгоритмов требуется набор данных, содержащий информацию о транзакциях за определенный период, с пометками о мошеннических и легитимных операциях. Однако разметка данных часто сопряжена с трудностями: процесс обычно выполняется вручную на основе актов расследований мошенничества за выбранный период. Альтернативный подход — автоматический парсинг документов расследований для формирования выборки, но из-за их неструктурированности добиться высокой точности разметки может быть сложно [2].

Глубокое обучение и внедрение ии-решений

Глубокое обучение, в частности рекуррентные нейронные сети (RNN) и LSTM, эффективно анализируют последовательности транзакций, выявляя сложные взаимосвязи и временные закономерности, характерные для мошеннических операций. Трансформерные модели, такие как BERT, могут обрабатывать текстовые данные, например, описания транзакций или жалобы клиентов, для повышения точности детектирования [3].

Крупные финансовые институты уже активно внедряют ИИ-решения для выявления случаев мошенничества. Например, PayPal использует машинное обучение для оценки рисков в реальном времени, а Mastercard разработала систему Decision Intelligence, которая анализирует сотни параметров для принятия решений о блокировке подозрительных платежей. Банки, такие как JPMorgan Chase, применяют ИИ для предотвращения мошенничества с чеками и выявления поддельных кредитных заявок.

Однако внедрение этих технологий сопряжено с рядом вызовов. Ложные срабатывания остаются серьезной проблемой, поскольку блокировка легальных операций создает неудобства для клиентов и снижает доверие к банку. Кроме того, недостаток размеченных данных о мошеннических случаях осложняет обучение моделей. Важным аспектом является также соблюдение регуляторных требований, таких как GDPR, поскольку системы анализа транзакций работают с персональными данными [4].

Перспективы искуственного интеллекта

В будущем развитие технологий позволит улучшить анализ данных без их централизации, что повысит безопасность и конфиденциальность. Решения алгоритмов станут более прозрачными, а интеграция с блокчейном может обеспечить дополнительный уровень защиты и отслеживаемости транзакций [5].

Перспективные направления развития искусственного интеллекта в борьбе с финансовым мошенничеством включают несколько ключевых технологических трендов, которые кардинально меняют подход к обнаружению и предотвращению fraudulent-активности. Одним из наиболее многообещающих направлений является использование графовых нейронных сетей (GNN), которые иначе анализируют взаимосвязи между различными сущностями финансовой системы — клиентами, счетами, транзакциями и устройствами. Эти сети особенно эффективны для выявления сложных сетевых мошеннических схем, когда несколько аккаунтов действуют согласованно, маскируя свои операции под законные [6]. Например, GNN могут обнаруживать цепочки транзакций, специально спроектированные для обхода традиционных систем мониторинга или выявлять скрытых лиц в схемах отмывания денег. Крупные финансовые институты уже активно тестируют эти технологии, демонстрируя на практике их преимущества перед классическими методами анализа.

Особое значение в современных условиях приобретает применение генеративно-состязательных сетей (GAN), которые помогают решить одну из главных проблем машинного обучения в сфере финансовой безопасности — недостаток размеченных данных о мошеннических операциях. Эти нейросети способны генерировать реалистичные примеры fraudulent-активности, что позволяет значительно расширять и балансировать обучающие выборки без риска нарушения конфиденциальности реальных клиентов. Более того, GAN можно использовать для моделирования потенциально новых схем мошенничества для тестирования и совершенствования защитных систем до того, как эти они будут применены злоумышленниками на практике [7].

Мультимодальный анализ данных и предиктивная аналитика

Современные системы обнаружения мошенничества все чаще используют мультимодальный анализ данных, комбинируя различные источники информации для повышения точности детектирования. Такой подход интегрирует традиционные транзакционные данные с биометрической аутентификацией [8]. Подобная комплексная аналитика позволяет не только более надежно выявлять подозрительную активность, но и значительно сокращать количество ложных срабатываний — например, когда система видит транзакцию с нового устройства в необычном месте, но подтверждает ее законность через биометрическую верификацию пользователя.

Особого внимания заслуживает развитие предиктивной аналитики, которая переводит борьбу с мошенничеством из активного в проактивный режим. Современные алгоритмы временных рядов и прогнозного моделирования позволяют выявлять подозрительные паттерны поведения еще до совершения потенциально мошеннической операции. Например, система может заметить нехарактерную активность карты после длительного периода неиспользования или спрогнозировать вероятность мошенничества на основе анализа микро-признаков в поведении пользователя [9].

Автоматизированные системы расследований

Автоматизированные системы расследований на базе ИИ представляют собой еще один важный технологический прорыв. Эти решения автоматизируют трудоемкий процесс анализа мошеннических инцидентов, выполняя автоматическую кластеризацию похожих случаев, генерацию подробных отчетов с объяснением причинно-следственных связей и даже интеграцию с CRM-системами для ускоренного взаимодействия с клиентами. В отличие от традиционных методов, где каждый случай требовал индивидуального расследования специалистом по безопасности, современные ИИ-системы могут мгновенно находить аналоги в исторических данных, определять степень риска и даже предлагать оптимальные действия по минимизации ущерба [10]. Однако внедрение этих передовых технологий сопровождается рядом серьезных вызовов и этических дилемм. Одной из ключевых проблем является потенциальная дискриминация алгоритмов, когда системы искусственного интеллекта могут необоснованно чаще блокировать операции определенных групп пользователей. Вопросы конфиденциальности данных также остаются крайне актуальными — агрессивный сбор информации для анализа поведенческих паттернов часто вступает в противоречие с нормами защиты персональных данных. Кроме того, сохраняется проблема адаптивности мошенников, которые быстро учатся обходить новые системы защиты и создают постоянную потребность в

обновлении и совершенствовании алгоритмов. Эти не решенные проблемы требуют комплексного подхода, сочетающего технологические инновации с продуманной политикой регулирования и правовыми стандартами.

Заключение

Финансовое мошенничество представляет собой серьезную угрозу для экономической безопасности, и традиционные методы его обнаружения уже не справляются с растущим объемом и сложностью мошеннических схем. Внедрение технологий искусственного интеллекта и машинного обучения позволит значительно повысить эффективность борьбы с fraudulent-активностью за счет автоматизированного анализа больших данных, выявления аномалий и прогнозирования новых видов мошенничества.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Зайченко В. Машинное обучение против фрода / В. Зайченко, М. Земскова // Открытые системы. — 2017. — URL: https://www.osp.ru/os/2017/02/13052223 (дата обращения: 02.04.25)

2. Melcher K. Fraud Detection Using Random Forest, Neural Autoencoder, and Isolation Forest Techniques / K. Melcher, R. Silipo // HabrHabr. — 2019. — URL: https://habr.com/ru/companies/nix/articles/478286/ (accessed: 28.03.25)

3. Cheng D. Graph Neural Networks for Financial Fraud Detection: A Review [Electronic source] / D. Cheng // paperswithcode. — 2024. — URL: https://paperswithcode.com/paper/graph-neural-networks-for-financial-fraud. (accessed: 01.04.25)

4. Рожков В.А. Использование искусственного интеллекта и машинного обучения для выявления и борьбы с финансовыми преступлениями. / В.А. Рожков // Теория и практика современной науки. — 2024. — № 6 (108). — URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-dlya-vyyavleniya-i-borby-s-finansovymi-prestupleniyami/viewer (дата обращения: 03.04.25).

5. Cormen T.H. Introduction to algorithms / T.H. Cormen, C.E. Leiserson, R.L. Rivest. — Cambridge: The MIT Press, 2021. — 1296 p. — URL: https://matematika76.ru/fm/%D0%9A%D0%BE%D1%80%D0%BC%D0%B5%D0%BD.pdf. (accessed: 06.04.25).

6. Машинное обучение для поиска аномалий // ХабрХабр. — 2022. — URL: https://habr.com/ru/articles/671670/ (дата обращения: 04.04.25).

7. Применение генеративных состязательных сетей в системах обнаружения аномалий. — 2021. — URL: https://moitvivt.ru/ru/journal/article?id=921 (дата обращения: 05.04.25)

8. Осипов Г.С. Методы искусственного интеллекта / Г.С. Осипов. — Москва: Физматлит, 2011. — 296 с.

