Оригинальная статья / Original article

УДК 338.2

https://doi.org/10.21869/2223-1552-2025-15-5-269-283

Стратегия защиты цифрового сервиса от мошенников, пытающихся легализовать доходы, полученные преступным путём

А. Л. Сидоров[1] ✉

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)
ул. Профессора Попова, д. 5, г. Санкт-Петербург 197022, Российская Федерация

✉ e-mail: arseniiy.sidorov@gmail.com

Резюме

Актуальность. *Отмывание денег через цифровые платформы, включая криптовалюты и децентрализованные финансовые сервисы, представляет серьезную угрозу для финансовой системы. Злоумышленники используют кросс-чейн-мосты и кошельки-миксеры для маскировки происхождения средств, что затрудняет их отслеживание. Это создает вызовы для регулирующих органов и финансовых институтов, требуя разработки новых методов противодействия.*

Цель *– разработать эффективную стратегию борьбы с отмыванием денег на цифровых платформах.*

Задачи: *проанализировать существующие методы выявления мошенничества; выявить их недостатки; предложить пути их устранения и эмпирически проверить эффективность новой стратегии.*

Методология. *Использованы диалектический метод, анализ и синтез. Исследование базируется на изучении научной и экономической литературы. Рассмотрено применение машинного обучения и искусственного интеллекта для мониторинга транзакций в реальном времени и выявления аномалий. Особое внимание уделено усилению систем KYC (Know Your Customer) и AML (Anti-Money Laundering). Проведен статистический эксперимент для подтверждения гипотезы.*

Результаты *исследования и эксперимента показывают, что внедрение интегрированных аналитических систем, основанных на анализе больших данных и поведении пользователей, могут способствовать более эффективному выявлению и предотвращению финансовых преступлений. Важным элементом стратегии является активное взаимодействие между составными частями системы защиты, такими как идентификация, верификация и мониторинг поведения пользователя.*

Выводы. *Интеграция передовых технологий и сотрудничество с регуляторами позволяют минимизировать риски и обеспечивать соблюдение международных стандартов. Постоянное совершенствование технологий необходимо для адаптации к новым угрозам в цифровой экономике.*

Ключевые слова: *цифровое мошенничество; верификация; мониторинг транзакций; противодействие отмыванию денег; финансовые преступления.*

Конфликт интересов: *В представленной публикации отсутствует заимствованный материал без ссылок на автора и (или) источник заимствования, нет результатов научных работ, выполненных авторами публикации лично и (или) в соавторстве, без соответствующих ссылок. Автор декларирует отсутствие конфликта интересов, связанных с публикацией данной статьи.*

Для цитирования: Сидоров А. Л. Стратегия защиты цифрового сервиса от мошенников, пытающихся легализовать доходы, полученные преступным путём // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2025. Т. 15, № 5. С. 269–283. https://doi.org/10.21869/2223-1552-2025-15-5-269-283

Поступила в редакцию 16.08.2025 Принята к публикации 15.09.2025 Опубликована 31.10.2025

A strategy for protecting a digital service from fraudsters attempting to launder illegally obtained income

Arseniy L. Sidorov[1] ✉

[1] Saint Petersburg Electrotechnical University "LETI"
5 Professora Popova Str., Saint Petersburg 197022, Russian Federation

✉ e-mail: arseniiy.sidorov@gmail.com

Abstract

Relevance. *Money laundering through digital platforms, including cryptocurrencies and decentralized financial services, poses a serious threat to the financial system. Attackers use cross-chain bridges and mixer wallets to disguise the origin of funds, making it difficult to track them. This creates challenges for regulators and financial institutions, requiring the development of new counteraction methods.*

The purpose *is to develop an effective strategy to combat money laundering on digital platforms.*

Objectives: *to analyze existing fraud detection methods; identify their shortcomings; propose ways to eliminate them and empirically verify the effectiveness of the new strategy.*

Methodology. *The dialectical method, analysis and synthesis are used. The research is based on the study of scientific and economic literature. The application of machine learning and artificial intelligence for monitoring transactions in real time and detecting anomalies is considered. Special attention is paid to strengthening KYC (Know Your Customer) and AML (Anti-Money Laundering) systems. A statistical experiment was conducted to confirm the hypothesis.*

The results *of the research and experiment show that the introduction of integrated analytical systems based on the analysis of big data and user behavior can contribute to more effective detection and prevention of financial crimes. An important element of the strategy is active interaction between the components of the protection system, such as identification, verification and monitoring of user behavior.*

Conclusions. *The integration of advanced technologies and cooperation with regulators make it possible to minimize risks and ensure compliance with international standards. Continuous technology improvement is necessary to adapt to new threats in the digital economy.*

Keywords*: digital fraud; verification; transaction monitoring; anti-money laundering; financial crimes.*

Conflict of interest*: In the presented publication there is no borrowed material without references to the author and (or) source of borrowing, there are no results of scientific works performed by the author of the publication, personally and (or) in co-authorship, without relevant links. The author declares no conflict of interest related to the publication of this article.*

For citation: Sidorov A.L. A strategy for protecting a digital service from fraudsters attempting to launder illegally obtained income*. Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Ekonomika. Sotsiologiya. Menedzhment = Proceedings of the Southwest State University. Series: Economics, Sociology and Management*. 2025;15(5):269–283. (In Russ.) https://doi.org/10.21869/ 2223-1552-2025-15-5-269-283

Received 16.08.2025 Accepted 15.09.2025 Published 31.10.2025

***

Введение

Отмывание денег через цифровые сервисы становится все более распространенным явлением, особенно с ростом популярности финансовых технологий и криптовалют. Например, по данным Chainanalysis (вендор, предоставляющий услуги криптомониторинга), за 2024 г. около 71% незаконных криптовалютных средств были обналичены через всего не-

сколько фиатных обменников, что подчеркивает уязвимость этих систем [1]. Наиболее уязвимыми оказываются платформы, предлагающие быстрый доступ к финансовым услугам, включая криптовалютные кошельки и обменники, а также сервисы, предполагающие в своей бизнес-модели как ввод, так и вывод денежных средств пользователем. При этом преступники также стали более изобретательными, используя сложные схемы, такие как кросс-чейн-мосты и кошельки-миксеры для сокрытия следов своих операций, что делает задачу для правоохранительных органов сложнее [2]. По данным аналитических агентств и Европола, ежегодно через цифровые сервисы проходит до 1 трлн долл. США, связанных с незаконной деятельностью, что составляет примерно 5% от мирового ВВП. Эти данные свидетельствуют о критической необходимости усиления механизмов контроля и предотвращения мошенничества, особенно в условиях постоянного появления новых технологических решений, которые могут быть использованы преступникам [3].

