ВЕСТНИК
КЕМЕРОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
СЕРИЯ: ГУМАНИТАРНЫЕ И ОБЩЕСТВЕННЫЕ НАУКИ

оригинальная статья

https://elibrary.ru/xjypjn

Цифровая трансформация платежных систем: проблемы мошенничества и перспективы развития средств и методов обнаружения

Абдурагимова Татьяна Иосифовна
Московский университет МВД России имени В. Я. Кикотя, Россия, Москва
eLibrary Author SPIN: 2009-0035
https://orcid.org/0009-0003-3771-5579
t.abduragimova@yandex.ru

Аннотация: В условиях стремительной цифровизации всех направлений человеческой деятельности, в том числе финансового сектора, ускоренной пандемией COVID-19, проблема мошенничества с кредитными картами приобретает особую актуальность. Данное исследование посвящено комплексному анализу современных технологий обнаружения мошеннических операций, включая методы искусственного интеллекта, обработки больших данных и облачных вычислений. Цель – осветить самые последние и актуальные разработки по обнаружению мошенничества с кредитными картами, влияющие на новые технологии в этой области. Особое внимание уделяется эволюции платежных систем, переходу от традиционных методов к инновационным решениям на основе IoT-устройств и биометрических данных. Рассматриваются ключевые уязвимости существующих систем безопасности, а также перспективные направления развития средств и методов обнаружения мошенничества. Анализируются современные подходы к обработке транзакционных данных, включая распределенные вычисления и машинное обучение, с акцентом на их эффективность в условиях динамично меняющегося поведения пользователей. Исследование подчеркивает необходимость интеграции разнородных источников, данных для повышения точности обнаружения мошеннических операций. Особую значимость приобретает изучение возможностей облачных технологий для создания систем, способных оперативно реагировать на новые виды мошенничества в реальном времени. Предлагаются направления будущих исследований, включающие разработку гибридных моделей на основе данных IoT-устройств и биометрических показателей.

Ключевые слова: мошенничество, банковские карты, цифровая трансформация, цифровые платежи, токенизация, биометрические системы, транзакции, искусственный интеллект, Интернет вещей (IoT)

Цитирование: Абдурагимова Т. И. Цифровая трансформация платежных систем: проблемы мошенничества и перспективы развития средств и методов обнаружения. *Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки*. 2025. Т. 9. № 3. С. 453–461. https://doi.org/10.21603/2542-1840-2025-9-3-453-461

Поступила в редакцию 19.05.2025. Принята после рецензирования 09.06.2025. Принята в печать 10.06.2025.

full article

Digital Transformation of Payment Systems: Fraud Issues and Detection Prospects

Tatyana I. Abduragimova
Moscow University of the Ministry of Internal Affairs of Russia, Russia, Moscow
eLibrary Author SPIN: 2009-0035
https://orcid.org/0009-0003-3771-5579
t.abduragimova@yandex.ru

Abstract: The COVID-19 pandemic boosted digitalization in all areas of human activity, including finances. As a result, the problem of credit card fraud is particularly relevant today. This comprehensive analysis highlights the latest and most relevant developments in the detection of credit card fraud, e.g., artificial intelligence, big data processing, and cloud computing methods. It focuses on the evolution of payment systems, including the shift from traditional methods to innovative solutions based on IoT devices and biometric data. The existing security systems remain vulnerable and require novel fraud detection tools and methods. The modern approaches to transaction data

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

processing include distributed computing and machine learning, which proved effective in the context of dynamically changing users' behavior patterns. Diverse data sources are needed to improve the accuracy of fraud detection. Cloud technologies can create systems capable of prompt response to new types of fraud in real time. Promising research directions include hybrid models based on data from IoT devices and biometric indicators.
Keywords: fraud, bank cards, digital transformation, digital payments, tokenization, biometric systems, transactions, artificial intelligence, Internet of things (IoT)

Citation: Abduragimova T. I. Digital Transformation of Payment Systems: Fraud Issues and Detection Prospects. *Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriia: Gumanitarnye i obshchestvennye nauki*, 2025, 9(3): 453–461. (In Russ.) https://doi.org/10.21603/2542-1840-2025-9-3-453-461

Received 19 May 2025. Accepted after review 9 Jun 2025. Accepted for publication 10 Jun 2025.

Введение

Устаревание наличных денег как основного способа оплаты, начавшееся в связи с развитием цифровой экономики, еще более ускорилось с пандемией COVID-19. В результате операции с кредитными картами стали доминирующей силой в мировой экономике. Различные заинтересованные стороны, включая финансовые учреждения, платежные системы и продавцов, постоянно стремятся использовать технологические достижения для более эффективного соответствия предпочтениям конечных пользователей.

Распространение устройств Интернета вещей (IoT), расширение возможностей подключения, системы оплаты в приложениях и повсеместное распространение мобильных устройств являются катализаторами как роста, так и разрушения экосистем платежей по кредитным картам. Например, такие организации, как Amazon Go, экспериментируют с платежными решениями на основе биометрических данных. Благодаря токенизации мобильные IoT-устройства [1, p. 13898], такие как смарт-часы, облегчают обмен информацией с близлежащими системами, позволяя совершать транзакции по требованию, и тем самым порождают новые парадигмы транзакционных коммуникаций.

Кредитные карты стали неотъемлемой частью онлайн-банкинга и широко используются в цифровых транзакциях и электронной коммерции. Однако эволюция и рост использования кредитных карт привели к появлению различных видов мошенничества. Мошенники используют все более изощренные методы для совершения незаконных операций, что приводит к значительным финансовым потерям как для держателей карт, так и для финансовых учреждений. Эти преступные действия варьируются от кражи и несанкционированного доступа к информации о кредитных картах до создания поддельных карт, которые имитируют поведение законных пользователей, что позволяет с беспрецедентной легкостью осуществлять незаконные действия.

Цель исследования – осветить самые последние и актуальные разработки по обнаружению мошенничества с кредитными картами, влияющие на новые технологии в этой области.

Результаты

Средства и методы обнаружения мошенничества и их развитие

Одновременно с этим нормализация данных и расширение применения нейронных сетей подчеркивают необходимость использования искусственного интеллекта (ИИ) и методов глубокого обучения для эмитентов кредитных карт и банковских служб [2–4]. Искусственный интеллект играет важную роль в разработке инновационных методик для выявления мошенничества с кредитными картами нового поколения, повышения уровня одобрения, минимизации отклоненных транзакций и проактивного контроля кредитных лимитов. Тем не менее интеллектуальная обработка банковских операций сопряжена с многочисленными трудностями, в том числе с необходимостью учета меняющегося поведения клиентов для обеспечения легитимности транзакций. В связи с этими динамичными изменениями и проблемами финансовые учреждения и процессоры платежей быстро модернизируют свои платежные технологии, что потенциально может привести к появлению уязвимостей в системе безопасности.

Поэтому крайне важно внедрять надежные и современные системы обнаружения мошенничества с кредитными картами. Надежная система обнаружения мошенничества классифицирует входящие транзакции на два различных класса: легитимные и нелегитимные. Мошенничество с кредитными картами может проявляться в двух основных формах: онлайн и офлайн. В случае онлайн-мошенничества злоумышленники совершают мошеннические покупки в Интернете, в то время как офлайн-мошенничество предполагает незаконные операции с использованием незаконно полученных кредитных карт.

Изощренность и адаптивность мошеннических действий требуют внедрения передовых механизмов обнаружения для защиты целостности финансовой экосистемы.

Анализ существующих исследований и современных проблем

В настоящее время опубликовано большое количество исследований, посвященных мошенничеству с кредитными картами, как отечественными авторами [5–8], так и зарубежными коллегами [9–13]. В этой связи крайне важно провести анализ освещаемых проблем и предлагаемых решений в целях формирования возможной «дорожной карты» в этой области. Несмотря на обилие исследований в данной сфере, в последнее время появилось много новых методов, что требует тщательного анализа. Кроме того, существующие обзоры в основном посвящены моделям обнаружения, а не использованию новых технологий и вычислительных методов. Поэтому в данной работе предлагается всестороннее рассмотрение нескольких аспектов обнаружения мошенничества с кредитными картами с акцентом на методы глубокого обучения и прорывные технологии.

Мошенничество, определяемое как хищение чужого имущества или приобретение права на него путем обмана либо злоупотребления доверием[1], получило широкое распространение с ростом использования электронных методов оплаты, таких как кредитные и дебетовые карты. Растущая популярность мобильного банкинга еще больше усугубила проблему, приведя к увеличению числа мошеннических платежных операций и, как следствие, финансовых потерь. Кредитные карты можно использовать для покупки товаров как онлайн, так и офлайн. Онлайн-платежи, не требующие физического присутствия карты, особенно уязвимы для атак, этот вид мошенничества известен как мошенничество без присутствия карты (Card-Not-Present, CNP)[2] [14; 15].

Технологические решения и будущие направления развития сферы противодействия мошенничеству с кредитными картами

Кроме того, особенно после пандемии COVID-19, все большее распространение получает использование бесконтактных платежей с помощью чиповых карт и мобильных устройств, использующих технологию Near Field Communication (NFC) [16, p. 10–11]. Эти способы оплаты используют беспроводную технологию ближнего радиуса действия для облегчения бесконтактных транзакций [17, p. 399]. В отличие от традиционных платежей, в платежах NFC участвуют два дополнительных партнера: производитель телефона и оператор мобильной связи. Политика безопасности этих партнеров может оказывать большее влияние на рынок телефонии, чем на рынок платежей [18, p. 95], что приводит к большим проблемам с безопасностью и подвергает клиентов большему количеству мошенничеств с виртуальными кредитными картами, чем с физическими. Хотя при таких платежах допускается взимание небольших сумм, мошенники могут изучить поведение пользователя и провести большое количество транзакций, прежде чем клиент сообщит об этом в банк.