9. Осипова Т.А. Применение алгоритмов машинного обучения к задаче выявления мошенничества при использовании пластиковых карт/ Т.А. Осипова, К.С. Зайцев, В.О. Биферт // International Journal of Open Information Technologies. — 2021. — URL: https://cyberleninka.ru/article/n/primenenie-algoritmov-mashinnogo-obucheniya-k-zadache-vyyavleniya-moshennichestva-pri-ispolzovanii-plastikovyh-kart/viewer (дата обращения: 06.04.25)

10. Николенко С. Глубокое обучение.Погружение в мир нейронных сетей / С. Николенко, А. Кадурин, Е. Архангельская. — Санкт-Петербург: Питер, 2018. — 481 с.

Список литературы на английском языке / References in English

1. Zaichenko V. Mashinnoe obuchenie protiv froda [Machine Learning against Fraud] / V. Zaichenko, M. Zemskova // Open Systems Publications. — 2017. — URL: https://www.osp.ru/os/2017/02/13052223 (accessed: 02.04.25) [in Russian]

2. Melcher K. Fraud Detection Using Random Forest, Neural Autoencoder, and Isolation Forest Techniques / K. Melcher, R. Silipo // HabrHabr. — 2019. — URL: https://habr.com/ru/companies/nix/articles/478286/ (accessed: 28.03.25)

3. Cheng D. Graph Neural Networks for Financial Fraud Detection: A Review [Electronic source] / D. Cheng // paperswithcode. — 2024. — URL: https://paperswithcode.com/paper/graph-neural-networks-for-financial-fraud. (accessed: 01.04.25)

4. Rozhkov V.A. Ispol'zovanie iskusstvennogo intellekta i mashinnogo obucheniya dlya vy'yavleniya i bor'by' s finansovy'mi prestupleniyami [Using artificial intelligence and machine learning to identify and combat financial crimes]. / V.A. Rozhkov // Theory and practice of modern science. — 2024. — № 6 (108). — URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-dlya-vyyavleniya-i-borby-s-finansovymi-prestupleniyami/viewer (accessed: 03.04.25). [in Russian]

5. Cormen T.H. Introduction to algorithms / T.H. Cormen, C.E. Leiserson, R.L. Rivest. — Cambridge: The MIT Press, 2021. — 1296 p. — URL: https://matematika76.ru/fm/%D0%9A%D0%BE%D1%80%D0%BC%D0%B5%D0%BD.pdf. (accessed: 06.04.25).

6. Mashinnoe obuchenie dlya poiska anomalii [Machine learning for anomaly detection] // Habr. — 2022. — URL: https://habr.com/ru/articles/671670/ (accessed: 04.04.25) [in Russian]

7. Primenenie generativnikh sostyazatelnikh setei v sistemakh obnaruzheniya anomalii [The use of generative adversarial networks in anomaly detection systems]. — 2021. — URL: https://moitvivt.ru/ru/journal/article?id=921 (accessed: 05.04.25) [in Russian]

8. Osipov G.S. Metody' iskusstvennogo intellekta [Methods of artificial intelligence] / G.S. Osipov. — Moscow: Fizmatlit, 2011. — 296 p. [in Russian]

9. Osipova T.A. Primenenie algoritmov mashinnogo obuchenija k zadache vyjavlenija moshennichestva pri ispol'zovanii plastikovyh kart [Application of machine learning algorithms to the task of detecting fraud when using plastic cards] / T.A. Osipova, K.S. Zaitsev, V.O. Bifert // International Journal of Open Information Technologies. — 2021. — URL: https://cyberleninka.ru/article/n/primenenie-algoritmov-mashinnogo-obucheniya-k-zadache-vyyavleniya-moshennichestva-pri-ispolzovanii-plastikovyh-kart/viewer (accessed: 06.04.25) [in Russian]

10. Nikolenko S. Glubokoe obuchenie.Pogruzhenie v mir nejronny'x setej [Deep learning.Diving into the world of neural networks] / S. Nikolenko, A. Kadurin, E. Arxangel'skaya. — Saint Petersburg: Piter, 2018. — 481 p. [in Russian]