Параллельно с этим объем цифровых платежей растет с невероятной скоростью, что создает дополнительные риски для финансовых компаний, вынужденных адаптировать свои системы для борьбы с мошенничеством и отмыванием денег [4]. Преступники активно используют слабые места таких систем, чтобы скрыть происхождение средств или вывести деньги из тени, что усложняет задачу регулирующим органам и повышает требования к системам контроля и мониторинга [5].

С учетом постоянно развивающегося характера мошеннических схем цифровым сервисам важно учитывать не только уже известные угрозы, но и быстро адаптироваться к новым вызовам. Например, с появлением технологий конфиденциальных транзакций (privacy coins) вроде Monero или Zcash [6] отслеживание незаконных операций становится еще сложнее из-за встроенной защиты анонимности [7]. Анализ Европола показывает, что объемы использования таких инструментов для отмывания денег растут ежегодно на 15–20%, что свидетельствует о необходимости разработки более продвинутых инструментов мониторинга и анализа данных. Этот фактор усиливает нагрузку на правоохранительные органы и регуляторов, а также требует более тесного сотрудничества между частными и государственными структурами.

С расширением цифровых технологий – от криптовалютных платформ до электронных платежных систем – увеличиваются возможности для незаконных финансовых операций. Анонимные криптовалютные транзакции создают особую сложность для правоохранительных органов, так как их можно проводить без привязки к географическим или регулятивным границам. Это подтверждается исследованиями по влиянию DeFi-платформ, где децентрализация и отсутствие посредников уменьшают возможности для контроля [8].

Также исследования показывают, что цифровые сервисы в странах с менее строгим регулированием сталкиваются с повышенным риском мошенничества и отмывания денег [9]. Мошенники выбирают наиболее уязвимую страну и сервис для повышения шанса успеха собственных схем. Ключевую роль в предотвращении отмывания денег играют международные стандарты, такие как рекомендации от Financial Action Task Force (FATF), которым необходимо следовать цифровым сервисам. Как отмечается в литературе, внедрение стандартов FATF, особенно в отношении верификации клиентов (KYC) [10] и мониторинга подозрительных транзакций (AML) [11], является обязательным для большинства цифровых платформ именно для предотвращения мошенничества с отмыванием денежных средств.

Отмывание денег через цифровые платформы не только подрывает их репу-

тацию, но и создает значительные финансовые риски для всех участников экосистемы [12]. Например, крупные штрафы за несоблюдение норм AML могут достигать миллионов долларов. Только в 2023 г. несколько глобальных цифровых платформ, включая крупные криптовалютные биржи, были оштрафованы на сумму более 2 млрд долл. [12] за несоблюдение стандартов KYC и AML [13]. Помимо этого, недоверие пользователей к платформам, которые не справляются с угрозами мошенничества, приводит к потере клиентской базы, что в долгосрочной перспективе угрожает их финансовой устойчивости.

Основной целью данного исследования, безусловно, является выявление стратегии, которая позволила бы цифровым сервисам защититься от такого рода мошенничества. Формирование данной стратегии будет основано на комбинации трех основных факторов. Во-первых, нами будут изучены текущие работы по данной теме в поисках конкретных рекомендаций, направленных предотвращение мошенничества. Во-вторых, нами будут изучены отчеты государственных органов и частных компаний, которые указывают на широкое распространение данной проблемы и также дают набор практических рекомендаций по противодействию мошенничества. Наконец, значительная часть стратегии будет основываться на собственной экспертизе автора в данном вопросе. Эффективность данной стратегии далее будет проверена на статистических данных.

Основной гипотезой данного исследования является предположение, что внедрение искусственного интеллекта (далее – ИИ) в интегрированную стратегию защиты, включающую этапы идентификации, верификации и мониторинга транзакций, позволяет сократить среднее время выявления подозрительных транзакций, связанных с отмыванием денег на цифровых платформах, по сравнению с традиционными методами, основанными на ручных проверках и строго заданных правилах, при сохранении уровня точности классификации. Под средним временем выявления понимается интервал между моментом совершения транзакции и моментом её пометки как подозрительной, а под точностью классификации – доля правильно классифицированных транзакций (легитимных и мошеннических) от общего числа транзакций. Конечно, более интересной метрикой для исследования являлось бы сравнение точности классификации, т. е. насколько ИИ повышает или, наоборот, понижает эффективность выявления мошенников. Однако статистически достоверно на данный момент мы не можем посчитать точность выявления мошенников из-за сложности оценки ложноотрицательных срабатываний. В контексте нашей гипотезы мы сможем проанализировать ложноположительные срабатывания (запрет транзакции честному пользователю), поскольку честные пользователи в таком случае обращаются с жалобами. Мошенники же в свою очередь затаиваются, и количество ложноотрицательных срабатываний крайне сложно исследовать. Для проверки гипотезы мы опираемся на статистические данные, которые позволяют измерить время выявления и долю ложноположительных срабатываний, обеспечивая воспроизводимость и объективность анализа.

Материалы и методы

В начале необходимо четко описать задачу цифрового мошенника в контексте нашего исследования. Легализация преступных доходов или отмывание денег в литературе описывается как процесс приведения незаконных финансов в законное обращение путем маскировки их происхождения [14]. Классическая модель отмывания денег включает три стадии: размещение, расслоение и интеграция. Согласно исследованиям, большинство цифровых сервисов вовлекаются во вторую стадию (расслоение), когда преступ-

ники пытаются скрыть источник средств с помощью множества транзакций через сложные схемы [15].

Мошенники преследуют основную цель – легализовать доход, который они уже получили преступным путем. Простыми словами, для легализации дохода через расслоение с помощью цифрового сервиса мошеннику необходимо сделать следующее: завести на цифровой сервис (криптообменник, банк, трейдинг-платформу, онлайн-казино и т. д.) денежные средства, а затем их вывести, тем самым их легализовав [16].

Цифровые сервисы не заинтересованы в такого рода клиентах по следующим причинам:

1) это преступники, а содействовать преступникам опасно для цифрового сервиса с точки зрения репутации. Более того, существует ряд законодательных актов, согласно которым цифровые сервисы должны бороться с такого рода мошенниками, например уже упомянутый FATF [17];

2) такие пользователи не используют цифровой сервис по своему назначению, а значит, не приносят прибыли для компании [18];

3) чаще всего в результате «прокрутки» большой суммы денег через цифровой сервис последний должен заплатить значительный процент от суммы платежной системе, таким образом теряя средства при работе с такого рода «клиентами» [18].

Интересно отметить, что в последние годы появляются исследования, которые акцентируют внимание на использовании ИИ для противодействия легализации незаконных доходов. Например, внедрение алгоритмов глубокого обучения позволяет не только анализировать исторические транзакции, но и выявлять скрытые закономерности в поведении пользователей, что ранее было практически невозможно. Тем не менее использование таких методов также сопряжено с рядом ограничений, включая необходимость обработки больших объемов данных [11] и возможные ошибки классификации, связанные с недостаточным качеством обучающего набора данных [19].

Сравнительный анализ подходов к борьбе с мошенничеством показывает, что наибольший успех достигается в странах, где внедрены гибридные модели противодействия. Такие модели комбинируют традиционные меры (сбор идентификационных данных) с инновационными технологиями, включая анализ больших данных (Big Data) и блокчейн-аналитику [19]. Например, в Сингапуре регуляторы активно сотрудничают с компаниями, предоставляющими криптовалютные услуги, разрабатывая специализированные платформы для мониторинга транзакций в реальном времени. Подобный опыт может быть полезен для стран с менее строгим регулированием, где мошенничество через цифровые сервисы остается значительной проблемой [20].

Таким образом, разработка стратегии защиты цифрового сервиса от мошенников, пытающихся легализовать доходы, полученные преступным путём, является крайне приоритетной задачей для науки и бизнеса сейчас. Разработанная нами стратегия может быть успешно применена для борьбы с цифровой легализацией незаконно полученных денежных средств. Более того, данная стратегия должна быть основана на использовании современных технологий, включая технологии анализа данных, ИИ, а также на анализе целей и задач самого мошенника.

Результаты и их обсуждение

Основным результатом нашего исследования, безусловно, является формулировка стратегии защиты цифровых сервисов от мошенников, занимающихся отмыванием денежных средств.

Перед формулированием конкретного набора шагов по предотвращению мошенничества данного вида необходимо явно выразить потенциальный ущерб от такого рода мошенничества. Представим

ущерб от мошенничества, который могут получить цифровые сервисы, в виде следующей формулы:

$$C_{ML} = C_{Admin} + C_{fines} + \\ + C_{lostprofit} + C_{Reputation}, \quad (1)$$

где C_{ML} – общая стоимость мошенничества от отмывания денег; C_{Admin} – административные затраты, включающие трудозатраты, ПО для анализа и проверки, комиссии платежных систем; C_{fines} – штрафы и санкции от регуляторов; $C_{lostprofit}$ – потерянная выгода из-за снижения доверия пользователей или временной блокировки операций, упущенные доходы из-за снижения активности пользователей; $C_{Reputation}$ – оценка стоимости репутационного ущерба, долгосрочные потери из-за утраты доверия.

Как видно из формулы (1), на общую стоимость данного вида мошенничества влияет множество факторов. Эффективная стратегия должна учитывать и предотвращать все факторы, указанные выше.

Стратегия предотвращения мошенничества состоит из следующих этапов работы с каждым пользователем платформы. Важно отметить, что все указанные ниже этапы должны быть применены к каждому пользователю цифрового сервиса:

1. *Идентификация пользователя.* Идентификация является первым этапом предотвращения мошенничества. При этом основной задачей данного этапа является создание аккаунта для пользователя и привязка к нему электронного почтового ящика и номера телефона, чтобы цифровой сервис мог отличить данного пользователя от других. Второстепенной же задачей является проверка, что данный почтовый ящик и номер телефона существует и действительно принадлежит пользователю. В цифровых сервисах, которые не предполагают вывод денежных средств из аккаунта, например онлайн-агрегатор по заказу такси со стороны пассажира, идентификация является единственным этапом проверки. Формально для получения мобильного номера российского оператора «Телеком», при заключении договора сотрудник на стороне оператора обязан произвести верификацию документа клиента. Таким образом, пользователи проходят идентификацию уже с верифицированным номером телефона. Однако номера телефонов часто передаются между родственниками, знакомыми или вовсе могут быть куплены у сторонних людей. В сервисах, более подверженных риску мошенничества, связанного с легализацией незаконно полученных денежных средств, одной лишь идентификации недостаточно, поскольку мошенник легко может создать новый почтовый ящик или использовать виртуальный номер телефона.

2. *Верификация пользователя (Know Your Customer).* Данная процедура является обязательным шагом стратегии по предотвращению легализации доходов, полученных незаконным путем. Верификация подразумевает сбор следующих данных: паспортные и личные данные: верификация личности через документы, удостоверяющие личность (паспорт, водительское удостоверение); проверка документа на подлинность; проверка возраста и срока действия документа. Важный аспект проверки на данном этапе – это анализ документа на поддельность. Необходимо проверить, не является ли документ распечатанным, нет ли на нем следов физического редактирования, нет ли следов графических редакторов и т. д.

Адрес проживания: подтверждение адреса с помощью коммунальных счетов или банковских выписок, что позволяет проверить, находится ли пользователь в юрисдикции с соблюдением нормативных требований. Верификация адреса проживания – крайне сложная задача, поскольку в отличие от идентифицирующих документов на коммунальных счетах или банковских выписках нет голограмм или других элементов безопасности, а значит, подделать данный тип документа достаточно просто.

Селфи или биометрическая проверка: необходимо проводить биометрическую проверку всех пользователей, запрашивать селфи для сверки лица пользователя с лицом в документе. При этом одной лишь сверки лиц недостаточно. Верификационная система также должна быть способна распознавать основные мошеннические уловки, такие как: маски, фотографии экранов, картины лиц и т. д. Одной из самых опасных угроз на данном этапе, безусловно, является технология Deepfake. С распространением генеративного искусственного интеллекта создать дипфейк любого человека стало невероятно просто. Больше не нужно иметь специальных навыков, достаточно лишь нажать несколько кнопок. Современные технологии позволяют повысить уровень надежности биометрической верификации. Например, использование многомодальной биометрии, которая включает сочетание нескольких факторов, таких как голос, отпечатки пальцев и сканирование радужной оболочки глаза, минимизирует риски обхода систем безопасности. Такие решения особенно эффективны при работе с высокорисковыми пользователями, связанными с криптовалютными транзакциями или финансовыми переводами больших сумм. Однако внедрение таких систем требует значительных финансовых вложений и высокой вычислительной мощности.

Верификация также должна включать проверку пользователя по спискам политически значимых лиц (PEP) и санкционным спискам. Платформы обязаны отслеживать пользователей, связанных с политикой или юридическими санкциями, так как они чаще вовлекаются в схемы отмывания денег. Важно убедиться, что для верификации используются все современные технологии, такие как Liveness Check, способность выявлять дипфейки, проверка на графические редакторы, анализ поведения пользователя, поведенческая биометрия и т. д. В противном случае даже при наличии этапа верификации часть мошенников все равно смогут обмануть систему.

3. *Мониторинг транзакций и поведения пользователя.* Данная процедура также является обязательным пунктом стратегии по предотвращению цифрового мошенничества. Ее суть заключается в использовании инструментов, отслеживающих и анализирующих поведение пользователей в реальном времени. Модели машинного обучения обучаются на типичных действиях пользователей и могут быстро идентифицировать подозрительные транзакции или действия, совершенные пользователем. Эти системы помогают выявлять случаи, когда пользователь пытается вывести средства через сложные схемы или когда объем операций не соответствует обычному поведению данного клиента цифрового сервиса. Система должна быть реализована следующим способом.

Во-первых, система должна работать в режиме реального времени и в случае обнаружения подозрительной активности не давать вывести деньги, блокируя транзакцию, или в случае сомнений отправлять данную транзакцию на дополнительную проверку.

Во-вторых, методология выявления подозрительной активности должна базироваться на двух основных аспектах, эффективность которых мы как раз и будем сравнивать в нашем эксперименте ниже. Первый аспект – это строго заданные правила работы системы и анализа транзакций. Одним из примеров таких правил может служить следующее: если пользователь решил вывести сумму денег более определенной границы, то его транзакция становится на паузу для детального рассмотрения юристом. Второй аспект – помимо правил, которые работают по жесткой прописанной логике, необходимо использовать алгоритмы ИИ машинного обучения, которые будут постоянно анализировать поведение всех пользователей и выявлять аномалии. ИИ в данном случае может играть роль «тре-

тьей руки» для контроля за теми пользователями, которые не будут выявлены правилами или специалистами цифрового сервиса, а также может, наоборот, проактивно выявлять мошенников до срабатывания строго заданных правил.

Также специалистами цифрового сервиса должна быть построена модель оценки транзакций с целью выявления мошеннических. Набор регрессоров будет отличаться в зависимости от цифрового сервиса, но сама модель может выглядеть следующим образом:

$$P(Y = 1) = \\ = \frac{1}{1+e^{-(\beta_0+\beta_1 X_1+\beta_2 X_2+\cdots+\beta_n X_n)}}, \quad (2)$$

где $P(Y = 1)$ – вероятность того, что транзакция является мошеннической, $X_1, X_2, ..., X_n$ – факторы, влияющие на риск мошенничества (например, размер транзакции, частота транзакций и т. д.).

В данном примере мы представили обычную логистическую модель предсказания вероятности, что конкретный пользователь является мошенником. Помимо данной модели также рекомендуется использовать методы градиентного бустинга, например Catboost, для выявления ключевых поведенческих «красных флагов» пользователей.

Помимо моделей, указанных выше, сервисы могут использовать кластеризацию данных пользователей и построение социальных графов, которые помогают выявлять взаимосвязи между анонимными аккаунтами. Например, в 2022 г. одна из крупных криптовалютных бирж обнаружила мошенническую сеть из более чем 1 000 связанных аккаунтов, что стало возможным благодаря анализу транзакционных паттернов и социального графа пользователей. Метод графов работает таким образом, что постоянно анализирует пользователей, а также их основные цифровые атрибуты. Например, если одно устройство используется множеством пользователей, они будут связаны в социальный граф. Помимо устройства кластеризация может проходить также на основе e-mail, номера телефона, локации, IP-адреса, общего фона на фотографии документов и т. д.

4. *Взаимодействие верификации и мониторинг транзакций и поведения пользователя*. Ключевой фактор успеха и надежности всей стратегии по выявлению мошенников подобного рода – это наличие сквозной аналитики между указанными выше этапами проверки пользователя. Идентификация, верификация и мониторинг должны обмениваться данными, чтобы предоставлять специалистам цифрового сервиса полную картину по каждому конкретному пользователю. Это позволит оперативно выявлять мошенников и принимать правильные решения на основе данных. В случае, если верификация пользователя и мониторинг его поведения осуществляются с помощью разных систем, цифровому сервису будет крайне сложно эффективно выявлять мошенников по следующим причинам:

1) системы могут быть построены на разной архитектуре, а значит, разработчикам будет крайне трудно или невозможно интегрировать их между собой;

2) даже в случае успешной интеграции часть данных может теряться, что негативно скажется на информированности юриста или комплаенс-офицера при принятии решения по конкретному пользователю;

3) взаимодействуя с двумя-тремя системами вместо одной, комплаенс-офицер или другой человек, осуществляющий контроль за пользователями с точки зрения предотвращения мошенничества, тратит гораздо больше времени на анализ всех событий по каждому пользователю, а значит, снижается операционная эффективность и увеличиваются затраты.

Наконец, проведём эксперимент с использованием статистических данных для проверки предложенной гипотезы. К сожалению, из-за соглашения о неразглашении мы не можем раскрыть источник данных, однако можем описать их

структуру и методологию анализа. Для эксперимента был проведён А/Б-тест с использованием датасета транзакционных данных. Датасет включает 100 000 пользовательских транзакций, каждая из которых была предварительно классифицирована как легитимная или подозрительная. Транзакции были собраны за период с 1 января 2024 г. по 31 декабря 2024 г. и включают такие параметры, как сумма транзакции, время её совершения, геолокация, устройство пользователя, IP-адрес и результаты первичной классификации. Перед экспериментом транзакции были несколько раз проверены на то, насколько верно они были классифицированы, чтобы результаты эксперимента были достоверны. Далее, данный сет транзакций был отправлен на анализ под видом «новых».

В рамках А/Б-теста транзакции были разделены на две группы по 50 000 транзакций в каждой:

1) *контрольная группа (традиционный метод)*. Транзакции классифицировались с использованием строго заданных правил, таких как пороговые значения суммы транзакции (например, транзакции свыше 10 000 долл. автоматически помечались как подозрительные) и базовые проверки на совпадение с санкционными списками. При выявлении подозрительной транзакции она отправлялась на ручную проверку специалистом (вторичная классификация);

2) *экспериментальная группа (ИИ-метод)*. Транзакции классифицировались с использованием модели ИИ, основанной на алгоритмах машинного обучения (логистическая регрессия и градиентный бустинг CatBoost). Модель была предварительно обучена на выборке из 500 000 транзакций, размеченных как легитимные или мошеннические, с использованием признаков, таких как частота транзакций, сумма, геолокация, устройство и поведенческие паттерны. При выявлении подозрительной транзакции она также отправлялась на вторичную ручную проверку.

Основное опасение исследователей заключалось в том, что ИИ может генерировать слишком большое количество ложноположительных срабатываний, т. е. помечать легитимные транзакции как подозрительные. Это могло бы усложнить вторичную классификацию, поскольку алгоритмы ИИ часто работают как чёрный ящик, затрудняя интерпретацию их решений человеком. Кроме того, избыточные ложноположительные срабатывания могли бы негативно повлиять на пользовательский опыт, увеличивая количество жалоб от честных клиентов.

Рассмотрим результаты анализа.

1. Среднее время выявления подозрительных транзакций:

– в контрольной группе (традиционный метод) среднее время выявления подозрительной транзакции составило 15,4 мин. Это время включает как автоматическую классификацию (в среднем около минуты, в основном из-за проверки по санкционным спискам), так и ручную проверку (в среднем 14,4 мин), учитывая ожидание в очереди на специалиста;

– в экспериментальной группе (ИИ-метод) среднее время выявления сократилось до 11 мин, что составляет снижение на 29,2% по сравнению с традиционным методом. Время автоматической проверки сохранилось примерно на таком же уровне, а время ручной проверки сократилось в основном благодаря сниженной общей очереди.

2. Ложноположительные срабатывания:

– в контрольной группе доля ложноположительных срабатываний (легитимные транзакции, ошибочно помеченные как подозрительные) составила 4,8%, что эквивалентно 2402 транзакциям из 50 000;

– в экспериментальной группе доля ложноположительных срабатываний уменьшилась до 3,9% (1953 транзакции). Помимо этого снижения было отмечено меньше временя обработки транзакции: благодаря автоматизированным уведом-

лениям и прозрачным логам ИИ среднее время обработки жалобы сократилось.

3. Качественный анализ: ИИ показал способность выявлять сложные паттерны, которые традиционные правила не могли обнаружить. Например, модель ИИ выявила группу транзакций, связанных через социальные графы (общие устройства и IP-адреса), что указывало на потенциальную мошенническую сеть. В традиционном методе такие транзакции не были помечены как подозрительные, так как не превышали пороговые значения по сумме.

Суммируя вышесказанное, необходимо представить модель, которая основывается на уже освещенных нами пунктах. Предотвращение цифрового мошенничества можно сравнить с предотвращением распространения вирусов. Для примера можно взять COVID-19. Для предотвращения распространения вируса используется набор методов, например: маски на лицо, принудительная и добровольная изоляция, вакцины, прием витаминов, личная гигиена и т. д. Если использовать только маску, но при этом посещать людные места, не мыть руки и иметь недостаток витаминов в организме, вирусу будет легко попасть в организм такого человека и заразить его. В случае, если человек соблюдает все рекомендации, заразить его вирусу будет крайне сложно, поскольку вирусу необходимо будет преодолеть все эти барьеры. То же самое можно сказать и про цифровой сервис. Мошенник может купить в Интернете поддельный документ хорошего качества и обмануть верификацию. Однако если цифровой сервис использует и идентификацию, и верификацию, и мониторинг поведения пользователя, а также имеет большой ряд проверок внутри каждого из этапов выше, преступнику становится крайне трудно одинаково хорошо создать подделки и преодолеть все этапы. Рассмотрим ключевые подэтапы стратегии защиты от мошенников, пытающихся легализовать доходы, полученные преступным путём (рис. 1).

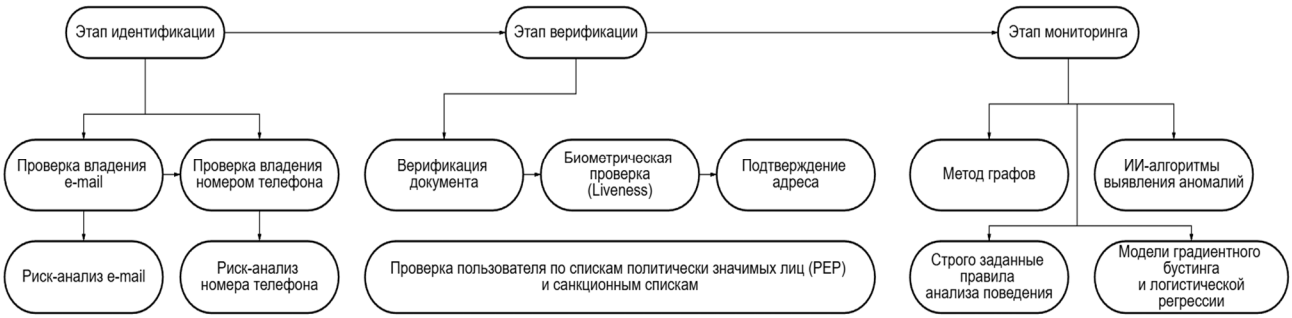

Рис. 1. Ключевые подэтапы стратегии защиты от мошенников пытающихся легализовать доходы, полученные преступным путём

Стоит отметить, что значительная часть существующих научных исследований по данной тематике подчеркивает важность того или иного метода (верификация [21], мониторинг [22]) в контексте предотвращения мошенничества [23]. Однако исследования не демонстрируют важности связи данных методов в единую систему предотвращения мошенничества, что, безусловно, важно в современном мире при борьбе с мошенниками, использующими современные технологии и генеративный искусственный интеллект. Помимо этого, существенным ограничением текущих исследований является практически полное отсутствие деталей расследования действий, совершенных пользователем. Для того чтобы с нужно долей вероятности сказать, что пользователь действительно совершил финансовое преступление, система опять же должна собрать как можно больше

информации о данном пользователе, а также автоматически проанализировать, насколько поведение данного пользователя аномально по сравнению с другими. При этом информация должна быть удобно представлена юристу цифрового сервиса для расследования.

Помимо этого, лишь в этом году в научной литературе начали появляться статьи о необходимости использования искусственного интеллекта для борьбы с подделками [24], созданными с помощью искусственного интеллекта, хотя данные подделки атакуют цифровые сервисы уже несколько лет [25]. Очевидно, что научному сообществу для успешного приращения научного знания в области предотвращения цифрового мошенничества необходимо работать на опережение и указывать бизнесу на существующие передовые технологии. Особенную роль здесь играют технологии ИИ и машинного обучения, продемонстрировавшие в эксперименте выше увеличенную общую скорость обработки транзакций и снижение ложноположительных срабатываний.

Выводы

Проблема отмывания денег через цифровые сервисы остаётся одной из наиболее актуальных угроз в условиях роста популярности финансовых технологий и криптовалют. Преступники используют сложные схемы, такие как анонимные транзакции, криптовалюты и кросс-чейн-мосты, для сокрытия источников незаконных доходов, что создаёт значительные риски для финансовых компаний и усложняет работу правоохранительных органов. Существует критическая необходимость разработки и внедрения эффективных стратегий по предотвращению отмывания денег через цифровые платформы. Основные результаты исследования заключаются в следующем:

1. *Формализация угроз и разработка стратегии защиты*. В работе представлена универсальная стратегия борьбы с отмыванием денег, включающая этапы идентификации, верификации пользователя, мониторинга транзакций и взаимодействия всех систем проверки. Уникальной особенностью стратегии является интеграция традиционных методов (идентификация и KYC) с передовыми технологиями, такими как машинное обучение, анализ социальных графов и биометрическая аутентификация. Проведённый эксперимент подтвердил эффективность предложенного подхода: внедрение ИИ позволило сократить среднее время выявления подозрительных транзакций на 29,2% (с 15,4 до 11 мин) по сравнению с традиционными методами, основанными на строго заданных правилах и ручных проверках. Кроме того, использование ИИ снизило долю ложноположительных срабатываний с 4,8% до 3,9%, что уменьшило нагрузку на вторичную проверку и улучшило пользовательский опыт.

2. *Раскрытие нового подхода к оценке ущерба*. Предложена формула C_ML – общей стоимости мошенничества от отмывания денег, учитывающая ущерб от отмывания денег, включая административные затраты, репутационные риски и штрафы. Данный подход позволяет компаниям не только оценивать текущие потери, но и моделировать потенциальные риски при недостаточном уровне защиты.

3. *Подтверждение гипотезы и новизна результатов*. Эксперимент подтвердил основную гипотезу исследования: внедрение ИИ в интегрированную стратегию защиты сокращает среднее время выявления подозрительных транзакций на цифровых платформах, при этом сохраняя высокую точность классификации. Более того, ИИ продемонстрировал способность выявлять сложные мошеннические паттерны, такие как сети связанных аккаунтов через социальные графы, что недоступно традиционным методам. Однако применение таких решений ограничено платформами с доступом к большим объёмам данных и значительными ресурсами для их обработки.

Для малых и средних цифровых сервисов внедрение предложенной стратегии требует упрощения архитектуры и оптимизации затрат, что может стать направлением дальнейших исследований.

4. *Практические рекомендации*. Результаты исследования предоставляют конкретный план действий для цифровых сервисов:

1) внедрение этапов идентификации и верификации с использованием современных технологий, включая проверку на дипфейки, Liveness Check и поведенческую биометрию;

2) использование кластеризации данных и построение социальных графов для выявления взаимосвязанных аккаунтов;

3) реализация системы мониторинга транзакций с использованием ИИ-алгоритмов и механизмов обратной связи между верификацией и мониторингом.

Также важно отметить, что технология поведенческой биометрии находится в процессе зарождения в должном виде, а значит, ее эффективность на данный момент может быть снижена. Однако в будущем, безусловно, эта технология продолжит свое развитие и, скорее всего, выйдет на передний план при борьбе с мошенничеством. Данная технология и ее влияние будут крайне интересны для анализа в будущем, а также для написания научных статей по данной тематике. При этом, если поведенческая биометрия – это реальность ближайшего будущего, то генеративный искусственный интеллект – это реальность настоящего. Ближайшие научные изыскания автора в контексте предотвращения мошенничества будут направлены именно на изучение генеративного искусственного интеллекта как защитника цифровых платформ, а также как средство, которое может быть использовано мошенниками для атаки этих самых платформ.

Необходимо подчеркнуть, что успех стратегии борьбы с отмыванием денег зависит от активного взаимодействия всех участников цифровой экосистемы, включая государственные органы, частные компании и международные организации. Совместная разработка стандартов, обмен информацией о подозрительных транзакциях и создание единых глобальных платформ для мониторинга могут стать важным шагом на пути к более безопасной цифровой среде. Важно также учитывать социально-экономические аспекты: повышение финансовой грамотности среди пользователей цифровых сервисов может стать дополнительным барьером для мошенников. Неразрешёнными остаются вопросы, связанные с адаптацией предложенной стратегии для малых цифровых сервисов, где ограничены ресурсы для внедрения ИИ и анализа больших данных, а также корректным анализом ложноотрицательных срабатываний. Также требуется дальнейшее изучение противодействия технологиям генеративного ИИ, используемым мошенниками.

Список литературы

1. Вендор, предоставляющий услуги по мониторингу крипто транзакций, ежегодный репорт // ChainAnalysis. URL: https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf (дата обращения: 04.07.2025).

2. Rathore M. M., Chaurasia S., Shukla D. Mixers detection in bitcoin network: A step towards detecting money laundering in crypto-currencies // 2022 IEEE International Conference on Big Data (Big Data). Osaka, Jaban: IEEE, 2022. P. 5775–5782. https://doi.org/ 10.1109/bigdata55660.2022.10020982

3. Hilal W., Gadsden S.A., Yawney J. Financial fraud: A review of anomaly detection techniques and recent advances // Expert Systems with Applications. 2022. Vol. 193. P. 118. https://doi.org/ 10.1016/j.eswa.2021.116429

4. Afjal M., Salamzadeh A., Dana L.-P. Financial fraud and credit risk: Illicit practices and their impact on banking stability // Journal of Risk and Financial Management. 2023. Vol. 16, N 9. P. 386. https://doi.org/ 10.3390/jrfm16090386

5. Crawford J., Guan Y. Knowing your bitcoin customer: Money laundering in the Bitcoin economy // 2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE). New York, USA: IEEE, 2020. P. 38–45. https://doi.org/ 10.1109/sadfe51007.2020.00013

6. Boreiko D. Initial coin offerings pitfalls: Scams, flops, and security breaches // Understanding Initial Coin Offerings: A New Era of Decentralized Finance (Understanding series). Cheltenham, United Kingdom: Edward Elgar Publishing, 2024. P. 176–200. https://doi.org/10.4337/9781803921587.00014

7. Hornuf L., Kück T., Schwienbacher A. Initial coin offerings, information disclosure, and fraud // Small Business Economics. 2021. Vol. 58, N 4. P. 1741–1759. https://doi.org/10.1007/s11187-021-00471-y

8. Roles of auditor in combating money laundering: A concept paper / Y. H. Yusoff [et al.] // International Journal of Academic Research in Business and Social Sciences. 2023. Vol. 13, N 4. P. 78–87. https://doi.org/10.6007/ijarbss/v13-i4/16593

9. Artificial Intelligence for anti-money laundering: A review and extension / J. Han [et al.] // Digital Finance. 2020. Vol. 2, N 3–4. P. 211–239. https://doi.org/10.1007/s42521-020-00023-1

10. Сидоров А. Л. Основные этапы верификации личности пользователя при регистрации в цифровых платформах // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей Международной научно-технической и научно-методической конференции. СПб.: Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч–Бруевича, 2023. Т. 4. С. 128–132.

11. Bello O., Olufemi K. Artificial Intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities // Computer Science & IT Research Journal. 2024. Vol. 5, N 6. P. 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

12. Skinner C. P. Coins, cross-border payments, and anti-money laundering law // Harvard Journal on Legislation. 2023. Vol. 60. P. 285.

13. Gupta A., Dwivedi D. N., Shah J. Overview of money laundering // Artificial Intelligence Applications in Banking and Financial Services. Singapore: Springer, 2023. P. 1–11. https://doi.org/10.1007/978-981-99-2571-1_1

14. Levi M., Reuter P. Money laundering // Crime and Justice. 2006. Vol. 34, N 1. P. 289–375. https://doi.org/10.1086/501508

15. Gotelaere S., Paoli L. Prevention and control of financial fraud: A scoping review // European Journal on Criminal Policy and Research. 2022. Vol. 31. P. 1–21. https://doi.org/10.1007/s10610-022-09532-8

16. Cox D.W. Handbook of anti-money laundering. Chichester, West Sussex: Wiley, 2014. 754 p.

17. Wronka C. Cyber-laundering: The change of money laundering in the Digital age // Journal of Money Laundering Control. 2021. Vol. 25, N 2. P. 330–344. https://doi.org/10.1108/jmlc-04-2021-0035

18. Wang H.-M., Hsieh M.-L. Cryptocurrency is new vogue: A reflection on money laundering prevention // Security Journal. 2023. Vol. 37, N 1. P. 25–46. https://doi.org/10.1057/s41284-023-00366-5

19. Dubey A., Choubey S. Blockchain and machine learning for data analytics, privacy preserving, and security in fraud detection // i-manager's Journal on Software Engineering. 2023. Vol. 18, N 1. P. 45. https://doi.org/10.26634/jse.18.1.20091

20. Lim J. W. A facilitative model for cryptocurrency regulation in Singapore // Handbook of Digital Currency. Academic Press, 2024. P. 341–361. https://doi.org/10.1016/b978-0-323-98973-2.00023-x

21. Aprilia G. F. Exploring detection and prevention of money laundering with information technology // Journal of Money Laundering Control. 2024. Vol. 27, N 6. P. 995–1004.

22. Dharmavaram V.G., Mishra O. KYC fraud: A new means to conduct financial fraud – how to tackle // Cybersecurity Issues, Challenges, and Solutions in the Business World. Global Scientific Publishing, 2022. P. 81–94. https://doi.org/10.4018/978-1-6684-5827-3.ch006

23. Fraud detection in financial transactions through data science for real-time monitoring and prevention / A. Sohel, M. A. Alam, M. Waliullah, A. Siddiki, M. M. Uddin // Academic Journal on Innovation, Engineering & Emerging Technology. 2024. Vol. 1, N 1. P. 91–107.

24. Javaid H. A. How artificial intelligence is revolutionizing fraud detection in financial services // Innovative Engineering Sciences Journal. 2024. Vol. 4, N 1. P. 4.

25. Shoetan P., Familoni B. Transforming fintech fraud detection with advanced artificial intelligence algorithms // Finance & Accounting Research Journal. 2024. Vol. 6, N 4. P. 602–625. https://doi.org/10.51594/farj.v6i4.1036

References

1. Vendor Providing Crypto Transaction Monitoring Services, Annual Report. ChainAnalysis. (In Russ.) Available at: https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf (accessed 04.07.2025).

2. Rathore M.M., Chaurasia S., Shukla D. Mixers detection in bitcoin network: A step towards detecting money laundering in crypto-currencies. In: *2022 IEEE International Conference on Big Data* (*Big Data*). Osaka, Jaban: IEEE; 2022. P. 5775-5782. https://doi.org/10.1109/bigdata55660.2022.10020982

3. Hilal W., Gadsden S.A., Yawney J. Financial fraud: A review of anomaly detection techniques and recent advances *Expert Systems with Applications*. 2022;193:118. https://doi.org/10.1016/j.eswa.2021.116429

4. Afjal M., Salamzadeh A., Dana L.-P. Financial fraud and credit risk: Illicit practices and their impact on banking stability. *Journal of Risk and Financial Management*. 2023;16(9):386. https://doi.org/10.3390/jrfm16090386

5. Crawford J., Guan Y. Knowing your bitcoin customer: Money laundering in the Bitcoin economy. In: *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering* (*SADFE*). New York, USA: IEEE; 2020. P. 38-45. https://doi.org/ 10.1109/sadfe51007.2020.00013

6. Boreiko D. Initial coin offerings pitfalls: Scams, flops, and security breaches. In: Understanding Initial Coin Offerings: A New Era of Decentralized Finance (Understanding series). Cheltenham, United Kingdom: Edward Elgar Publishing. 2024. P. 176-200. https://doi.org/10.4337/9781803921587.00014

7. Hornuf L., Kück T., Schwienbacher A. Initial coin offerings, information disclosure, and fraud. *Small Business Economics*. 2021;58(4):1741-1759. https://doi.org/10.1007/s11187-021-00471-y

8. Yusoff Y.H., et al. Roles of auditor in combating money laundering: A concept paper. *International Journal of Academic Research in Business and Social Sciences*. 2023;13(4):78-87. https://doi.org/10.6007/ijarbss/v13-i4/16593

9. Han J., et al. Artificial Intelligence for anti-money laundering: A review and extension. *Digital Finance*. 2020;2(3-4):211-239. https://doi.org/10.1007/s42521-020-00023-1

10. Sidorov A.L. The main stages of user identity verification during registration in digital platforms. In: *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii: sbornik gauchnykh statei Mezhdunarodnoi nauchno-tekhnicheskoi i nauchno-metodicheskoi konferentsii = Actual problems of infotelec communications in science and education: Collection of scientific articles of the International scientific, technical and scientific-methodical conference*. Vol. 4. St. Petersburg: Sankt-Peterburgskii gosudarstvennyi universitet telekommunikatsii imeni professora M.A. Bonch–Bruevicha; 2023. P. 128-132. (In Russ.)

11. Bello O., Olufemi K. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*. 2024;5(6):1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

12. Skinner C.P. Coins, cross-border payments, and anti-money laundering law. *Harvard Journal on Legislation*. 2023;60:285.

13. Gupta A., Dwivedi D.N., Shah J. Overview of money laundering. In: Artificial Intelligence Applications in Banking and Financial Services. Singapore: Springer; 2023. P. 1-11. https://doi.org/10.1007/978-981-99-2571-1_1

14. Levi M., Reuter P. Money laundering. *Crime and Justice*. 2006;34(1):289-375. https://doi.org/10.1086/501508

15. Gotelaere S., Paoli L. Prevention and control of financial fraud: A scoping review. *European Journal on Criminal Policy and Research*. 2022;31:1-21. https://doi.org/10.1007/s10610-022-09532-8

16. Cox D.W. Handbook of anti-money laundering. Chichester, West Sussex: Wiley; 2014. 754 p.

17. Wronka C. Cyber-laundering: The change of money laundering in the Digital age. *Journal of Money Laundering Control*. 2021;25(2):330-344. https://doi.org/10.1108/jmlc-04-2021-0035

18. Wang H.-M., Hsieh M.-L. Cryptocurrency is new vogue: A reflection on money laundering prevention. *Security Journal*. 2023;37(1):25-46. https://doi.org/10.1057/s41284-023-00366-5

19. Dubey A., Choubey S. Blockchain and machine learning for data analytics, privacy preserving, and security in fraud detection. *i-manager's Journal on Software Engineering*. 2023;18(1):45. https://doi.org/10.26634/jse.18.1.20091

20. Lim J.W. A facilitative model for cryptocurrency regulation in Singapore. In: Handbook of Digital Currency. Academic Press; 2024. P. 341-361. https://doi.org/10.1016/b978-0-323-98973-2.00023-x

21. Aprilia G. F. Exploring detection and prevention of money laundering with information technology. *Journal of Money Laundering Control*. 2024;27(6):995-1004.

22. Dharmavaram V.G., Mishra O. KYC Fraud: A New Means to Conduct Financial Fraud – How to Tackle. In: Cybersecurity Issues, Challenges, and Solutions in the Business World. Global Scientific Publishing; 2022. P. 81-94. https://doi.org/10.4018/978-1-6684-5827-3.ch006

23. Sohel A., Alam M.A., Waliullah M., Siddiki A., Uddin M.M. Fraud detection in financial transactions through data science for real-time monitoring and prevention. *Academic Journal on Innovation, Engineering & Emerging Technology*. 2024;1(1):91-107.

24. Javaid H.A. How Artificial Intelligence is Revolutionizing Fraud Detection in Financial Services. *Innovative Engineering Sciences Journal*. 2024;4(1):4.

25. Shoetan P., Familoni B. Transforming Fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal*. 2024;6(4):602-625. https://doi.org/10.51594/farj.v6i4.1036

Информация об авторе / Information about the Author

Сидоров Арсений Леонидович, аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), г. Санкт-Петербург, Российская Федерация, e-mail: arseniiy.sidorov@gmail.com, ORCID: 0009-0003-3929-9126

Arseniy L. Sidorov, Postgraduate, Saint Petersburg Electrotechnical University "LETI", Saint Petersburg, Russian Federation, e-mail: arseniiy.sidorov@gmail.com ORCID: 0009-0003-3929-9126