МАТЕМАТИЧЕСКИЕ, СТАТИСТИЧЕСКИЕ И ИНСТРУМЕНТАЛЬНЫЕ МЕТОДЫ ЭКОНОМИКИ/MATHEMATICAL, STATISTICAL AND INSTRUMENTAL METHODS OF ECONOMICS

DOI: https://doi.org/10.60797/IRJ.2025.161.90

ОСНОВНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ, ИСПОЛЬЗУЕМЫЕ В ЦИФРОВЫХ СЕРВИСАХ ПОСЛЕ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Научная статья

Винюков А.А.[1, *], Сидоров А.Л.[2], Покровская Н.Н.[3], Кубасов С.Н.[4]
[1] ORCID : 0009-0000-7310-8440;
[2] ORCID : 0009-0003-3929-9126;
[3] ORCID : 0000-0002-0795-8102;
[4] ORCID : 0009-0006-3556-3702;
[1, 2, 3] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, Российская Федерация
[4] Московская международная академия, Москва, Российская Федерация

* Корреспондирующий автор (andrey.vinyukov.99[at]mail.ru)

Аннотация

Вместе с взрывным ростом популярности различных цифровых сервисов стремительно увеличивается количество цифрового мошенничества. Мошенники обманывают не только доверчивых пользователей, но и сами цифровые сервисы, получая несанкционированный доступ к аккаунтам, «отмывая» нелегальные денежные средства, совершая кражу персональных данных или финансовых ресурсов. Эти действия приводят к финансовым потерям и, что более важно, к репутационным рискам для компаний. С появлением систем верификации удалось предотвратить часть мошеннических действий, ограничив доступ злоумышленников к цифровым сервисам. Однако в настоящее время мошенники разработали новые методы обхода таких систем, продолжая совершать преступления. Особенно важным является тот факт, что с развитием технологий появляются более сложные схемы мошенничества, что требует от компаний постоянной адаптации своих защитных механизмов.

В данной статье мы кратко рассмотрим, почему верификация не может считаться панацеей в борьбе с мошенничеством по состоянию на 2024 год. Основное внимание уделяется анализу наиболее распространённых мошеннических схем, которые злоумышленники применяют после успешного обхода верификационных систем, а также ключевым методам их выявления и противодействия. На первый план выходят технологии анализа поведения пользователя, а также мониторинга его цифровых атрибутов, например IP-адреса, e-mail и так далее. Это исследование особенно актуально, поскольку объем цифрового мошенничества ежегодно увеличивается, превышая в стоимостном выражении уже 10 млрд долларов США только на рынке США, а предложенные технологии и подходы могут значительно усилить успешность борьбы с мошенниками.

Ключевые слова: цифровое мошенничество, верификация, цифровой сервис, анализ пользовательского поведения, аутентификация.

PREDOMINANT FRAUD SCHEMES IN DIGITAL SERVICES POST-USER VERIFICATION

Research article

Vinyukov A.A.[1, *], Sidorov A.L.[2], Pokrovskaya N.N.[3], Kubasov S.N.[4]
[1] ORCID : 0009-0000-7310-8440;
[2] ORCID : 0009-0003-3929-9126;
[3] ORCID : 0000-0002-0795-8102;
[4] ORCID : 0009-0006-3556-3702;
[1, 2, 3] Saint Petersburg State Electrotechnical University "LETI" V.I. Ulyanov (Lenin), Saint-Petersburg, Russian Federation
[4] Moscow international academy, Moscow, Russian Federation

* Corresponding author (andrey.vinyukov.99[at]mail.ru)

Abstract

The explosive growth in popularity of various digital services has been accompanied by a rapid increase in digital fraud. Fraudsters deceive not only trusting users but also the digital services themselves, gaining unauthorized access to accounts, "laundering" illegal funds, and stealing personal data or financial resources. These actions lead to financial losses and, more importantly, to reputational risks for companies. The introduction of verification systems has helped prevent a portion of fraudulent activity by restricting attackers' access to digital services. However, fraudsters have now developed new methods to bypass such systems and continue to commit crimes. A particularly important fact is that as technology evolves, more sophisticated fraud schemes are emerging, requiring companies to constantly adapt their defense mechanisms.

This article briefly examines why verification can no longer be considered a panacea in the fight against fraud as of 2024. The focus is on analyzing the most common fraudulent schemes that malicious actors employ after successfully bypassing verification systems, as well as the key methods for their detection and prevention. Technologies for analyzing user behavior and monitoring their digital attributes, such as IP addresses, email, etc., are coming to the fore. This research is particularly relevant as the volume of digital fraud increases annually, exceeding a value of over $10 billion in the US market alone. The proposed technologies and approaches can significantly enhance the success rate in combating fraudsters.

Keywords: digital fraud, verification, digital service, user behavior analysis, authentication.

Введение

В современном цифровом мире, где технологии становятся неотъемлемой частью повседневной жизни, мошенничество в цифровых сервисах принимает всё более сложные и изощрённые формы. Взломы аккаунтов, фишинг, мошенничество с использованием украденных персональных данных и другие виды киберпреступлений представляют серьёзную угрозу как безопасности и конфиденциальности пользователей, так и финансовой стабильности частных лиц и организаций. Согласно данным Федеральной торговой комиссии США (FTC), в 2023 году мошеннические действия нанесли цифровым платформам ущерб на сумму $10 млрд [1]. Эта сумма продолжает расти с каждым годом. Проблема носит глобальный характер и требует комплексного подхода для её решения. Стремительное развитие технологий принесло не только удобство, но и новые вызовы: цифровое мошенничество становится всё более изощрённым и опасным. Актуальность данной проблемы с каждым годом возрастает.

Развитие технологий приводит к тому, что мошенники постоянно разрабатывают новые способы обхода защитных механизмов и проникновения в цифровые системы. Основная сложность борьбы с мошенничеством заключается в его динамике. Если вчера наиболее популярной схемой был фишинг, то сегодня на первый план выходят сложные комбинированные атаки, объединяющие элементы социальной инженерии, технические уязвимости и подделку данных. В связи с этим, как замечает А.П. Дурандина [2, С. 20-21] и B. Mohanty et al. [3, С. 11-14], понимание природы и классификации мошеннических схем в цифровых сервисах, а также разработка методов их предотвращения становится насущной необходимостью для обеспечения безопасности в онлайн-среде.

В данной статье рассматриваются основные виды мошеннических схем, используемых в цифровых сервисах, анализируются их природа и механизмы действия, а также предлагаются эффективные методы предотвращения, которые могут помочь пользователям и компаниям минимизировать риски и повысить уровень цифровой безопасности.

Важно отметить, что в статье будут рассмотрены мошеннические действия, совершаемые со стороны клиентов (пользователей) цифровых сервисов или внешних злоумышленников, и не затрагиваются случаи мошенничества со стороны сотрудников компаний.

Наиболее уязвимыми к цифровому мошенничеству являются сервисы, которые предполагают ввод и вывод денежных средств, например крипто биржи, крипто обменники, трейдинговые платформы, онлайн инвестиции, платежные сервисы, банки и необанки, а также другие финансовые институты. Такие сервисы как онлайн агрегаторы такси и е-коммерс платформы, менее уязвимы для атаки со стороны пользователя — клиента, поскольку у клиента нет механизма вывода денежных средств, но более уязвимы со стороны поставщика услуг — в данном случае водителя такси или продавца на маркетплейсе

Методы и принципы исследования

Во время расцвета цифровых сервисов в середине 2010-х годов практически сразу возникла необходимость защищать платформы от мошенников и предотвращать их регистрацию. В то же время, как отмечается в работе D. Malhotra et al. [4, С. 1987-1995] появились первые вендоры, предоставляющие услуги онлайн-верификации. Верификация — это процесс проверки подлинности и подтверждения личности пользователя в цифровой среде. Этот механизм, как считает P.C. Mondal et al. [5, С. 537-538] необходим для обеспечения безопасности и доверия в различных цифровых сервисах, включая онлайн-платформы, приложения и интернет-сервисы.

Основная цель верификации — удостовериться, что лицо или устройство, заявляющее о своей идентичности, действительно является тем, за кого себя выдает. Для этого, как правило, у пользователя запрашивается фотография удостоверяющего документа и селфи для сравнения изображения на документе с лицом пользователя. Система также должна проверить, что документ не является поддельным, просроченным, а также не принадлежит другому человеку, как указывает N. Kapsoulis et al. [6, С. 41].

На ранних этапах развития онлайн-верификации эти решения были недостаточно эффективными: систему можно было обмануть с помощью простейших графических редакторов, отмечает S. Baechler [7, С. 380-385]. Со временем продукты совершенствовались, и обход верификации стал всё более сложным для злоумышленников. В какой-то момент системы верификации стали крайне необходимыми для многих цифровых сервисов, включая каршеринги, финтех-компании и криптообменники, став неотъемлемой частью обеспечения безопасности и эффективной работы платформ. Они способствуют созданию доверительной среды для пользователей и предотвращению потенциальных угроз, подчеркивают A. Gomaa et al. [8, С.13].

Эффективность системы верификации может быть представлена в следующем виде:

$$E = S/P * 100, \quad (1)$$

где E — эффективность верификации,

S — количество успешно идентифицированных мошенников,

P — общее количество проверенных пользователей.

Это поможет понять, насколько эффективно система верификации справляется с задачей предотвращения мошенничества. Также авторами F. Poskriakov et al. [9, С. 120-130] большое внимание уделяется метрикам FAR, FRR. FAR (False Acceptance Rate), является метрикой, показывающей насколько много честных пользователей, которые не являются мошенниками, были помечены системой как мошенники. Иными словами, это метрика ложноположительного срабатывания. FRR (False Rejection Rate) — обратная метрика, ложноотрицательное срабатывание, пользователь является мошенником, но верификационная система пометила его как честного пользователя и пропустила дальше. Для эффективной верификации, FAR и FRR должны быть минимизированы, то есть точность самой верификации максимизирована. При этом стоит отметить, что данные метрики крайне сложно

объективно измерить, потому что крайне сложно выявить ложно положительные и ложно отрицательные срабатывания, а значит, значительная часть таких срабатываний может остаться не учтенной.

Тем не менее с развитием новых методов мошенничества эффективность верификации падает, а сама верификация пользователей более не является универсальным решением, поскольку её внедрение и поддержка требуют затрат, а также создают барьеры при регистрации для честных пользователей Пользователи, как правило, стремятся получить доступ к сервису как можно быстрее и часто неохотно предоставляют свои удостоверяющие документы. Учитывая контекст современного цифрового сервиса, особенно говоря о молодой аудитории, временной промежуток удержания внимания снижается, а значит, чем сложнее и длиннее процесс верификации, тем больше шанс, что пользователь просто закроет приложение или сервис и пойдет заниматься другим делом. Таким образом, усложняя процесс для мошенников, цифровые сервисы одновременно затрудняют его и для добросовестных пользователей, которые могут отказаться от завершения процесса регистрации из-за сложностей верификации. В результате возникает проблема баланса между конверсией в платящих пользователей и тщательностью проверки, сформулированная А.Л. Сидоровым [10, С. 282-287]. Для простоты понимания, данная проблема может быть представлена в виде следующей формулы:

$$\pi = X(1 - d) * LTV - q - p, \quad (2)$$

где π — общая выгода компании от организации процедур проверки в процессе адаптации,

X — равно количеству пользователей, начавших процедуру проверки,

d — средний процент пользователей, которые не завершили процесс регистрации, вследствие чего отказались от услуги,

LTV — средняя ценность, которую клиент принесет компании за время взаимодействия,

q — общие потери из-за мошеннических атак на платформу,

p — общая стоимость проведения процесса проверки.

Как упоминалось выше, δ и σ обычно обратно пропорциональны. Другими словами, чем выше средний процент пользователей, не завершивших регистрацию (если процесс регистрации сложный и требовательный), тем ниже общая сумма потерь от мошеннических атак. При этом σ также во многом зависит от типа бизнес-модели и общей уязвимости цифровой платформы. Согласно А.Л. Сидорову [11, С. 128-132], чем сложнее проверка, тем меньше мошенников, но также снижается количество честных пользователей.

Кроме того, согласно последним отчетам компаний Veriff [12] и Sumsub [13], специализирующихся на верификации, использование этого метода в изоляции от других инструментов борьбы с мошенничеством на сегодняшний день оказывается недостаточно эффективным по двум основным причинам.

Во-первых, как отмечено компаниями, указанными выше, а также исследователем M. Westerlund [14, С. 39-44] мошенники быстро осваивают новые технологии и активно применяют генеративный искусственный интеллект для создания цифровых личностей и дипфейков. Не каждая современная верификационная система способна распознать и предотвратить такой сложный вид мошенничества. Более того, создать дипфейк сейчас не составляет труда. С развитием цифровых сервисов искусственного интеллекта создать любой дипфейк можно за пару кликов мыши. Это значит, как утверждают S. Parate et al. [15, С. 128-137], что больше не нужно иметь специальных навыков или устройств для создания подделок. Теперь высококачественную подделку может создать любой человек, даже тот, который никогда до этого не был мошенником.

Во-вторых, мошенники часто используют так называемых «мулов» для проведения незаконных операций, согласно данным M.I. Abdul Rani et al. [16, С. 347-352]. За небольшую плату злоумышленник просит реального человека с настоящими документами пройти верификацию. После этого мошенник получает доступ к верифицированному аккаунту и совершает противозаконные действия. Верификационная система не может предотвратить данный вид мошенничества, поскольку «видит» только честного пользователя с подлинными документами, проходящего процесс верификации, как указывает Esoimeme [17, С. 205].

Таким образом, становится очевидно, что на текущий момент этап верификации сам по себе не способен полностью предотвратить мошенничество. Далее мы рассмотрим основные мошеннические схемы, применяемые злоумышленниками после успешного прохождения этапа верификации.

Основные результаты

Следует отметить, что, несмотря на широкое распространение мошенничества и значительные убытки цифровых сервисов от действий злоумышленников, принципиально новые мошеннические схемы появляются достаточно редко. Скорее, мошенники находят новые способы использования существующих лазеек и адаптируют уже известные схемы мошенничества, согласно словам M. Junger et al. [18, С. 13].

Таким образом, классификация наиболее популярных схем, применяемых в цифровых сервисах, сохраняет свою актуальность и будет востребована в ближайшие несколько лет. Существует пять основных видов цифрового мошенничества, которые применяются преступниками именно после того, как они успешно прошли верификацию в сервисе.

Взлом аккаунта. Цифровые сервисы, такие как онлайн-казино, криптоплатформы и онлайн-банки, являются одними из наиболее привлекательных целей для злоумышленников. Получив доступ к паролям или персональным данным, мошенники взламывают аккаунты пользователей и переводят деньги на счета, аффилированные с ними, о чем пишут и P. Doerfler et al. [19, С. 375-376] и G. Milka [20].

Механизмы взлома включают:

– Фишинг. Злоумышленники отправляют пользователям письма, маскируясь под официальные организации, и пытаются выманить данные для входа.

– Атаки грубой силы (Brute force). Перебор паролей до успешного подбора.

– Использование украденных баз данных. Мошенники используют ранее украденные данные для доступа к аккаунтам на разных платформах.

Пример: в 2022 году утечка базы данных одного из крупных стриминговых сервисов позволила мошенникам получить доступ к персональным данным более чем 240 миллионов пользователей [21].

Мультиаккаунтинг. Этот метод мошенничества часто служит катализатором для других схем. Пользователи создают множество аккаунтов, которые затем используются для реализации различных мошеннических операций, таких как отмывание денег или злоупотребление промоакциями. Хотя верификация может частично предотвратить этот вид мошенничества, она не является полностью эффективной, отмечают авторы T. Mauritsius et al. [22, С. 1-6]. Данный аспект будет рассмотрен подробнее далее.

Промоабьюз. Многие цифровые платформы предлагают бонусы при регистрации новых пользователей. Эти бонусы предоставляются единовременно и только новым клиентам, часто на весьма выгодных условиях. Например, платформы для ставок предлагают бонусы к депозитам, сервисы доставки еды — скидки на первый заказ, а маркетплейсы — купоны на скидку. Мошенники создают новые аккаунты для получения этих бонусов, что приводит к нецелевому расходованию маркетингового бюджета, предназначенного для привлечения новых пользователей. О данной мошеннической схеме рассказывают исследователи R. Desrousseaux et al. [23, С. 556-563], а также S.N. Aprisadianti, L. Dwiyanti [24, С. 208].

Отмывание денежных средств. Этот вид мошенничества широко распространён на платформах, которые позволяют ввод и вывод денежных средств, таких как онлайн-казино, криптообменники и инвестиционные платформы. Суть схемы, согласно исследователям M. Levi, P. Reuter [25. С. 350-360] и Z. Chen et al. [26, С. 255-278], заключается в том, что мошенник вводит на платформу деньги, полученные нелегальным путём, а затем выводит их уже «отмытыми», после чего использует их по своему усмотрению.

Чарджбэки и платёжное мошенничество. Чарджбэк (chargeback) — это процедура оспаривания платежа по банковской карте. Мошенники совершают покупку, получают товар или услугу, а затем инициируют процедуру чарджбэка, чтобы вернуть свои деньги. Чарджбэки также могут инициироваться честными пользователями, если их аккаунты были взломаны и деньги украдены. В таком случае цифровому сервису приходится возмещать как выведенные средства, так и расходы на процедуру чарджбэка, как описывают этот процесс Y. Guo et al. [27, С. 359-383].

Каждая из этих категорий мошенничества широко распространена, и часто злоумышленники комбинируют различные схемы. Некоторые из описанных схем могут непосредственно способствовать реализации других, более сложных видов мошенничества, что делает их взаимодействие особенно важным для понимания, указывают M. Ahmed et al. [28, С. 649]. Если цифровой сервис недостаточно защищён и упускает из виду одну из схем, это может привести к ещё большим убыткам для компании. Теперь кратко рассмотрим к чему могут привести данные схемы. Стоимость мошенничества на примере финансового сервиса может быть представлена следующим образом, основываясь на опыте указанном в работах M. Levi [29, С.461-474], R. Anderson et al. [30, С. 1-25], C. Cross [31, С. 120-131].

$$Ctotal = (Cm * FM * T) + CpRc + (Sf * Risk) + (Cm * Tr), \quad (3)$$

где:

Средняя стоимость мошенничества на одну транзакцию (Cm): Стоимость одной мошеннической транзакции, которая может включать потерянные средства и другие расходы, например, стоимость ресурсов для восстановления данных.

Частота мошенничества (Fm): Вероятность того, что каждая транзакция или пользователь может быть вовлечён в мошенничество. Это может быть определено как доля мошеннических транзакций от общего числа транзакций.

Общее число транзакций (T): Общее количество транзакций или действий, которые могут быть потенциально затронуты мошенничеством за определённый период времени.

Стоимость предотвращения (Cp): Это расходы на предотвращение мошенничества, включая программное обеспечение, затраты на аналитику и команду по безопасности.

Репутационные издержки (Rc): Потенциальные потери доходов из-за утраты доверия пользователей к платформе, которые можно оценить в проценте от общего дохода компании.

Время восстановления после инцидента (Tr): Затраты на время, необходимое для восстановления работы системы и урегулирования последствий после инцидента.

Штрафы и санкции (Sf): В случае законодательных последствий за утечку данных или ненадлежащее управление данными клиентов.

Пояснение:

Cm*Fm*T— прямые потери от мошеннических транзакций.

Sf*Risk of the fine— возможные юридические расходы.

Cm*Tr— дополнительные расходы, связанные с восстановлением после инцидента.

Эта модель помогает учесть все основные аспекты, влияющие на стоимость мошенничества в цифровом сервисе. В следующих разделах будут рассмотрены ключевые современные методы выявления указанных выше мошеннических схем.

Следует отметить, что борьба с мошенничеством в цифровых сервисах включает два основных этапа. Во-первых, мошенничество необходимо выявить. Во-вторых, на выявленные мошеннические действия необходимо соответствующим образом отреагировать. Вначале рассмотрим методы выявления мошеннических схем.

Таблица 1 - Основные способы выявления мошеннических схем в цифровых сервисах

DOI: https://doi.org/10.60797/IRJ.2025.161.90.1

Тип мошенничества	Способ выявления мошенничества
Взлом аккаунта	– Анализ девайса, IP-адреса, геолокации пользователя; – Привязка новых платежных методов; – Нетипичное пользовательское поведение; – Вывод всех денежных средств.
Мультиаккаунтинг	– Анализ email адреса (существование email адреса, время создания email адреса, зарегистрирован на платформе или нет и другие параметры); – Анализ номера телефона (существование номера телефона, время создание номера телефона, зарегистрирован на платформе или нет, является ли виртуальным и другие параметры); – Анализ девайса, IP-адреса, геолокации пользователя; – С помощью метода графов; – С помощью анализа биометрии и поиска по лицам.
Промо Абьюз	– Все способы, которые также применяются к мультиаккаунтингу; – Пользовательское поведение, характерное для данного метода.
Отмывание денежных средств	– Мониторинг транзакций, отслеживание больших транзакций и повторяющихся транзакций; – Верификация пользователя; – Проверка пользователя по санкционным спискам; – С помощью метода графов.
Чарджбэки и платежное мошенничество	– Мониторинг транзакций, отслеживание нетипичных транзакций; – Нетипичное пользовательское поведение; – Привязка новых платежных методов; – Анализ девайса, IP-адреса, геолокации пользователя.

Примечание: исследование авторов

Теперь рассмотрим каждый способ выявления мошенничества более подробно.

Таблица 2 - Детальное описание каждого способа выявления цифрового мошенничества

DOI: https://doi.org/10.60797/IRJ.2025.161.90.2

Анализ устройства, IP-адреса и геолокации пользователя.	Этот метод помогает обнаружить резкие изменения указанных параметров, что может сигнализировать о том, что другой человек получил доступ к аккаунту. Он также используется для борьбы с мультиаккаунтингом — когда система замечает, что одно и то же устройство или геолокация используются для входа в несколько аккаунтов. Для эффективности такой мониторинг должен работать постоянно.
Привязка новых платежных методов.	Каждый раз, когда пользователь пытается вывести средства на новую карту, это может служить индикатором того, что аккаунт был скомпрометирован, и мошенники пытаются

Анализ устройства, IP-адреса и геолокации пользователя.	Этот метод помогает обнаружить резкие изменения указанных параметров, что может сигнализировать о том, что другой человек получил доступ к аккаунту. Он также используется для борьбы с мультиаккаунтингом — когда система замечает, что одно и то же устройство или геолокация используются для входа в несколько аккаунтов. Для эффективности такой мониторинг должен работать постоянно.
	вывести средства на свои счета.
Нетипичное поведение пользователя.	Этот метод основывается на анализе поведения пользователя с использованием нейронных сетей и методов машинного обучения. При значительных изменениях в поведении (что может свидетельствовать о взломе аккаунта) система должна уведомить команду по противодействию мошенничеству.
Вывод всех денежных средств.	Если с аккаунта выводятся все доступные средства, это может быть еще одним сигналом, что аккаунт попал в руки мошенников.
Анализ адреса электронной почты и номера телефона.	Эти методы схожи между собой, но не следует путать их с верификацией. Верификация заключается в проверке принадлежности данных активов пользователю через одноразовые коды. Однако мошенники могут легко создать новый почтовый ящик или виртуальный номер. Поэтому важно учитывать дополнительные параметры: как давно создан email или номер, в каких сервисах они зарегистрированы, не связаны ли они с подозрительной активностью. Недавно созданные email-адрес или номер телефона — это красный флаг, указывающий на возможный мультиаккаунтинг.
Метод графов (Fraud Networks).	Этот метод объединяет остальные способы выявления мошенничества. Пользователи связываются в графы на основе различных признаков: совпадение IP-адресов, личных данных, устройств, телефонов или биометрической информации. Если идентификаторы используются в разных аккаунтах, это может свидетельствовать о создании мошеннической сети. Этот метод помогает выявлять мультиаккаунтинг и схемы отмывания денег.
Мониторинг транзакций.	Этот метод обязателен для многих финансовых компаний в соответствии с законодательством. Он включает отслеживание всех транзакций в цифровом сервисе и особенно важен для предотвращения отмывания денег. Мониторинг помогает обнаружить попытки ввода и немедленного вывода средств с целью их легализации.

Примечание: исследование авторов

Особо стоит упомянуть верификацию пользователей. Несмотря на важность всех вышеупомянутых методов, верификация остаётся первым этапом защиты. Все методы должны работать в совокупности, обеспечивая анализ и защиту на каждом этапе взаимодействия пользователя с сервисом. Кроме того, важным элементом борьбы с мультиаккаунтингом является использование технологий поиска по лицам, фону фотографий и шаблонам документов. Мошенники часто используют одни и те же фоны и шаблоны, что можно выявить с помощью автоматических систем.

Мультиаккаунтинг выделяется среди других схем, так как в некоторых бизнес-моделях цифровых сервисов (например, в онлайн-казино) он может происходить до этапа верификации, в зависимости от страны и её лицензионных требований.

Обсуждение

Как уже было сказано, важно не только своевременно выявлять мошеннические схемы, но и делать это в реальном времени, а не постфактум. Когда мошенничество уже совершено и средства украдены, обнаружение этого факта постфактум приносит мало пользы. Поэтому крайне важно выявлять мошеннические действия в режиме реального времени, и, что не менее важно, оперативно реагировать на них.

Проще говоря, после получения уведомления о подозрительной активности у цифрового сервиса есть два варианта: либо заблокировать пользователя, либо ничего не предпринимать, позволив ему продолжать пользоваться сервисом. Однако зачастую цифровым сервисам не хватает информации для столь категоричного решения, а политика блокировки всех подозрительных пользователей может привести к потере большой доли честных пользователей из-за высокого показателя FRR, что, в свою очередь, приведет к недовольству пользователей и падению репутации сервиса. Если система указывает на подозрительную активность, в большинстве случаев целесообразно запросить у пользователя дополнительное подтверждение личности.

Простым примером является двухфакторная аутентификация (2FA). При её включении система всегда запрашивает ввод одноразового пароля, отправленного на email или телефон. 2FA можно использовать при смене пароля, способа оплаты, входе с нового устройства или IP-адреса, а также при выводе средств. Однако в некоторых ситуациях этого может быть недостаточно. Если пользователь проходил биометрическую верификацию при регистрации, можно запросить двухфакторную аутентификацию в формате Liveness-проверки. Эта проверка подтверждает, что перед экраном находится реальный человек, и сопоставляет его лицо с тем, что было использовано при верификации. Если система подтверждает совпадение, целевое действие может быть выполнено. В противном случае система должна заблокировать пользователя до выяснения обстоятельств.

Двухфакторная аутентификация и Liveness-проверка — это мощные способы реагирования на потенциальное мошенничество, позволяющие с высокой точностью определить, является ли тревога ложной или действительно имеет место мошенничество. Помимо этих методов, существуют и другие, хотя они встречаются реже. Например, в случае подозрения на отмывание денежных средств финансовые сервисы обязаны сообщать об этом финансовым регуляторам, заполняя специальные отчеты. Это позволяет регуляторам отслеживать рынок и проактивно предотвращать отмывание денег.

При смене платежного метода также часто требуется его проверка — важно убедиться, что банковская карта действительно принадлежит пользователю, а не была украдена. Кроме того, цифровые сервисы могут запрашивать персональные данные для их сверки с государственными базами данных, чтобы подтвердить личность пользователя.

Таким образом, эффективная схема противодействия цифровому мошенничеству может быть представлена в следующем виде (рис. 1):

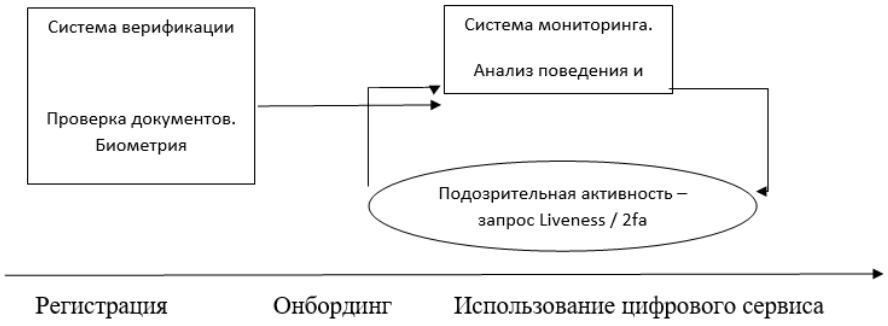

Рисунок 1 - Жизненный цикл пользователя цифрового сервиса
DOI: https://doi.org/10.60797/IRJ.2025.161.90.3

Примечание: исследование авторов

Для эффективного противодействия современным цифровым угрозам, цифровой сервис должен предпринять следующие действия:

1) Использовать эффективную систему верификации для отсечения части мошенников на ранних этапах. Под эффективной системой подразумевается та система, которая способна выявлять все современные виды кражи личности и создания фейков: использование фотошопа, использование полностью сгенерированных идентифицирующих документов, использование дипфейков, использование гиперреалистичных масок, использование распечатанных документов.

2) Внедрить мощную защиту от мошеннических схем, работающую после этапа верификации. Эта защита должна включать следующие технологии:

• Анализ устройства, IP-адреса, номера телефона, email-адреса и геолокации пользователя.
• Анализ поведения пользователя и выявление аномалий.
• Тщательный анализ и верификация платёжных методов.
• Анализ транзакций, поиск подозрительных паттернов и значительных выводов средств.
• Применение метода графов для выявления серийного мошенничества.

Помимо строго прописанной риск-логики в мониторинговой системе, на основе строго заданных правил, например, выдавать модератору предупреждение, если пользователь пытается вывести денежную сумму выше определенного порога, необходимо также использовать современные алгоритмы искусственного интеллекта для выявления аномалий в поведении пользователей. В данном случае искусственный интеллект может служить некой третьей контролирующей рукой, которая будет выявлять то, что не увидел человек и строго заданные правила мониторинга.

3) Необходимо не только выявлять подозрительную активность в режиме реального времени (а не постфактум), но и оперативно на неё реагировать, запрашивая у пользователя прохождение двухфакторной аутентификации или Liveness-теста.

Заключение

Суммируя вышесказанное, следует отметить, что на момент написания данной статьи цифровое мошенничество продолжает расти, а мошенники изобретают всё новые способы обмана бизнесов. Ключевые мошеннические схемы за последние несколько лет остаются неизменными; злоумышленники лишь адаптируют методы их реализации к современным технологиям и особенностям систем безопасности.

Наиболее распространённые схемы, с которыми сталкиваются цифровые сервисы, включают:

• Взлом аккаунтов — использование фишинга, перебора паролей (brute force) или утечек данных для получения доступа к чужим учётным записям.
• Промо-абьюз — злоупотребление акциями и бонусами (например, регистрация множества аккаунтов для получения скидок).
• Мультиаккаунтинг — создание множества учётных записей для обхода ограничений, манипуляции рейтинговых систем или получения выгоды.
• Отмывание денег — использование легальных платёжных платформ для «очистки» средств, полученных преступным путём.
• Чарджбэки и платёжное мошенничество — возврат средств по фиктивным претензиям, использование краденых карт для покупок.

Также мы рассмотрели ключевые технологии и методы защиты от данных мошеннических схем. Таким образом, борьба с цифровым мошенничеством требует комплексного подхода, объединяющего технологии, обучение пользователей и постоянное совершенствование процессов безопасности.

Ограничением данной статьи является рассмотрение лишь части пользовательского пути. Анализ сосредоточен на отрезке, начинающемся после процесса верификации пользователя. Однако защита на этапах регистрации, первоначальной авторизации и взаимодействия с данными также является критически важной. Дальнейшие исследования в области цифрового мошенничества могут быть направлены на анализ эффективности методов поведенческой аналитики, влияния на процесс новых технологий, в первую очередь искусственного интеллекта, а также на анализ поведения мошенников в течение всего цикла жизни пользователя.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.60797/IRJ.2025.161.90.4

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.60797/IRJ.2025.161.90.4

Список литературы / References

1. As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public : press releases // Federal Trade Commission. — 2024. — URL: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public (accessed: 31.07.2024).

2. Дурандина А.П. Интеграция рисков информационной безопасности в систему управления операционной надежностью организации / А.П. Дурандина // Петербургский экономический журнал. — 2023. — № 3. — С. 19–32.

3. Mohanty B. Role of Artificial Intelligence in Financial Fraud Detection / B. Mohanty, S. Mishra // Academy of Marketing Studies Journal. — 2023. — Vol. 27. — № S4.

4. Malhotra D. How blockchain can automate KYC: Systematic review / D. Malhotra, P. Saini, A.K. Singh // Wireless Personal Communications. — 2022. — Vol. 122. — № 2. — P. 1987–2021. — DOI: 10.1007/s11277-021-08977-0.

5. Mondal P.C. Know your customer (KYC) based authentication method for financial services through the internet / P.C. Mondal, R. Deb, M.N. Huda // 2016 19th International Conference on Computer and Information Technology (ICCIT). — IEEE, 2016. — P. 535–540. — DOI: 10.1109/ICCITECHN.2016.7860255.

6. Kapsoulis N. Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture / N. Kapsoulis, A. Psychas, G. Palaiokrassas [et al.] // Future Internet. — 2020. — Vol. 12. — № 2. — 41 p. — DOI: 10.3390/fi12020041.

7. Baechler S. Document fraud: Will your identity be secure in the twenty-first century? / S. Baechler // European Journal on Criminal Policy and Research. — 2020. — Vol. 26. — № 3. — P. 379–398. — DOI: 10.1007/s10610-020-09441-8.

8. Gomaa A. A new framework for an eKYC system / A. Gomaa, O. Rashed, A. Refaey [et al.] // 2022 20th International Conference on Language Engineering (ESOLEC). — IEEE, 2022. — Vol. 20. — P. 11–18. — DOI: 10.1109/ESOLEC54569.2022.10009253.

9. Poskriakov F. Cryptocurrency compliance and risks: A European KYC/AML perspective / F. Poskriakov, M. Chiriaeva, C. Cavin // Blockchain & Cryptocurrency Regulation. — 2020. — P. 130–145.

10. Сидоров А.Л. Актуальность внедрения дополнительных защитных мер для цифровых сервисов при регистрации пользователей / А.Л. Сидоров // Актуальные аспекты модернизации российской экономики : материалы IX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. — Санкт-Петербург : СПбГЭТУ «ЛЭТИ», 2022. — С. 282–287.

11. Сидоров А.Л. Основные этапы верификации личности пользователя при регистрации в цифровых платформах / А.Л. Сидоров // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : сборник научных статей XII Международной научно-технической и научно-методической конференции. — 2023. — Т. 4. — С. 128–132.

12. Identity Fraud Report 2023 // Sumsub. — 2023. — URL: https://sumsub.com/guides-reports/identity-fraud-report-2023/ (accessed: 07.08.2024).

13. Veriff Fraud Index 2024 // Veriff. — 2024. — URL: https://www.veriff.com/ebooks/veriff-fraud-index-2024 (accessed: 07.08.2024).

14. Westerlund M. The emergence of deepfake technology: A review / M. Westerlund // Technology Innovation Management Review. — 2019. — Vol. 9. — № 11. — P. 39–52. — DOI: 10.22215/timreview/1282.

15. Parate S. Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures / S. Parate, H.P. Josyula, L.T. Reddi // International Research Journal of Modernization in Engineering Technology and Science. — 2023. — Vol. 5. — № 9. — P. 128–137. — DOI: 10.56726/IRJMETS44476.

16. Abdul Rani M.I. A systematic literature review of money mule: Its roles, recruitment and awareness / M.I. Abdul Rani, S.N.F. Syed Mustapha Nazri, S. Zolkaflil // Journal of Financial Crime. — 2024. — Vol. 31. — № 2. — P. 347–361. — DOI: 10.1108/JFC-10-2022-0243.

17. Esoimeme E.E. Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules / E.E. Esoimeme // Journal of Money Laundering Control. — 2021. — Vol. 24. — № 1. — P. 201–212. — DOI: 10.1108/JMLC-05-2020-0053.

18. Junger M. Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits / M. Junger, V. Wang, M. Schlömer // Crime Science. — 2020. — Vol. 9. — № 1. — 13 p. — DOI: 10.1186/s40163-020-00119-4.

19. Doerfler P. Evaluating login challenges as a defense against account takeover / P. Doerfler, K. Thomas, M. Marincenko [et al.] // The World Wide Web Conference. — 2019. — P. 372–382. — DOI: 10.1145/3308558.3313481.

20. Milka G. Anatomy of account takeover / G. Milka // Enigma 2018. — 2018.

21. Personal data leak, music streaming service Deezer // ClaimBack. — URL: https://claimback.de/en/articles/deezer-data-leak-money-back-for-affected-deezer-users (accessed: 16.08.2024).

22. Mauritsius T. Promo abuse modeling in e-commerce using machine learning approach / T. Mauritsius, S. Alatas, F. Binsar [et al.] // 2020 8th International Conference on Orange Technology (ICOT). — IEEE, 2020. — P. 1–6. — DOI: 10.1109/ICOT51877.2020.9468744.

23. Desrousseaux R. Identify Theft Detection on e-Banking Account Opening / R. Desrousseaux, G. Bernard, J.J. Mariage // IJCCI. — 2019. — P. 556–563.

24. Aprisadianti S.N. Promotion Abuse Fraud Detection Application Development using Risk Scoring / S.N. Aprisadianti, L. Dwiyanti // 2023 IEEE International Conference on Data and Software Engineering (ICoDSE). — IEEE, 2023. — P. 208–213. — DOI: 10.1109/ICoDSE59534.2023.1029149.

25. Levi M. Money laundering / M. Levi, P. Reuter // Crime and Justice. — 2006. — Vol. 34. — № 1. — P. 289–375. — DOI: 10.1086/501508.

26. Chen Z. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review / Z. Chen, L.D. Van Khoa, E.N. Teoh [et al.] // Knowledge and Information Systems. — 2018. — Vol. 57. — P. 245–285. — DOI: 10.1007/s10115-017-1144-z.

27. Guo Y. To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce / Y. Guo, Y. Bao, B.J. Stuart [et al.] // Information Systems Journal. — 2018. — Vol. 28. — № 2. — P. 359–383. — DOI: 10.1111/isj.12144.

28. Ahmed M. A semantic rule based digital fraud detection / M. Ahmed, K. Ansar, C.B. Muckley [et al.] // PeerJ Computer Science. — 2021. — Vol. 7. — e649 p. — DOI: 10.7717/peerj-cs.649.

29. Levi M. Assessing the cost of fraud / M. Levi // The SAGE Handbook of Criminological Research Methods. — 2012. — P. 461–474.

30. Anderson R. Measuring the changing cost of cybercrime / R. Anderson, C. Barton, R. Böhme [et al.] // The 18th Annual Workshop on the Economics of Information Security (WEIS 2019). — 2019. — P. 1–25.

31. Cross C. Is online fraud just fraud? Examining the efficacy of the digital divide / C. Cross // Journal of Criminological Research, Policy and Practice. — 2019. — Vol. 5. — № 2. — P. 120–131. — DOI: 10.1108/JCRPP-01-2019-0008.

Список литературы на английском языке / References in English

1. As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public : press releases // Federal Trade Commission. — 2024. — URL: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public (accessed: 31.07.2024).

2. Durandina A.P. Integratsiya riskov informatsionnoy bezopasnosti v sistemu upravleniya operatsionnoy nadezhnostyu organizatsii [Integration of information security risks into the operational risk management system of the organization] / A.P. Durandina // Peterburgskiy ekonomicheskiy zhurnal [Petersburg Economic Journal]. — 2023. — № 3. — P. 19–32. [in Russian]

3. Mohanty B. Role of Artificial Intelligence in Financial Fraud Detection / B. Mohanty, S. Mishra // Academy of Marketing Studies Journal. — 2023. — Vol. 27. — № S4.

4. Malhotra D. How blockchain can automate KYC: Systematic review / D. Malhotra, P. Saini, A.K. Singh // Wireless Personal Communications. — 2022. — Vol. 122. — № 2. — P. 1987–2021. — DOI: 10.1007/s11277-021-08977-0.

5. Mondal P.C. Know your customer (KYC) based authentication method for financial services through the internet / P.C. Mondal, R. Deb, M.N. Huda // 2016 19th International Conference on Computer and Information Technology (ICCIT). — IEEE, 2016. — P. 535–540. — DOI: 10.1109/ICCITECHN.2016.7860255.

6. Kapsoulis N. Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture / N. Kapsoulis, A. Psychas, G. Palaiokrassas [et al.] // Future Internet. — 2020. — Vol. 12. — № 2. — 41 p. — DOI: 10.3390/fi12020041.

7. Baechler S. Document fraud: Will your identity be secure in the twenty-first century? / S. Baechler // European Journal on Criminal Policy and Research. — 2020. — Vol. 26. — № 3. — P. 379–398. — DOI: 10.1007/s10610-020-09441-8.

8. Gomaa A. A new framework for an eKYC system / A. Gomaa, O. Rashed, A. Refaey [et al.] // 2022 20th International Conference on Language Engineering (ESOLEC). — IEEE, 2022. — Vol. 20. — P. 11–18. — DOI: 10.1109/ESOLEC54569.2022.10009253.

9. Poskriakov F. Cryptocurrency compliance and risks: A European KYC/AML perspective / F. Poskriakov, M. Chiriaeva, C. Cavin // Blockchain & Cryptocurrency Regulation. — 2020. — P. 130–145.

10. Sidorov A.L. Aktualnost vnedreniya dopolnitelnykh zashchitnykh mer dlya tsifrovykh servisov pri registratsii polzovateley [The Relevance of Implementing Additional Security Measures for Digital Services during User Registration] / A.L. Sidorov // Aktualnye aspekty modernizatsii rossiyskoy ekonomiki [Relevant Aspects of Modernization of the Russian Economy] : materials from the IX All-Russian Scientific and Practical Conference for Students, Postgraduates and Young Scientists. — Saint Petersburg : SPbGETU "LETI", 2022. — P. 282–287. [in Russian]

11. Sidorov A.L. Osnovnye etapy verifikatsii lichnosti polzovatelya pri registratsii v tsifrovykh platformakh [Main Stages of User Identity Verification During the Onboarding Process in Digital Platforms] / A.L. Sidorov // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2023) [Actual problems of infotelec communications in science and education (APINO 2023)] : collection of scientific articles of the XII International Scientific, Technical and Methodological Conference. — 2023. — Vol. 4. — P. 128–132. [in Russian]

12. