ФИНАНСЫ ГОСУДАРСТВА И ПРЕДПРИЯТИЙ
FINANCES OF THE STATE AND ENTERPRISES

УДК 336.7:004.8
DOI 10.52575/2687-0932-2025-52-1-110-124

Сравнительный анализ и возможности ИИ-технологий для предотвращения мошенничества в финансовом секторе

Бабанская А.С., Ермольева Д.Р., Ефименко Н.А., Акулова С.А.
Финансовый университет при Правительстве РФ, Факультет экономики и бизнеса,
Кафедра экономической безопасности и управления рисками
Россия, 125993, г. Москва, Ленинградский проспект, 49
banasti@mail.ru, ermolyeva@gmail.com, nefima19@mail.ru, sophia0105@mail.ru

Аннотация. Технологии искусственного интеллекта (ИИ) охватывают ключевые области обеспечения безопасности в финансовом секторе, включая противодействие отмыванию денег и мошенничеству, сбор данных о безопасности, мониторинг и предотвращение киберугроз. Несмотря на большое количество публикаций, практически отсутствуют исследования по внедрению и использованию ИИ, сравнению отдельных субтехнологий ИИ, что затрудняет оценку их эффективности, скорости и точности распознавания мошеннических схем, что обосновывает актуальность исследования. Цель – оценить возможности применения различных ИИ-технологий для выявления подозрительной активности и аномалий и провести сравнительный анализ их эффективности при противодействии мошенничеству в финансовом секторе. Методы: общенаучные методы теоретического познания – проведения аналогий, индукции и дедукции, сравнительный анализ, монографический анализ, кейс-стади. Особое внимание было уделено опыту финансового сектора США. В качестве эмпирической базы использовались статистические данные из исследований Центра Исследований и Разработок Аль-Кинди. В статье определены возможности ИИ-технологий: 1) на различных этапах предотвращения мошенничества согласно модели CIMA; 2) для различных типов финансового мошенничества. Согласно результатам исследования, показатели эффективности различных моделей колеблются в диапазоне 88–94 %, что говорит об их хорошей адаптивности к различным сценариям обнаружения мошенничества. Наибольшую полноту раскрытия демонстрируют субтехнологии машинного обучения (дерево решений) и модели глубокого изучения (нейронные сети и сверточные нейронные сети). Положительное влияние ИИ-технологий на процедуру выявления мошенничества заключается в повышении точности обнаружения мошенничества на 85 %, росте скорости выявления новых схем мошенничества на 78 %, росте обнаружения мошенничества на 70 %, снижении ложных срабатываний на 92 %. Предложены решения по развитию ИИ в целях предотвращения мошенничества в финансовом секторе, которые включают подготовку данных на этапе сбора, обоснованный выбор ИИ-моделей, проверку возможностей интеграции ИИ-моделей, сотрудничество с ИТ-компаниями.

Ключевые слова: искусственный интеллект, модели ИИ, финансовые данные, мошенничество, выявление аномалий, подозрительная активность

Для цитирования: Бабанская А.С., Ермольева Д.Р., Ефименко Н.А., Акулова С.А. 2025. Сравнительный анализ и возможности ИИ-технологий для предотвращения мошенничества в финансовом секторе. *Экономика. Информатика,* 52(1): 110–124. DOI 10.52575/2687-0932-2025-52-1-110-124

Benchmarking and Opportunities of AI Technologies for Fraud Prevention in the Financial Sector

Anastasia S. Babanskaya, Daria R. Ermoleva, Nadezhda A. Efimenko, Sofia A. Akulova
Financial University under the Government of the Russian Federation, Faculty of Economics and Business, Department of Economic Security and Risk Management
49 Leningradsky Ave, Moscow 125993, Russia
banasti@mail.ru, ermolyeva@gmail.com, nefima19@mail.ru, sophia0105@mail.ru

Abstract Artificial intelligence (AI) technologies cover key areas of financial sector security, including combating money laundering and fraud, collecting security data, monitoring and preventing cyber threats. The relevance of this study is explained by a lack of research on the implementation and use of AI and comparing individual AI subtechnologies, which makes it difficult to assess their effectiveness, speed and accuracy of recognizing fraudulent schemes. The goal of our research was to assess the possibilities of using various AI technologies to identify suspicious activity and anomalies and to conduct a comparative analysis of their effectiveness in combating fraud in the financial sector. The methods employed included general scientific methods of theoretical knowledge – drawing analogies, induction and deduction, comparative analysis, monographic analysis, and case study. We paid special attention to the experience of the US financial sector. As an empirical base, we used statistical data from Al-Kindi Research and Development Center. The article defines the capabilities of AI technologies: 1) at various stages of fraud prevention according to the CIMA model 2) for various types of financial fraud. According to the results of the study, the efficiency of various models ranges from 88 to 94 %, which indicates their good adaptability to various fraud detection scenarios. Machine learning subtechnologies (decision trees) and deep learning models (neural networks and convolutional neural networks) demonstrate the highest completeness of information disclosure. The positive impact of AI technologies on the fraud detection procedure is an increase in the accuracy of fraud detection by 85 %, an increase in the speed of identifying new fraud schemes by 78 %, an increase in fraud detection by 70 %, and a decrease in false positives by 92 %. We offered the following solutions for the development of AI and the prevention of fraud in the financial sector: data preparation at the collection stage, informed selection of AI models, testing the integration capabilities of AI models, and cooperation with IT companies.

Keywords: artificial intelligence, AI models, financial data, fraud, anomaly detection, suspicious activity

For citation: Babanskaya A.S., Ermoleva D.R., Efimenko N.A., Akulova S.A. 2025. Benchmarking and Opportunities of AI Technologies for Fraud Prevention in the Financial Sector. *Economics. Information technologies*, 52(1): 110–124 (in Russian). DOI 10.52575/2687-0932-2025-52-1-110-124

Введение

В условиях цифровой экономики технологии искусственного интеллекта (ИИ) все активнее используются для обеспечения кибербезопасности банковского сектора и затрагивают многие сферы, в том числе борьбу с отмыванием денег и мошенничеством, агрегирование данных безопасности, мониторинг и предотвращение киберугроз.

Многие исследователи затрагивают задачи анализа эффективности использования цифровых технологий в финансовой сфере. Так, в своих совместных исследованиях многие ученые [Bello et al., 2023; Bello et al., 2024; Daraojimba et al., 2023] утверждали, что обнаружение мошенничества на основе ИИ предлагает многочисленные преимущества для финансовых учреждений, однако также создает ряд проблем этического, правового, репутационного характера [Toth & Blut, 2024; Hasan, 2024], которые только предстоит решить. В исследованиях [Багреева и др., 2022; Pacific Data Integrators, 2024] приходят к выводу, что внедрение и использование ИИ значительно повышает скорость и эффективность распознавания мошеннических схем, однако ввиду разнообразия самих технических решений на основе ИИ и существенной дифференциации возможностей не проводится сравнение их эффективности между собой.

Как отмечают аналитики Business Insider Intelligence [Горян, 2019; Statista, 2023; Statista, 2024], около 80 % банковских учреждений с активами более 100 млрд долларов США и чуть менее половины банков с активами менее 100 млрд долларов США в настоящее время реализуют проекты с применением ИИ. Однако отдельные авторы [Беспалов, Богатырева, 2023] обращают внимание, что технологии ИИ для противодействия мошенничеству в финансовом секторе весьма разнообразны и реализуются с помощью различных ИИ-моделей, которые отличаются возможностями, сферой применения и уровнем эффективности. Это в свою очередь требует более тщательного выбора и обоснования тех или иных ИИ-технологий, наиболее подходящих для конкретных случаев защиты от мошенничества, что обуславливает *актуальность исследования*.

Цель – оценить возможности применения различных ИИ-технологий для выявления подозрительной активности и аномалий и провести сравнительный анализ их эффективности при противодействии мошенничеству в финансовом секторе.

Задачи: оценить уровень развития ИИ-технологий как средства безопасности в финансовом секторе. Определить ключевые возможности ИИ по предотвращению мошенничества в финансовом секторе. Оценить и сравнить эффективность использования различных ИИ-технологий при выявлении и предотвращении случаев мошенничества. Определить проблемы и предложить решения по развитию ИИ в финансовом секторе.

Объекты и методы исследования

Объектом данного исследования являются различные ИИ-технологии, которые используются для выявления аномалий в массивах финансовой информации, для противодействия мошенничеству в финансовом секторе.

Предмет исследования – социально-экономические возможности использования ИИ-технологий для предотвращения мошенничества в финансовом секторе и уровень эффективности различных моделей ИИ.

Методы, применяемые в рамках исследования: общенаучные методы теоретического познания – проведения аналогий, индукции и дедукции, а также сравнительный анализ, монографический анализ, кейс-стади. Источником информации послужили нормативно-правовые акты и программы развития, труды российских и зарубежных ученых по вопросам применения различных моделей ИИ для противодействия мошенничеству. Особое внимание было уделено опыту финансового сектора США. В качестве эмпирической базы исследования использовались статистические данные из исследований Центра Исследований и Разработок Аль-Кинди (Al-Kindi Center for Research and Development), Института статистических исследований и экономики знаний ВШЭ [ИСИЭЗ ВШЭ, 2024; Kamuangu, 2024]. Под синтетическими данными мы понимаем данные, созданные искусственно с помощью алгоритмов на основе фактических данных и учитывающие их паттерны и распределение, но не раскрывающие их конфиденциальность.

В качестве параметров эффективности различных ИИ-технологий для выявления и предотвращения мошенничества использовались показатели, предложенные для этих целей в исследовании [Bello et al., 2023; Bello et al., 2024; Alooba, 2024]:

1. Accuracy (Точность) – показатель, отражающий долю правильных ответов модели среди всех предсказаний. Эта основополагающая метрика представляет не только правильность модели, но и ее надежность на практике.

2. Precision (Точность, меткость, аккуратность) – показатель, отражающий долю истинно положительных ответов среди всех положительных ответов модели, то есть количество фактических положительных примеров, которые модель правильно предсказала как положительные.

3. Recall (Полнота, отзывчивость) – показатель, отражающий долю истинно положительных ответов среди всех правильных ответов модели, показывает, насколько хорошо модель может их идентифицировать. Recall измеряет способность модели фиксировать все положительные примеры.

4. F1 Score – гармоническое среднее между Precision и Recall. Данный показатель полезен, когда необходимо найти баланс между Precision и Recall, особенно в случаях, когда классы не сбалансированы (например, когда положительных примеров значительно меньше, чем отрицательных). Чем выше данный показатель, тем лучше модель справляется с задачей классификации. F1 Score дает более полное представление о производительности модели, чем использование только одного из анализируемых показателей.

5. AUC-ROC (площадь (Area Under Curve) под кривой ошибок (Receiver Operating Characteristic curve)) – показатель, отражающий то, насколько хорошо модель различает положительные и отрицательные классы. Чем выше данный показатель, тем лучше справляется модель.

Результаты и их обсуждение

Уровень развития ИИ как средства безопасности в финансовом секторе

На сегодня технологии ИИ используются во всем мире не только в качестве научно-технического инструмента, но и для борьбы с коррупцией и мошенничеством в самых разных формах и сферах безопасности. В России набор технологических задач и субтехнологий, связанных с развитием цифровых технологий, четко представлен в Дорожной карте развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект» [Правительство Российской Федерации, 2020; Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, 2019]. Согласно этому проекту, отмечается высокое разнообразие фактически применяемых средств информационной безопасности для предотвращения мошенничества, однако среди них крайне мала доля высокотехнологичных методов ИИ (рис. 1).

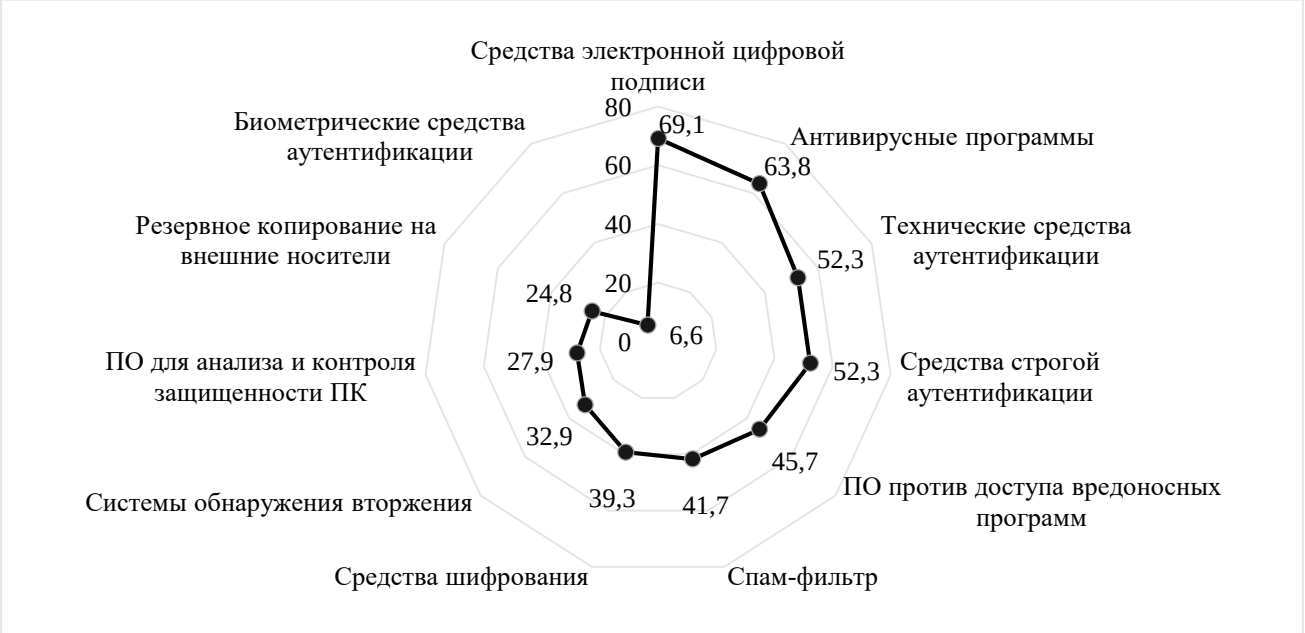

Рис. 1. Степень использования средств информационной безопасности российскими организациями в 2022 году (доля от общего числа организаций), %
Fig. 1. Degree of use of information security tools by Russian organizations in 2022 (share of the total number of organizations), %

Источник: составлено авторами на основе обзора [ИСИЭЗ ВШЭ, 2024]

В условиях цифровой экономики финансовые учреждения также опираются на решения ИИ для снижения финансовых рисков, проверки деловых партнеров и клиентов, улучшения своих возможностей по обнаружению мошенничества [Бабанская, Груднева, 2020; Хоружий и др., 2018]. Наблюдается ежегодный рост финансирования в данные технологии обеспечения безопасности. Согласно исследованиям Juniper Research

[Mayanard, 2022; Mayanard, 2023], в 2022 глобальные расходы бизнеса ведущих поставщиков ИИ в сфере обнаружения и предотвращения финансового мошенничества составили 6,5 млрд долл. США, а к 2027 году превысят 10 млрд долл. При этом мировые затраты финансового сектора на ИИ, по прогнозам аналитиков [V7 Labs, 2022], возрастут с 35 млрд долл. США в 2023 году до 97 млрд долл. США в 2027 году (рис. 2). Рост рынка решений для предотвращения мошенничества на базе ИИ увеличится за 6 лет в среднем на 54 % [Mayanard, 2022]. Самые существенные затраты (более 90 %) на внедрение ИИ-технологий для предотвращения мошенничества традиционно будут осуществлять страны Дальнего Востока и Китая, Западной Европы и Северной Америки (рис. 3) [Mayanard, 2023].

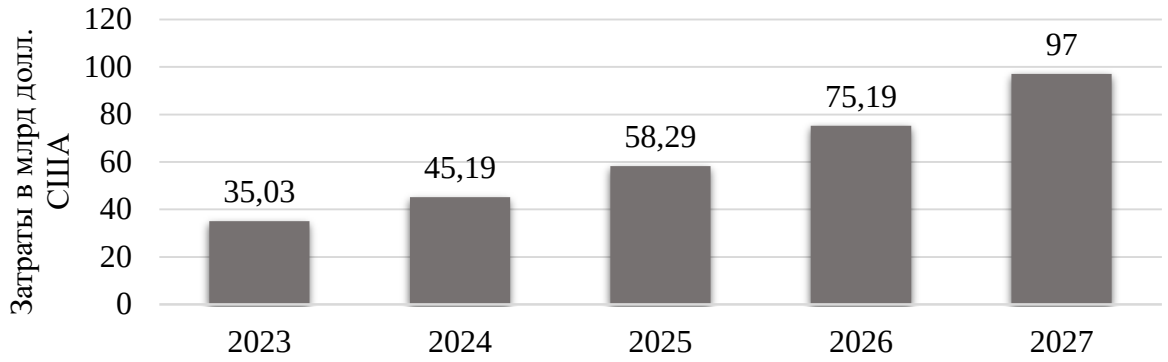

Рис. 2. Мировые затраты финансового сектора на ИИ в 2023–2027 гг. (прогнозные значения в 2024–2027 гг.), млрд долл. США
Fig. 2. Global financial sector spending on AI from 2023 to 2027 (forecast values in 2024–2027), billion USD
Источник: составлено авторами на основе обзора [Mayanard, 2022]

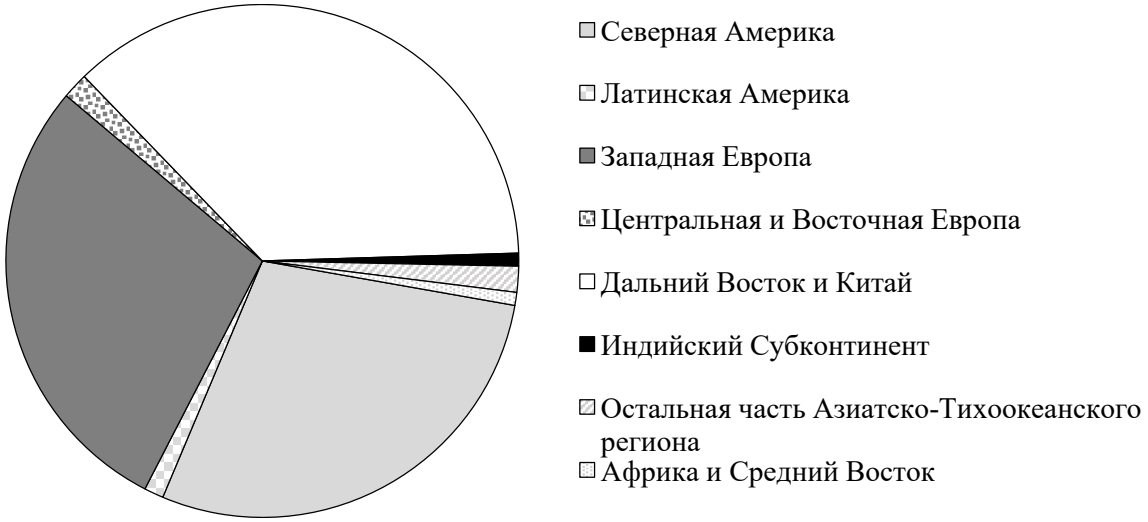

Рис. 3. Структура затрат по отдельным странам на платформы обнаружения финансового мошенничества с поддержкой ИИ в 2027 году (прогнозные значения), %
Fig. 3. Cost structure by individual countries for AI-enabled financial fraud detection platforms in 2027 (forecast values), %
Источник: составлено авторами на основе обзора [Mayanard, 2023]

Возможности ИИ по предотвращению мошенничества в финансовом секторе

По сравнению с традиционными подходами системы ИИ более динамичны и могут адаптироваться к меняющимся схемам мошенничества в режиме реального времени, а также их можно непрерывно обучать на новых данных, что позволяет им распознавать возникающие угрозы и корректировать свои стратегии обнаружения аномалий и подозрительностей.

Анализируя огромные объемы данных и выявляя сложные закономерности, технологии ИИ значительно сокращают количество ложных положительных и ложных отрицательных результатов. Эти системы могут обучаться как на исторических, так и на реальных данных, чтобы со временем повышать свою точность, могут обрабатывать и анализировать большие объемы транзакций в режиме реального времени [Udeh et al., 2024].

Именно эта возможность оперативной работы с большими объемами данных имеет решающее значение для финансовых учреждений, которые на ежедневной основе имеют дело с миллионами транзакций [Золотова и др., 2023]. Все эти преимущества позволяют выявлять подозрительные действия до того, как они приведут к значительным финансовым потерям. Разнообразие технических решений на основе ИИ позволяет использовать их в различных сферах предотвращения мошенничества (рис. 4). Наибольший эффект в финансовом секторе дает многоуровневый подход с комбинированием сразу нескольких ИИ-технологий, например, глубокого обучения и обнаружения аномалий.

Машинное обучение (МО)

- Автоматическое обучение и адаптация к переменам делает их устойчивее к новым способам мошенничества.
- Системы МО могут быть интегрированы в анализ нескольких источников информации, обеспечивая более глубокое представление о поведении пользователей и шаблонах их финансовых транзакций и выявляя аномалии действий. Сюда относятся модели логистической регрессии, дерева решений и др.

Методы обнаружения аномалий

- **Кластерный анализ** подразумевает группировку схожих по признакам транзакций, а также выделние тех, которые не вписываются ни в один кластер, что сигнализирует об их аномальности. Обнаружение аномалий основывается на плотности распределения данных и поиске выбросов вокруг кластеров, которые отклоняются от большинства точек данных, помогая выявлять потенциальное мошенничество.

Обработка естественного языка (NLP)

- **Анализ неструктурированных текстовых данных**, связанных с транзакциями (напимер, описания и сообщения клиентов).
- **Распознавание именованных сущностей** (NER): идентифицирует и классифицирует данные в тексте, которые могут быть полезны для обнаружения мошенничества (например, имена, местоположения, даты).
- **Анализ настроений** (сентимент-анализ) оценивает эмоциональный тон текстовых данных для выявления подозрительного поведения, а также оценивает настроения сообщений клиентов.

Модели глубокого изучения

- Способны выявить сложные паттерны в больших объемах данных, моделировать сложные связи.
- **Базовые нейронные сети** могут моделировать нелинейные отношения в транзакционных данных, что подходит для простых задач обнаружения мошенничества.
- **Сверточные нейронные сети (CNN)** подходят для обработки данных транзакций как «изображения», где важны пространственные иерархии, так как они могут автоматически извлекать иерархические признаки из необработанных транзакционных данных (например, проверки оформления чеков (CSV-AI), автоматическая проверка подписей (ASV-AI))
- **Рекуррентные нейронные сети (RNN)** и **Сети с долговременной краткосрочной памятью (LSTM)** упрощают обработку последовательных данных и исторический анализ транзакций.

Гибридные модели

- Объединение различных методов ИИ в гибридные модели повышает надежность и точность систем обнаружения мошенничества, объединяя прогнозы из нескольких моделей.

Рис. 4. Сфера применения разнообразных ИИ-технологий для предотвращения мошенничества в финансовом секторе

Fig. 4. Scope of application of various AI technologies to prevent fraud in the financial sector

Источник: составлено авторами на основе обзора литературы [Bello et al., 2024; Беспалов, Богатырева, 2023; Adelakun et al., 2024]

Все системы обнаружения мошенничества на основе ИИ значительно снижают уровень мошенничества за счет работы на всех этапах противодействия мошенничеству: обнаружения, предотвращения мошеннических действий в режиме реального времени и принятия ответных мер. Использование систем МО, глубокого обучения и других помогает финансовым учреждениям более эффективно выявлять мошенничество, минимизируя финансовые потери и защищая активы клиентов на разных этапах предотвращения мошенничества (рис. 5).

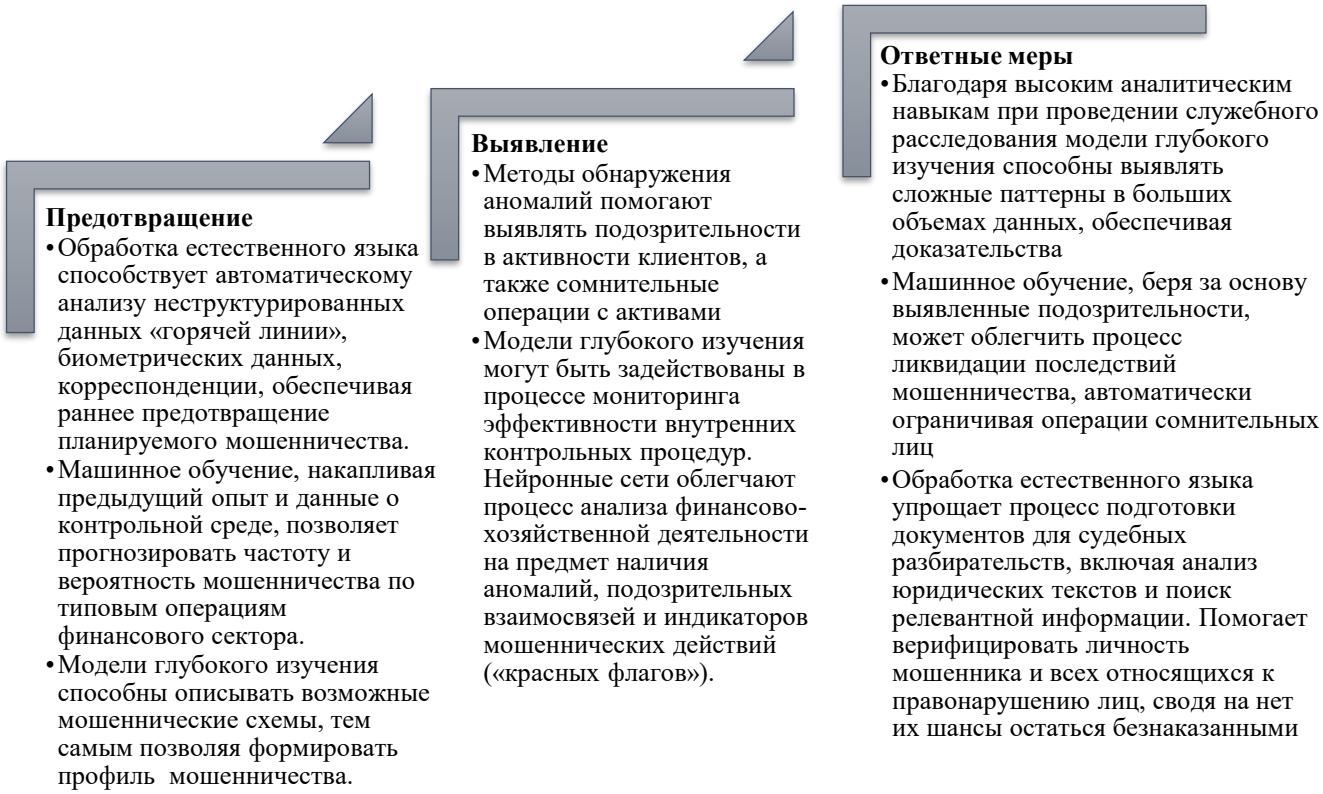

Рис. 5. Возможности ИИ-технологий на различных этапах предотвращения мошенничества по модели CIMA (Chartered Institute of Management Accountants)
Fig. 5. The capabilities of AI technologies at various stages of fraud prevention according to the CIMA (Chartered Institute of Management Accountants) model
Источник: составлено авторами.

Стоит отметить, что системы ИИ и решения на базе ИИ работают с разнообразными категориями мошенничества в финансовом секторе (табл. 1).

Сравнительный анализ эффективности использования ИИ-моделей

Исследование оценки эффективности является важной составляющей использования ИИ для обнаружения мошенничества. В исследованиях современных цифровых технологий [Bello et al., 2023; Bello et al., 2024; Alooba, 2024] используют большое количество различных показателей, рассматривают многие параметры, раскрывающие результаты производительности ИИ-моделей. За основу исследования были приняты следующие показатели: Accuracy (точность), Precision (точность, меткость, аккуратность), Recall (полнота, отзывчивость), F1 Score (гармоническое среднее между Precision и Recall), AUC-ROC (площадь под кривой ошибок (Receiver Operating Characteristic curve)).

Таблица 1
Table 1

Возможности ИИ для выявления различных типов финансового мошенничества
The power of AI to detect different types of financial fraud

Тип	Характеристика финансового мошенничества	Решения на основе МО и ИИ
Физические атаки	Традиционные виды мошенничества: подделка чеков, скимминг в банкоматах, кража кредитных карт. Хотя они самые простые, но сохраняются благодаря своей эффективности, особенно когда нацелены на более уязвимые категории граждан (подростки, пенсионеры и т. п.)	Видеоаналитика на базе ИИ может обнаруживать подозрительное поведение и предупреждать сотрудников службы безопасности в режиме реального времени. Алгоритмы МО могут анализировать огромные объемы данных транзакций в режиме реального времени, выявляя аномалии, которые отклоняются от типичного поведения клиента. Ускоряется процесс выявления и реагирования в случае подозрительной активности.
Нарушение принципа двойной авторизации	Это мера безопасности, когда важная или конфиденциальная транзакция согласовывается сразу несколькими сотрудниками компании. Это защищает от внутреннего мошенничества одного сотрудника, однако не работает в случае их сговора (когда два человека вместе совершают мошенничество) или по ошибке (если один из двоих одобряет мошенническую транзакцию, не осознавая этого).	Алгоритмы МО отслеживают действия сотрудников, выявляя необычные закономерности, которые могут указывать на сговор или неэтичные действия, обеспечивая соблюдение требований двойной авторизации. Например, если два сотрудника всегда быстро одобряют транзакции друг друга без надлежащих проверок, система может пометить это как подозрительное поведение. Так, компания может эффективней расследовать потенциальное мошенничество на ранних этапах.
Цифровое мошенничество	Мошенничество в цифровом банкинге: захват онлайн-аккаунтов, фишинг, мошеннические переводы. Скорость и анонимность Интернета делают их особенно трудными для обнаружения.	Системы ИИ эффективно обнаруживают онлайн-мошенничество (кража личных данных, фишинг), анализируя поведение пользователей и модели транзакций, отмечая аномалии для немедленного вмешательства.

Источник: составлено авторами

Согласно результатам исследования по оценке эффективности некоторых ИИ-технологий (табл. 2), все показатели эффективности превышают 80 %, что говорит об их хорошей адаптивности к различным сценариям обнаружения мошенничества. Среднее значение всех показателей эффективности колеблется в диапазоне 88–94 %, что означает неполноту раскрытия потенциала рассмотренных методов. Ученым только предстоит найти способы роста этих показателей и улучшить их результативность Маленький размах вариации говорит о том, что все значения находятся достаточно близко к среднему, следовательно, среднее значение хорошо обобщает совокупность. Невысокий коэффициент вариации показывает, что степень изменчивости эффективности разных методов не так высока. Они все являются важными составляющими процесса выявления мошенничества, улучшая качество и скорость данного процесса.

Несмотря на достаточно высокие показатели всех моделей, пока что ни одна из моделей не достигает 100 % значения показателей. Это связано с множеством факторов, проблему влияния которых ученым только предстоит изучить. Оценка эффективности ИИ-технологий достаточно многогранна, поэтому стоит учитывать не только количественные показатели, но и практическую применимость, устойчивость к изменениям данных и возможность различной интерпретации результатов.

Таблица 2
Table 2

Результаты оценки эффективности ИИ-технологий для целей выявления мошенничества
Results of assessing the effectiveness of AI technologies for fraud detection purposes

Технология ИИ	**Метод**	**Показатели эффективности**				
		Accuracy	**Precision**	**Recall**	**F1 Score**	**AUC-ROC**
Машинное обучение	Логистическая регрессия	0,92	0,89	0,85	0,87	0,94
	Дерево решений	0,94	0,91	0,88	0,89	0,94
Методы обнаружения аномалий	Кластерный анализ	0,85	-	-	-	0,88
Модели глубокого изучения	Нейронные сети	0,94	0,91	0,88	0,89	0,96
	Сверточные нейронные сети (CNN)	0,95	0,92	0,90	0,91	0,97
	Рекуррентные нейронные сети (RNN) и сети с долговременной краткосрочной памятью (LSTM)	0,93	0,89	0,87	0,88	0,95
Среднее значение		0,92	0,90	0,88	0,89	0,94
Размах вариации		0,10	0,03	0,05	0,04	0,09
Коэфф. вариации		0,04	0,01	0,02	0,02	0,03

Источник: составлено авторами с использованием данных Al-Kindi Center for Research and Development [Bello et al., 2024]

Постоянная гонка финансовых учреждений за усиленной безопасностью стимулирует мошенников постоянно адаптировать свои незаконные методы. Все это делает сложным предотвращение мошенничества, требуя непрерывности процесса адаптации и гибкости систем безопасности. Это подчеркивает необходимость развития систем обнаружения мошенничества на основе ИИ, которые могут выявлять развивающиеся схемы мошенничества.

Они облегчают процесс расследования случаев мошенничества, позволяя быстро и точно выявлять аномалии, отслеживать подозрительные транзакции и проводить более глубокий анализ кейсов на ранних стадиях, когда закономерности не очевидны широкому кругу заинтересованных лиц.

Согласно исследованию Международного журнала исследований в области прикладной науки и инженерных технологий (IJRASET) [Mohammad, 2024], технологии ИИ повышают эффективность выявления случаев мошенничества в среднем более чем на 70 % (табл. 3).

Как можно заметить, системы обнаружения мошенничества на основе ИИ весьма эффективны и способствуют снижению уровня мошенничества за счет обнаружения и предотвращения мошеннических действий в режиме реального времени. Использование на практике передовых ИИ-технологий помогает финансовым учреждениями более эффективно выявлять и сокращать число случаев мошенничества, минимизируя финансовые потери и защищая активы клиентов.

Проблемы и решения по развитию ИИ в финансовом секторе

Успешное внедрение цифровых технологий в финансовых учреждениях требует комплексного подхода. Хотя внедрение обещает значительное повышение эффективности

борьбы с мошенническими действиями, существует множество сложностей и проблем при интеграции ИИ-технологий в деятельность финансовых учреждений:

1. Совместимость систем. Многие банки используют в своей работе устаревшие системы, выбирая проверенную временем надежность. Это усложняет процесс интеграции ИИ в силу низкой совместимости передовых цифровых технологий со старыми системами. Например, 60 % банков испытывают трудности с интеграцией именно по этой причине [Mohammad, 2024]. Возможным решением данной проблемы может стать предшествующее обновление систем или интеграция на основе API – программного интерфейса для приложений, позволяющего разным программам взаимодействовать друг с другом, общаться между собой и обмениваться данными, следуя заданным правилам и способам.

2. Качество данных и стандартизация. Для лучшей работы ИИ-технологий им необходимо задавать высококачественную базу данных для улучшения точности и эффективности работы. В связи с этим около 40 % времени проекта интеграции ИИ уходит на подготовку и согласование данных, которые в будущем станут основой работы всей ИИ-технологии. Основными источниками данных являются: записи финансовых транзакций (включая суммы, временные метки, местоположения и данные о клиентах), дополнительные данные из внешних источников, которые могут предоставить дополнительный контекст для транзакций, записи известных мошеннических транзакций, которые имеют решающее значение для обучения моделей [Daraojimba et al., 2023]. Если повлиять на внешние источники данных сложнее, при работе с внутренней информацией оптимальным решением будет внедрение стандартизированных протоколов данных, которые преждевременно будут отбирать лишь необходимую информацию, автоматически очищая ненужные данные.

3. Необходимость обработки в реальном времени. Оптимальность многих ИИ-технологий достигается постоянной работой, направленной на анализ больших данных. Для этого требуются значительные вычислительные мощности, которых у финансовых учреждений может и не быть [Udeh et al., 2024]. Справиться с этой проблемой поможет использование облачных систем для производства необходимых вычислений.

4. Модель управления. Для управления цифровыми технологиями на основе ИИ необходимы эффективные модели управления внутри компаний, обеспечивающие надежность работы всех систем. Вариант решения данной проблемы – внедрение эффективной модели управления рисками.

5. Обучение персонала и недостаточные навыки. Для внедрения ИИ большие требования предъявляются к квалификации и компетентности персонала. Высокий разрыв знаний в области ИИ и науки о данных (Data Science) затрудняет работу и может привести к недостаточному использованию потенциала цифровых технологий. Решение – формирование комплексных программ обучения, затрагивающих как вопросы интеграции ИИ-технологий, так и цифровую аналитику.

6. Слабое сотрудничество финансовых учреждений и IT-фирм. Партнерства между финансовыми учреждениями и IT-фирмами способствуют облегчению обмена знаниями и передовой практикой, повышая эффективность использования цифровых технологий и ускоряя процесс внедрения ИИ-технологий для предотвращения мошенничества.

В результате проведенной работы были предложены решения для финансового сектора, которые помогут успешно внедрять и использовать технологии ИИ в своей практике для предотвращения мошенничества (рис. 6).

Таким образом, учет предлагаемых решений позволит финансовым учреждениям более эффективно внедрять и использовать ИИ для борьбы с мошенничеством и для защиты своих клиентов.

Таблица 3
Table 3

Анализ влияния ИИ-технологий на процедуру выявления мошенничества
Analysis of the impact of AI technologies on the fraud detection procedure

Технологии ИИ	Влияние на обнаружение мошенничества	Возникающие сложности
Машинное обучение	Повышение точности обнаружения мошенничества на 85 %	Для повышения эффективности требуются большие объемы данных с высоким качеством
Методы обнаружения аномалий	Рост скорости выявления новых схем мошенничества на 78 %	Изначально высокий уровень ложноположительных результатов в моделях
Обработка естественного языка	Рост обнаружения мошенничества на 70 %	Необходимость тщательно задавать контекст и детали для точности социальной инженерии
Модели глубокого изучения	Снижение ложных срабатываний на 92 %	Высокие вычислительные требования

Источник: составлено авторами на основе исследования IJRASET [Mohammad, 2024]

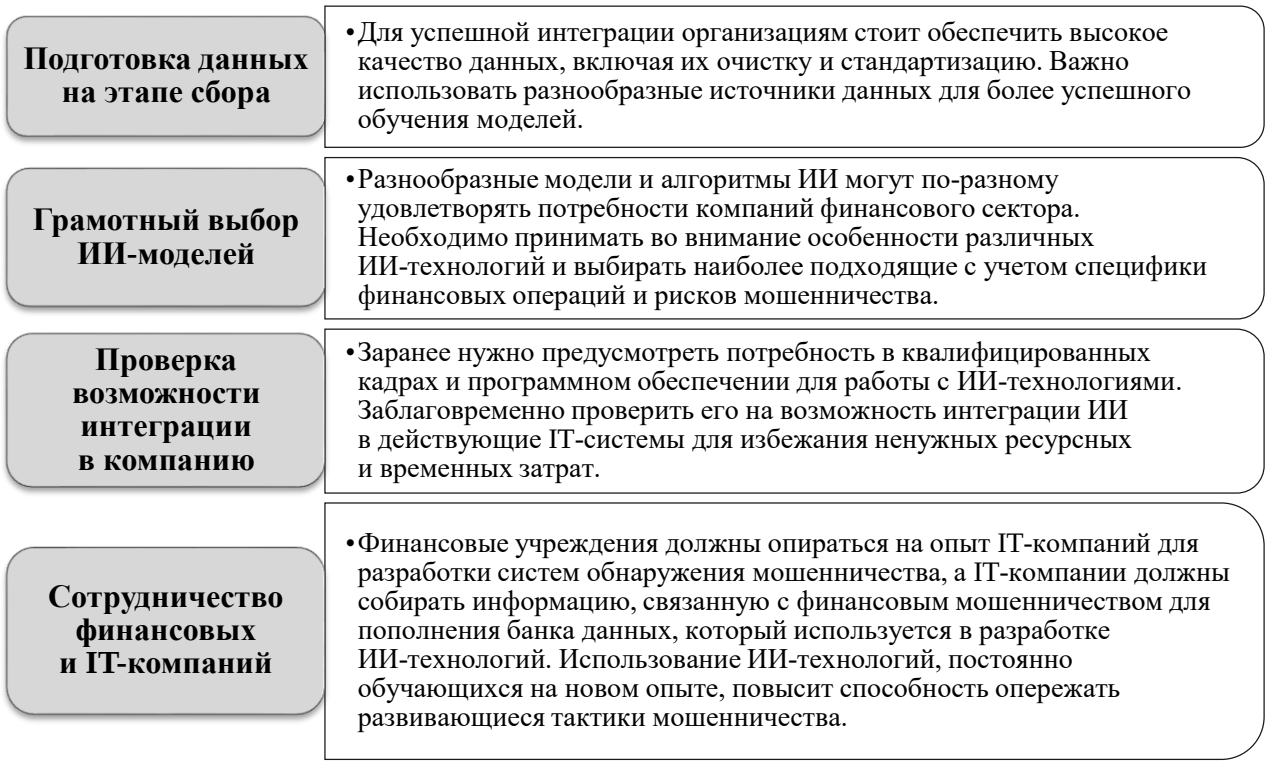

Рис. 6. Предлагаемые решения по развитию ИИ в целях предотвращения мошенничества в финансовом секторе
Fig. 6. Proposed solutions for the development of AI to prevent fraud in the financial sector
Источник: составлено авторами.

Заключение

В ходе проделанной работы мы пришли к тому, что использование цифровых технологий для обнаружения мошенничества в финансовой сфере обладает рядом преимуществ, делающих эти технологии приоритетными для изучения, развития и применения на практике. Несмотря на возникающие сложности в изучении данного вопроса, такие как постоянная изменчивость данных, сложность интеграции, соблюдение

правовых и этических аспектов, а также неполнота раскрытия конфиденциальной информации, стоит стремиться к повышению эффективности использования данных технологий, минуя существующие ограничения.

Изучение мирового опыта использования ИИ для предотвращения мошенничества позволяет осознать и сравнить, насколько эффективным является использование различных ИИ-технологий, а также насколько полезны данные технологии при борьбе с рисками мошенничества, в выявлении аномалий и идентификации подозрительных операций, проводимых финансовыми учреждениями. Использование ИИ-технологий при принятии решений гарантирует существенные возможности для моделирования схем мошенничества и адаптации к новым, постоянно меняющимся угрозам.

Однако использование ИИ не лишено проблем. Правовые и этические аспекты, проблемы конфиденциальности данных и потребность в объяснимости и рационализации решений ИИ являются критически важными вопросами, которые только предстоит решить.

Данное исследование может быть использовано в различных областях финансового сектора. Оно полезно для банковских и кредитных организаций, через которые регулярно проходит огромное количество денежных средств, подвергая их риску мошеннических действий, так и для страховых компаний, позволяя им преждевременно фиксировать потенциальную опасность среди своих клиентов и вовремя принимать меры реагирования против этих рисков. Сравнительный анализ различных ИИ-технологий поможет финансовым учреждениям выбрать наиболее эффективные алгоритмы, что снизит количество ложных срабатываний и улучшит общий пользовательский опыт.

Изученная тема может послужить поводом к дальнейшему изучению проблем интеграции ИИ-технологий в работу организаций, к анализу их фактического влияния на процесс выявления мошенничества. Также в условиях финансового сектора, где важна прозрачность принятия решений, будущие исследования могут сосредоточиться на разработке методов, позволяющих объяснять выводы ИИ. Нахождение ошибок в алгоритмах принятия решений и их исправление поможет повысить качество работы технологий. Наконец, важным аспектом будущих исследований будет изучение этических вопросов, связанных с использованием ИИ, что включает в себя вопросы конфиденциальности данных, предвзятости алгоритмов и потенциальных последствий для клиентов. Разработка этических стандартов и рекомендаций для использования ИИ в борьбе с мошенничеством станет важным шагом к безопасному и ответственному применению технологий.

Список источников

Индикаторы цифровой экономики: 2024: статистический сборник. 2024. В.Л. Абашкин, Г.И. Абдрахманова, К.О. Вишневский, Л.М. Гохберг и др. Нац. исслед. ун-т «Высшая школа экономики». М.: ИСИЭЗ ВШЭ, 276. ISBN 978-5-7598-3008-5. https://doi.org/10.17323/978-5-7598-3008-5

Паспорт федерального проекта «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации». 2020. Правительство Российской Федерации. URL: https://spa.msu.ru/wp-content/uploads/5-1.pdf (дата обращения 30.11.2024)

Дорожная карта развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект». 2019. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/uploaded/files/07102019ii.pdf (дата обращения 30.11.2024)

Estimated value of the financial sector's artificial intelligence (AI) spending worldwide in 2023, with forecasts from 2024 to 2027. 2024. Statista.com. URL: https://www.statista.com/statistics/1446037/financial-sector-estimated-ai-spending-forecast/ (дата обращения: 30.11.2024).

F1 Score in Machine Learning: Intro & Calculation. 2022. V7 Labs. URL: https://www.v7labs.com/blog/f1-score-guide (дата обращения: 30.11.2024).

Financial sector AI spending worldwide 2023, with forecasts to 2027. 2023. Statista. URL: https://www.statista.com/statistics/1446037/financial-sector-estimated-ai-spending-forecast/

How LLMs in banking enhance fraud detection, risk assessment, and credit evaluation // Pacific Data Integrators. PDI Marketing Team. URL: https://www.pacificdataintegrators.com/ (дат обращения: 30.11.2024).

Mayanard N. 2022. AI in Financial Fraud Detection: Key Trends, Competitor Leaderboard & Market Forecasts 2022-2027. JUNIPER Research. URL: https://www.juniperresearch.com/research/fintech-payments/fraud-identity/ai-financial-fraud-detection-trends-report/

Mayanard N. 2023. AI in Financial Fraud Detection Market Summary 2022-2027. JUNIPER Research URL: https://www.juniperresearch.com/resources/infographics/ai-financial-fraud-detection-infographic/

What are evaluation metrics in natural language processing? Alooba. URL: https://www.alooba.com/skills/concepts/natural-language-processing/evaluation-metrics/ (дата обращения: 30.11.2024).

Список литературы

Бабанская А.С., Груднева А.А. 2020. Анализ и оценка финансовых рисков. *Бухучет в сельском хозяйстве*, 4: 66–75.

Багреева Е.Г., Исмаилов Н.Э.О., Бобылева Л.М. 2022. Искусственный интеллект как противодействие мошенничеству в банковской сфере. *Евразийская адвокатура*, 2 (57): 90–95. https://doi.org/10.52068/2304-9839_2022_57_2_90

Беспалов Д.А., Богатырева М.В. 2023. Роль искусственного интеллекта в финансовом секторе. *Вестник Алтайской академии экономики и права*, 7-1: 10–16. DOI https://doi.org/10.17513/vaael.2892

Горян Э.В. 2019. Зарубежный опыт использования технологий искусственного интеллекта в обеспечении информационной безопасности банковского сектора. Территория новых возможностей. *Вестник Владивостокского государственного университета экономики и сервиса*, 11, 4: 62–73. https://doi.org/10.24866/VVSU/2073-3984/2019-4/062-073

Золотова Е.А., Калашникова Е.Ю., Чувилова О.Н., Гришанов С.М. 2023. Российская и зарубежная практика искусственного интеллекта в банковской деятельности и его значимость для бизнес-процессов. *Вестник Северо-Кавказского федерального университета*, 1 (94): 21–31. https://doi.org/10.37493/2307-907X.2023.1.3

Хоружий Л.И., Бабанская А.С., Трясцина Н.Ю. 2018. Мошенничество с финансовой информацией: анализ и оценка деловых партнеров. *Бухучет в сельском хозяйстве*, 5: 68–80.

Adelakun B.O., Antwi B.O., Fatogun D.T., Olaiya O.P. 2024. Enhancing audit accuracy: The role of AI in detecting financial anomalies and fraud. *Finance & Accounting Research Journal (FARJ)*, 6, 6: 1049–1068. https://doi.org/10.51594/farj.v6i6.1235

Bello O.A., Folorunso A., Onwuchekwa J., Ejiofor O.E., Budale F.Z., & Maryann Egwuonwu M.N. 2023. Analysing the impact of advanced analytics on fraud detection: a machine learning perspective. *European Journal of Computer Science and Information Technology*, 11 (6): 103–126. https://doi.org/10.37745/ejcsit.2013/vol11n6103126

Bello O.A., Ogundipe A., Mohammed D., Folorunso A., & Alonge O.A. 2024. AI-Driven approaches for real-time fraud detection in US financial transactions: challenges and opportunities. *European Journal of Computer Science and Information Technology*, 121(6): 88–106. https://doi.org/10.37745/ejcsit.2013/vol11n684102

Daraojimba R.E., Farayola O.A., Olatoye F.O., Mhlongo N., Oke T.T. 2023. Forensic accounting in the digital age: a U.S. perspective: scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, 5, 11: 342–360. https://doi.org/10.51594/farj.v5i11.614

Hasan M.F, Amanah A.A., Fadhil A.H., & Falih A.J. 2024. Corporate political responsibility in the digital age: trends and challenges. International Conference on Science, Innovations and Global Solutions, July: 165–172. https://doi.org/10.5281/zenodo.13701910

Kamuangu P.K. 2024. A review on financial fraud detection using AI and Machine Learning. *Journal of Economics, Finance and Accounting Studies (JEFAS)*, 6(1): 67–77. https://doi.org/10.32996/jefas.2024.6.1.7

Mohammad R. 2024. Generative AI in Fintech: advancing risk assessment and fraud detection in digital payment technologies. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 12, VIII: 1318–1326. https://doi.org/10.22214/ijraset.2024.64110

Toth Z., Blut M. 2024. Ethical compass: the need for corporate digital responsibility in the use of Artificial Intelligence in financial services. *Organizational Dynamics*, 53, 2: 101041. https://doi.org/10.1016/j.orgdyn.2024.101041

Udeh E.O., Amajuoyi P., Adeusi K.B., Scott A.O. 2024. The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, 22(02): 1746–1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

References

Babanskaya A.S., Grudneva A.A. 2020. Analysis and assessment of financial risks. *Accounting in agriculture*, 4: 66–75.

Bagreeva E.G., Ismailov N.E.O., Bobyleva L.M. 2022. Artificial intelligence as a means of counteracting fraud in the banking sector. *Eurasian Advocacy*, 2 (57): 90–95. https://doi.org/10.52068/2304-9839_2022_57_2_90

Bespalov D.A., Bogatyreva M.V. 2023. The role of artificial intelligence in the financial sector. *Bulletin of the Altai Academy of Economics and Law*, 7-1: 10–16. DOI https://doi.org/10.17513/vaael.2892

Goryan E.V. 2019. Foreign experience of using artificial intelligence technologies in ensuring information security of the banking sector. Territory of new opportunities. *Bulletin of Vladivostok State University of Economics and Service*, 11, 4: 62–73. https://doi.org/10.24866/VVSU/2073-3984/2019-4/062-073

Zolotova E.A., Kalashnikova E.Yu., Chuvilova O.N., Grishanov S.M. 2023. Russian and foreign practice of artificial intelligence in banking and its significance for business processes. *Bulletin of the North Caucasian Federal University*, 1 (94): 21–31. https://doi.org/10.37493/2307-907X.2023.1.3

Khoruzhy L.I., Babanskaya A.S., Tryascina N.Yu. 2018. Fraud with financial information: analysis and assessment of business partners. *Accounting in agriculture*, 5: 68–80.

Adelakun B.O., Antwi B.O., Fatogun D.T., Olaiya O.P. 2024. Enhancing audit accuracy: The role of AI in detecting financial anomalies and fraud. *Finance & Accounting Research Journal (FARJ)*, 6, 6: 1049–1068. https://doi.org/10.51594/farj.v6i6.1235

Bello O.A., Folorunso A., Onwuchekwa J., Ejiofor O.E., Budale F.Z., & Maryann Egwuonwu M.N. 2023. Analysing the impact of advanced analytics on fraud detection: a machine learning perspective. *European Journal of Computer Science and Information Technology*, 11 (6): 103–126. https://doi.org/10.37745/ejcsit.2013/vol11n6103126

Bello O.A., Ogundipe A., Mohammed D., Folorunso A., & Alonge O.A. 2024. AI-Driven approaches for real-time fraud detection in US financial transactions: challenges and opportunities. *European Journal of Computer Science and Information Technology*, 121(6): 88–106. https://doi.org/10.37745/ejcsit.2013/vol11n684102

Daraojimba R.E., Farayola O.A., Olatoye F.O., Mhlongo N., Oke T.T. 2023. Forensic accounting in the digital age: a U.S. perspective: scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, 5, 11: 342–360. https://doi.org/10.51594/farj.v5i11.614

Hasan M.F, Amanah A.A., Fadhil A.H., & Falih A.J. 2024. Corporate political responsibility in the digital age: trends and challenges. International Conference on Science, Innovations and Global Solutions, July: 165–172. https://doi.org/10.5281/zenodo.13701910

Kamuangu P.K. 2024. A review on financial fraud detection using AI and Machine Learning. *Journal of Economics, Finance and Accounting Studies (JEFAS)*, 6(1): 67–77. https://doi.org/10.32996/jefas.2024.6.1.7

Mohammad R. 2024. Generative AI in Fintech: advancing risk assessment and fraud detection in digital payment technologies. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 12, VIII: 1318–1326. https://doi.org/10.22214/ijraset.2024.64110

Toth Z., Blut M. 2024. Ethical compass: the need for corporate digital responsibility in the use of Artificial Intelligence in financial services. *Organizational Dynamics*, 53, 2: 101041. https://doi.org/10.1016/j.orgdyn.2024.101041

Udeh E.O., Amajuoyi P., Adeusi K.B., Scott A.O. 2024. The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, 22(02): 1746–1760. https://doi.org/10.30574/wjarr.2024.22.2.1575

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 03.12.2024
Поступила после рецензирования 24.01.2025
Принята к публикации 31.01.2025

Received December 03, 2024
Revised January 24, 2025
Accepted January 31, 2025

ИНФОРМАЦИЯ ОБ АВТОРАХ

Бабанская Анастасия Сергеевна, кандидат экономических наук, доцент кафедры экономической безопасности и управления рисками, Финансовый университет при Правительстве РФ, г. Москва, Россия
ORCID: 0000-0002-4695-1587

Ермольева Дарья Романовна, студентка 4 курса, Финансовый университет при Правительстве РФ, г. Москва, Россия
ORCID: 0009-0009-5911-3425

Ефименко Надежда Александровна, студентка 4 курса, Финансовый университет при Правительстве РФ, г. Москва, Россия
ORCID: 0009-0006-9843-4000

Акулова Софья Алексеевна, студентка 4 курса, Финансовый университет при Правительстве РФ, г. Москва, Россия
ORCID: 0009-0009-2222-0518

INFORMATION ABOUT THE AUTHORS

Anastasia S. Babanskaya, Candidate of Economic Sciences, Associate Professor of the Department of Economic Security and Risk Management, Financial University under the Government of the Russian Federation, Moscow, Russia
ORCID: 0000-0002-4695-1587

Daria R. Ermoleva, 4th year student, Financial University under the Government of the Russian Federation, Moscow, Russia
ORCID: 0009-0009-5911-3425

Nadezhda A. Efimenko, 4th year student, Financial University under the Government of the Russian Federation, Moscow, Russia
ORCID: 0009-0006-9843-4000

Sofia A. Akulova, 4th year student, Financial University under the Government of the Russian Federation, Moscow, Russia
ORCID: 0009-0009-2222-0518