Согласно отчету Единой европейской платежной зоны (Single European Payments Area (SEPA))[3], опубликованному в 2023 г. и анализирующему данные за 2021 г., общая стоимость мошеннических операций составила 1,53 млрд евро, из которых 84 % пришлись на CNP-платежи. Доля мошенничества в банкоматах и терминалах в точках продаж, напротив, снизилась до 5 % и 12 % от общего объема мошенничества соответственно. По сравнению с мошенничеством при предъявлении карты, мошенничество CNP в последние годы значительно возросло, что делает его серьезной проблемой для индустрии кредитных карт.

В этой связи стоит рассмотреть современные возможности обнаружения и противодействия мошенничеству с использованием банковских карт, выделить основные проблемы и направления будущих исследований, которые необходимо изучить.

В современном цифровом пространстве постоянно генерируются и собираются огромные объемы данных. Очевидно, что к настоящему времени человек получил широкую возможность использовать ИИ в практике повседневной жизни, например, при создании или обработке графических или текстовых файлов [19, с. 148], а растущее внедрение Интернета вещей (IoT), умных технологий и умных городов привело к появлению огромных массивов данных (Big Data), требующих обработки для получения более четких представлений у лиц, принимающих решения.

Термин *большие данные* (Big Data) был впервые введен в научный лексикон Клиффордом Линчем, главным редактором авторитетного научного журнала "Nature", в специальном тематическом выпуске

[1] Уголовный кодекс РФ. ФЗ № 63-ФЗ от 13.06.1996. Ст. 159. *СПС КонсультантПлюс*.

[2] INTERPOL. Global Financial Fraud Assessment. URL: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf (accessed 3 May 2025).

[3] Report on card fraud in 2020 and 2021. *Europa.eu*. URL: https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202305~5d832d6515.en.pdf (accessed 3 May 2025).

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

за 2008 г. В данной публикации акцент был сделан на феномен экспоненциального роста объемов глобальной информации, что свидетельствовало о начале новой эры в области обработки и анализа данных. Клиффорд Линч определил большие данные как массивы разнообразной информации, превышающие 150 Гб за сутки[4]. По мнению В. А. Мирончука, А. Л. Золкина, А. В. Батищева и А. Б. Урусова, большие данные представляют собой объемные массивы структурированной и неструктурированной информации, которые требуют сложных методов обработки с целью получения статистической, аналитической, прогностической и иной ценной информации для принятия решений [20, с. 228].

Как отмечают F. Doko и I. Miskovski, большие данные и наука о данных – это применение программного обеспечения и технологий, интегрированных с передовыми алгоритмами и методиками, для получения более глубоких знаний, подготовки обоснованных выводов, прогнозирования рисков и определения преимуществ [21]. Согласно Оксфордскому английскому словарю, большие данные являются информацией очень большого размера, как правило, в том смысле, что представляют серьезные трудности в материально-техническом обеспечении по манипуляциям и управлению ими; (также) направление вычислений с использованием такого типа данных[5].

Интересными являются не только дефиниции термина *большие данные*, но и характеристики и классификации этого феномена. Так, исследователь Лэйни охарактеризовал и классифицировал концепцию *больших данных* по объему (*volume*), скорости (*velocity*) и множеству (*variety*), известным как 3Vs [22]. В свою очередь еще одно четвертое "V" для описания больших данных, называемое правдивостью (*veracity*), добавила компания IBM [23]. В ряде работ в качестве еще одного 5-го "V" рассматривается ценность (*value*) [24], 6 – изменчивость (*variability*) добавляют исследователи Jeffrey Dean и Sanjay Ghemawat [25], 7 и 8 "V" ученые указывают как валидность (*validity*) и волатильность (*volatility*) [26].

Таким образом, большие данные включают в себя более крупные и сложные наборы данных, полученные преимущественно из новых и разнородных источников. Эти наборы данных характеризуются большим объемом, что делает традиционное (устоявшееся) программное обеспечение для обработки данных неадекватным. Тем не менее эти огромные объемы данных имеют неоценимое значение для поддержки бизнес-аналитики, особенно при обработке в режиме реального времени масштабных банковских данных, что повышает эффективность выявления мошенничества. Более того, технологии больших данных позволяют интегрировать разнородные данные из различных источников для более эффективного выявления мошеннических действий.

Параллелизм данных предполагает разделение большого набора данных на несколько узлов в рамках кластера. Каждый узел обрабатывает небольшую часть данных, а затем результаты объединяются для получения конечного результата. Такой подход отличается высокой эффективностью, позволяя быстро реагировать и оперативно принимать решения.

MapReduce от Google [27] обрабатывает данные параллельно на двух этапах: Map и Reduce. На этапе Map данные распределяются между отдельными заданиями на разных узлах. Каждое задание map создает набор пар ключ-значение, которые передаются заданиям reduce, также известным как reducers. Эти редукторы объединяют пары ключ-значение в меньший набор, который формирует конечный результат. Hadoop – основной фреймворк для анализа больших данных, основанный на MapReduce от Google, а также распределенной файловой системе HDFS [28, p. 1] и орхистраторе ресурсов Yarn [29, p. 2]. Однако Hadoop создает дополнительные накладные расходы, поскольку задачи отображения и сокращения данных считывают и записывают их на диск дважды. Это привело к разработке нового фреймворка – Spark [30, p. 287]. Основополагающим принципом Spark является способность обрабатывать данные в памяти, что значительно повышает эффективность и масштабируемость по сравнению с Hadoop. Spark похож на MapReduce, предоставляя функции отображения и сокращения, но поддерживает больше операций с большими и распределенными наборами данных, таких как фильтрация и SQL-подобные операции с распределенными и постоянными структурами данных, RDD и фреймами данных.

Поскольку объем данных о финансовых транзакциях продолжает значительно увеличиваться, надежное обнаружение мошеннических операций в режиме реального времени с помощью традиционных методов становится все более сложной задачей. Поэтому необходим подход к аналитике больших данных, который изучает закономерности на основе так называемых «больших исторических наборов данных» и использует распределенную инфраструктуру для облегчения интенсивных вычислений.

[4] Nature. Vol. 455, iss. 7209, 4 Sep 2008. URL: https://www.nature.com/nature/volumes/455/issues/7209 (accessed 3 May 2025).
[5] Oxford English Dictionary. URL: http://www.oed.com/view/Entry/18833#eid301162177 (accessed 3 May 2025).

 https://doi.org/10.21603/2542-1840-2025-9-3-453-461

Несмотря на важность распределенного подхода, нельзя не согласиться с исследователями H. Zhou, G. Sun, S. Fu, L. Wang, J. Hu и Y. Gao о том, что очень мало научных работ, посвященных использованию аналитики больших данных в рамках распределенной архитектуры для обнаружения и / или прогнозирования мошенничества с кредитными картами [31]. Таким образом, необходимы дополнительные исследования для создания систем реального времени и изучения проблем, которые могут препятствовать эффективному использованию таких технологий при сохранении конфиденциальности пользователей. Кроме того, интеграция множества данных из различных разнородных источников имеет решающее значение для получения более точных результатов. Помимо этого, все еще существует потребность в открытых наборах больших данных для поддержки исследователей в аналитике больших данных. Одним из возможных направлений исследований может стать разработка ценных синтетических наборов больших данных.

В этом контексте особую значимость приобретают облачные технологии, которые могут стать ключевым элементом в решении указанных проблем. Облачные технологии, определяемые как модель, обеспечивающая универсальный сетевой доступ к распределенным вычислительным ресурсам и хранилищам данных по запросу, которые выделяются и освобождаются автоматически, без прямого участия пользователя [32, с. 230]. Облачные вычисления отличаются пятью ключевыми аспектами: самообслуживание по требованию, широкий доступ к сети, объединение ресурсов [33, p. 47], быстрая эластичность и измеряемый сервис [34, p. 264]. Эти характеристики позволяют организациям совместно использовать ресурсы, гибко масштабировать их, приобретать и оплачивать ресурсы по требованию, обеспечивая тем самым многочисленные преимущества для управления бизнесом и минимизируя затраты. Облачные вычисления позволяют организациям постоянно совершенствовать свои стратегические возможности, одновременно снижая сложность бизнес- и ИТ-функций, что помогает им конкурировать на современном динамичном рынке. По прогнозам Gartner, в 2025 г. более 95 % новых цифровых рабочих нагрузок будет развертываться на облачных платформах, что значительно больше, чем это было в 2021 г.[6] Согласно ежегодному отчету Cloud Native Computing Foundation (CNCF) за 2023 г., 66 % респондентов заявили, что их организация уже использует облачные нативные технологии[7]. Такой стремительный рост рынка облачных вычислений привлек значительное внимание как научных, так и промышленных кругов.

В частности, облачные вычисления дают значительные преимущества для обнаружения мошенничества с кредитными картами с различных точек зрения, включая экономию средств и предоставление вычислительных мощностей. В облачных вычислениях нет ограничений на память, вычисления или хранение данных, поскольку в качестве ресурсов выступают крупные центры обработки данных. Все более широкое использование небольших устройств для обнаружения мошенничества с кредитными картами поднимает интригующие исследовательские вопросы об эффективности переноса вычислений в облако для разработки новых легких решений и алгоритмов для удаленных устройств. Кроме того, использование облачной архитектуры и повторное использование облачных интеллектуальных сервисов и инфраструктур может повысить эффективность обнаружения мошенничества с кредитными картами. Очень немногие исследования посвящены облачным вычислениям для обнаружения мошенничества с кредитными картами, что открывает несколько направлений исследований в этой области, таких как использование облаков для сбора и хранения данных о клиентах, а также вычислений и моделей искусственного интеллекта, размещенных в облаке. Кроме того, объединение разнородных источников, данных и обеспечение совместимости между несколькими организациями может повысить эффективность обнаружения мошенничества в режиме реального времени.

В будущих исследованиях можно изучить объединенное машинное обучение и использование облачных / краевых вычислений для моделирования проблемы обнаружения мошенничества с кредитными картами в виде распределенной системы машинного обучения, которая включает множество разнородных наборов данных из нескольких банков, сохраняя при этом конфиденциальность данных о держателях карт. Этот подход позволяет использовать распределенную природу облачных и краевых вычислений для локальной обработки данных, уменьшая задержки и повышая конфиденциальность. Интегрируя данные из различных источников и используя передовые методы машинного обучения, эта система может обеспечить более точное и своевременное обнаружение мошенничества,

[6] Gartner says cloud will be the Centerpice of new digital experiences. *Gartner*. 10.11.2021. URL: https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences (accessed 3 May 2025).

[7] Cloud native 2023: The undisputed infrastructure of global technology. URL: https://www.cncf.io/reports/cncf-annual-survey-2023/ (accessed 3 May 2025).

BULLETIN
KEMEROVO STATE UNIVERSITY
SERIES: HUMANITIES AND SOCIAL SCIENCES

в конечном итоге защищая финансовые учреждения и потребителей от мошеннических действий.

Таким образом, интеграция облачных технологий в систему обнаружения мошенничества с кредитными картами открывает перспективные возможности для повышения эффективности и результативности систем обнаружения мошенничества. Решив открытые исследовательские вопросы и изучив потенциал объединенного машинного обучения и облачных / краевых вычислений, эта область может добиться значительных успехов в борьбе с мошенничеством с кредитными картами и обеспечении безопасности финансовых операций. Однако, помимо облачных технологий, современная финансовая экосистема испытывает трансформационное влияние еще одного технологического прорыва.

Расцвет технологии Интернета вещей (IoT) катализирует глобальные изменения парадигмы в сфере платежей по кредитным картам, вызывая значительные метаморфозы в глобальном секторе финансовых услуг. Цифровые платежи переживают стремительную эволюцию, чему способствуют растущий потребительский спрос на удобные, взаимосвязанные платежные решения и прилив современных инновационных технологий. Помимо все более совершенных технологий анализа данных, искусственного интеллекта и облачных архитектур, одной из наиболее разрушительных технологий, оказывающих влияние на индустрию кредитных карт, является IoT. Экосистема IoT развивается ускоренными темпами, обеспечивая значительный рост во многих областях [35, p. 112]. По прогнозам, в ближайшее десятилетие она будет развиваться по экспоненте[8]. По данным Statista, в 2025 г. мировые расходы на технологии IoT могут достичь 342,5 млрд долларов, причем финансовые услуги являются одним из секторов, наиболее тесно связанных с их внедрением[9].

За последнее десятилетие каждый смартфон превратился в потенциальный инструмент для совершения покупок. В ближайшем будущем все устройства должны стать платформами для приобретения товаров и услуг. Это привело к появлению концепции Интернета платежей (Internet of Payments, IoP)[10]. Хотя эта терминология остается относительно неизученной в научных кругах, она набирает обороты в промышленном контексте благодаря сотрудничеству с производителями IoT. Mastercard и Visa являясь «пионерами» в области IoP-услуг, предлагают различным организациям новые решения, направленные на обеспечение бесперебойных карточных платежей через устройства, подключенные к IoT. Этому способствуют носимые IoT-устройства, которые заменяют традиционную кредитную карту.

IoP проникает в огромное количество аспектов нашей повседневной экономической и социальной деятельности. Пандемия COVID-19 увеличила объем онлайн-транзакций и побудила многих потребителей перейти на обслуживание к онлайн-провайдерам, что привело к росту платежей через IoT-устройства и мобильные телефоны [36, p. 3414].

Стремительное распространение мобильных и IoT-сервисов финансовых платежей не только обеспечило удобство и эффективность для потребителей, но и создало дополнительные скрытые риски мошенничества. Запутанные сети, лежащие в основе этих услуг, могут стать питательной средой для мошеннических действий, совершаемых преступниками. Управление и снижение риска мошенничества становится все более сложной задачей, т. к. частота мошеннических действий возрастает, что приводит к значительным денежным потерям коммерческих банков и финансовых учреждений.

Возможные направления будущих исследований могут включать рассмотрение гибридных наборов данных, объединяющих как транзакционные данные, так и внешние данные, собранные с IoT-устройств. Значительный прогресс может принести разработка новых системных конструкций и методик обучения с использованием данных, собранных с IoT-устройств. Кроме того, биометрические поведенческие данные, собранные с IoT-устройств, могут быть использованы для аутентификации пользователей и предотвращения мошеннических операций. Следовательно, изучение новых моделей обнаружения и аутентификации необходимо для решения проблемы мошенничества с кредитными картами в эпоху IoT.

Заключение

Пересечение IoT и операций с кредитными картами представляет собой сложную и многогранную проблему, требующую применения передовых научных методологий и технологий. Благодаря интеграции

[8] 60+ Amazing IoT Statistics (2024–2030). URL: https://explodingtopics.com/blog/iot-stats (accessed 3 May 2025).

[9] State of IoT 2024: Number of connected IoT devices growning 13% to 18.8 billion globally. URL: https://iot-analytics.com/number-connected-iot-devices/; Naveen Kumar. Internet of Things (IoT) Statistics: Market & Growth Data. 05.07.2025. URL: https://www.demandsage.com/internet-of-things-statistics/ (accessed 3 May 2025).

[10] SEALSQ integrates internet of payment (IoP) in next-generation IoT-enabled semiconductors, revolutionizing connected commerce. URL: https://www.sealsq.com/investors/news-releases/sealsq-integrates-internet-of-payment-iop-in-next-generation-iot-enabled-semiconductors-revolutionizing-connected-commerce (accessed 3 May 2025).

 https://doi.org/10.21603/2542-1840-2025-9-3-453-461

гибридных наборов данных, использованию биометрических поведенческих данных и разработке инновационных систем финансовый сектор может расширить свои возможности по выявлению и смягчению последствий мошеннических действий, тем самым обеспечивая целостность глобальной финансовой экосистемы В этом контексте особенно актуальным становится утверждение исследователя И. С. Лукинского о том, что в эпоху промышленной революции использование открывающихся перспектив при одновременном решении возникающих проблем будет играть существенную роль в дальнейшем развитии возможностей раскрытия, расследования и предупреждения преступлений [37, с. 510].

Таким образом, развитие технологий IoT и финансов, основанных на данных, оказывает серьезное влияние на повседневную жизнь и поведение клиентов. Цифровые платежи быстро распространяются и приобретают все большее значение, в основном после пандемии COVID-19.

Конфликт интересов: Автор заявил об отсутствии потенциальных конфликтов интересов в отношении исследования, авторства и / или публикации данной статьи.
Conflict of interests: The author declared no potential conflict of interests regarding the research, authorship, and / or publication of this article.

Литература / References

1. Liu W., Wang X., Peng W. State of the art: Secure mobile payment. *IEEE Access*, 2020, 8: 13898–13914. https://doi.org/10.1109/ACCESS.2019.2963480
2. Сумина А. В. Возможности искусственного интеллекта в раскрытии, расследовании и предупреждении преступлений. *Актуальные проблемы права и правоприменительной деятельности: региональные аспекты*: Всерос. науч.-практ. конф. (Краснодар, 27 октября 2023 г.) Краснодар: Краснодарский университет МВД России, 2024. С. 179–181. [Sumina A. V. Possibilities of artificial intelligence in the detection, investigation, and prevention of crimes. *Actual problems of law and law enforcement activity*: *Regional aspects*: Proc. All-Russian Sci.-Prac. Conf., Krasnodar, 27 Oct 2023. Krasnodar: Krasnodar University of the MIA of Russia, 2024, 179–181. (In Russ.)] https://elibrary.ru/yxcvqr
3. Сумина А. В. Внедрение информационных технологий в правоохранительную деятельность: возможности искусственного интеллекта в раскрытии, расследовании и предупреждении преступлений. *Информационные технологии в деятельности органов внутренних дел*: Междунар. науч.-практ. конф. (Москва, 18 апреля 2024 г.) М.: Московский университет МВД РФ им. В. Я. Кикотя, 2024. С. 266–268. [Sumina A. V. Introduction of information technology in law enforcement: The possibilities of artificial intelligence in the detection, investigation, and prevention of crime. *Information technology in the activities of internal affairs*: Proc. Intern. Sci.-Prac. Conf., Moscow, 18 Apr 2024. Moscow: V. Y. Kikotya Moscow University of the MIA of the Russian Federation, 2024, 266–268. (In Russ.)] https://elibrary.ru/hwnxbv
4. Васильева Ю. Д., Сумина А. В. Использование искусственного интеллекта в правоохранительной деятельности: потенциальные возможности применения для раскрытия и расследования преступлений. *Право, общество, государство: проблемы истории, теории и практики*: Всерос. науч.-практ. конф. (Старотеряево, 12 апреля 2024 г.) М.: Московский университет МВД России им. В. Я. Кикотя, 2024. С. 547–551. [Vasilieva Y. D., Sumina A. V. Artificial intelligence in law enforcement: Potential applications for crime detection and investigation. *Law, society, and state: Problems of history, theory, and practice*: Proc. All-Russian Sci.-Prac. Conf., Moscow, 12 Apr 2024. Staroteryaevo: V. Y. Kikotya Moscow University of the MIA of Russia, 2024, 547–551. (In Russ.)] https://elibrary.ru/qmfidx
5. Абдурагимова Т. И. Раскрытие и расследование изготовления, сбыта и использования поддельных кредитных и расчетных пластиковых карт: дис. … канд. юрид. наук. М., 2001. 201 с. [Abduragimova T. I. *Disclosure and investigation of manufacturing, sale, and use of counterfeit credit and settlement plastic cards*. Cand. Law Sci. Diss. Moscow, 2001, 201. (In Russ.)] https://elibrary.ru/nntouz
6. Сучкова Е. А. Исследование личности преступника в ходе расследования неправомерного оборота средств платежей. *Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова*. 2024. № 3. С. 258–265. [Suchkova E. A. Investigation of the identity of the perpetrator in the course of investigation of illegal circulation of means of payment. *Scientific Bulletin of the Orel Law Institute of the Ministry of the Interior of Russia named after V. V. Lukyanov*, 2024, (3): 258–265. (In Russ.)] https://elibrary.ru/cvztfo
7. Филиппов М. Н. Методика расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов. *Ведомости уголовно-исполнительной системы*. 2015. № 5. С. 26–30. [Filippov M. N. Technique of investigation of thefts and frauds, committed with the use of credit cards of bank details. *Vedomosti penal-executive system*, 2015, (5): 26–30. (In Russ.)] https://elibrary.ru/uygmnj

8. Мещеряков В. А. Теоретические основы механизма следообразования в цифровой криминалистике. М.: Проспект, 2022. 176 с. [Meshcheryakov V. A. *Theoretical foundations of the mechanism of trace formation in digital forensics*. Moscow: Prospect, 2022, 176. (In Russ.)] https://elibrary.ru/ejfpkb
9. Al Hashedi K. G., Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, 2021, 40. https://doi.org/10.1016/j.cosrev.2021.100402
10. Yvan Lucas, Johannes Jurgovsky. Credit card fraud detection using machine learning: A survey. *arXiv*, 2020. https://doi.org/10.48550/arXiv.2010.06479
11. Popat R., Chaudhary J. A survey on credit card fraud detection using machine learning. *2018 2nd International conference on trends in electronics and informatics (ICOEI)*: Proc. Conf., Tirunelveli, 11–12 May 2018. IEEE, 2018, 1120–1125. https://doi.org/10.1109/ICOEI.2018.8553963
12. Kanika, Singla J. A survey of deep learning based online transactions fraud detection systems. *2020 International conference on intelligent engineering and management (ICIEM)*: Proc. Conf., London, 17–19 Jun 2020. IEEE, 2020, 130–136. https://doi.org/10.1109/ICIEM48762.2020.9160200
13. Mittal S., Tyagi S. Computational techniques for real-time credit card fraud detection. *Handbook of computer networks and cyber security*, eds. Gupta B., Perez G., Agrawal D., Gupta D. Cham: Springer, 2020. https://doi.org/10.1007/978-3-030-22277-2_26
14. Singh A., Jain A. An empirical study of AML approach for credit card fraud detection–financial transactions. *International Journal of Computers Communications & Control*, 2019, 14(6): 670–690. https://doi.org/10.15837/ijccc.2019.6.3498
15. DiGabriele J., Heitger L., Riley R. A synthesis of non-fraud forensic accounting research. *Journal of Forensic Accounting Research*, 2020, 5(1): 257–277. https://doi.org/10.2308/JFAR-19-034
16. Hossein Motlagh N. *Near field communication (NFC) – A technical overview*. Dr. Diss. 2012, 73. https://doi.org/10.13140/RG.2.1.1232.0720
17. Vishwakarma P. P., Tripathy A. K., Vemuru S. Fraud detection in NFC-enabled mobile payments: A comparative analysis. *Innovative data communication technologies and application*, eds. Raj J. S., Iliyasu A. M., Bestak R., Baig Z. A. Singapore: Springer, 2021, vol. 59, 397–403. https://doi.org/10.1007/978-981-15-9651-3_34
18. Pasquet M., Gerbaix S. The complexity of security studies in NFC payment system. *Australian information security management conference*: Proc. 8 Conf., Perth, 30 Nov 2010. Pert: Cowan University, 2010, 95–101. https://doi.org/10.4225/75/57b674cb34783
19. Лукинский И. С., Горшенева И. А. Промт-инжиниринг в образовательном процессе и научной деятельности или к вопросу о необходимости обучения работе с искусственным интеллектом. *Психология и педагогика служебной деятельности*. 2024. № 4. С. 148–154. [Lukinsky I. S., Gorsheneva I. A. Promt engineering in the educational process and scientific activity or to the question of the necessity of training to work with artificial intelligence. *Psychology and pedagogy of service activity*, 2024, (4): 148–154. (In Russ.)] https://doi.org/10.24412/2658-638X-2024-4-148-154
20. Мирончук В. А., Золкин А. Л., Батищев А. В., Урусова А. Б. Интеграция больших данных и аналитических возможностей в современные системы поддержки принятия решений. *Вестник Академии знаний*. 2023. № 5. С. 227–230. [Mironchuk V. A., Zolkin A. L., Batishchev A. V., Urusova A. B. Integration of big data and analytical capabilities into modern decision support systems. *Vestnik of the Academy of Knowledge*, 2023, (5): 227–230. (In Russ.)] https://elibrary.ru/decrqv
21. Doko F., Miskovski I. An overview of big data analytics in banking: Approaches, challenges and issues. *UBT international conference*. 2019, 11–17. URL: https://knowledgecenter.ubt-uni.net/conference/2019/events/270 (accessed 3 May 2025).
22. Laney D. 3D data management: Controlling data volume, velocity and variety. *META Group Research*. 2001. URL: https://diegonogare.net/wp-content/uploads/2020/08/3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (accessed 3 May 2025).
23. Schroeck M., Shockley R., Smart J. *Analytics: The real-world use of big data: How innovative enterprises extract value from uncertain data, Executive Report*. 2012. URL: https://www.researchgate.net/publication/315786855_Analytics_the_real-world_use_of_big_data_How_innovative_enterprises_extract_value_from_uncertain_data_Executive_Report (accessed 13 May 2025).
24. Gandomi A., Haider M. Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 2015, 35(2): 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007
25. Jeffrey Dean, Sanjay Ghemawat. MapReduce: Simplified data processing on large clusters. *Communications of the ACM*, 2008, 51(1): 107–113. https://doi.org/10.1145/1327452.1327492

26. Nawsher Khan, Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Zakira Inayat, Waleed Kamaleldin Mahmoud Ali, Muhammad Alam, Muhammad Shiraz, Abdullah Gani. Big Data: Survey, technologies, opportunities, and challenges. *The Scientific World Journal*, 2014, 2014(1): 1–18. https://doi.org/10.1155/2014/712826
27. Dean J., Ghemawat S. MapReduce: A flexible data processing tool. *Communications of the ACM*, 2019, 53(1): 72–77. https://doi.org/10.1145/1629175.1629198
28. Shvachko K. V., Kuang H., Radia S. R., Chansler R. J. The hadoop distributed file system. *2010 IEEE 26th Symposium on mass storage systems and technologies (MSST)*: Proc. Conf., Incline Village, NV, 3–7 May 2010. IEEE, 2010, 1–10. https://doi.org/10.1109/MSST.2010.5496972
29. Vavilapalli V. K., Murthy A. C., Douglas C., Agarwal S., Konar M., Evans R., Graves T., Lowe J., Shah H., Seth S., Saha B., Curino C., O'Malley O., Radia S., Reed B., Baldeschwieler E. Apache Hadoop YARN: Yet another resource negotiator. *SOCC '13: ACMsymposium on cloud computing*: Proc. Conf., California, 1–3 Oct 2013. NY: Association for Computing Machinery, 2013, 1–16. https://doi.org/10.1145/2523616.2523633
30. Madhavi A., Sivaramireddy T. Real-Time credit card fraud detection using spark framework. *Machine learning technologies and applications*, eds. Kiran Mai C., Brahmananda Reddy A., Srujan Raju K. Springer, 2021, 287–298. https://doi.org/10.1007/978-981-33-4046-6_28
31. Zhou H., Sun G., Fu S., Wang L., Hu J., Gao Y. Internet financial fraud detection based on a distributed big data approach with Node2vec. *IEEE Access*, 2021, 9: 43378–43386. https://doi.org/10.1109/ACCESS.2021.3062467
32. Мирончук В. А., Золкин А. Л., Мекшенева Ж. В., Поскряков И. А. Современные компьютерные системы поддержки принятия решений. *Естественно-гуманитарные исследования*. 2023. № 4. С. 228–231. [Mironchuk V. A., Zolkin A. L., Meksheneva Zh. V., Poskryakov I. A. Modern computer decision support systems. *Natural and Humanitarian Research*, 2023, (4): 228–231. (In Russ.)] https://elibrary.ru/ebeehk
33. Wischik D., Handley M., Braun M. B. The resource pooling principle. *ACM SIGCOMM Computer Communication Review*, 2008, 38(5): 47–52. https://doi.org/10.1145/1452335.1452342
34. Galante G., de Bona L. C. E. A survey on cloud computing elasticity. *2012 IEEE fifth international conference on utility and cloud computing*: Proc. Conf., Chicago, 5–8 Nov 2012. IEEE, 2012, 263–270. https://doi.org/10.1109/UCC.2012.30
35. Kumari P., Mishra S. P. Analysis of credit card fraud detection using fusion classifiers. *Computational intelligence in data mining*, eds. Behera H., Nayak J., Naik B., Abraham A. Singapore: Springer, 2019, vol. 711, 111–122. https://doi.org/10.1007/978-981-10-8055-5_11
36. Wiścicka-Fernando M. The use of mobile technologies in online shopping during the covid-19 pandemic – an empirical study. *Procedia Computer Science*, 2021, 192: 3413–3422. https://doi.org/10.1016/j.procs.2021.09.114
37. Лукинский И. С. Типология промышленных революций и их классификаций через призму инноваций в области технико-криминалистического обеспечения. *Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки*. 2023. Т. 7. № 4. С. 505–511. [Lukinsky I. S. Typology of industrial revolutions and their classifications through the prism of innovations in the field of technical and forensic support. *Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriia: Gumanitarnye i obshchestvennye nauki*, 2023, 7(4): 505–511. (In Russ.)] https://doi.org/10.21603/2542-1840-2023-7-4-505-511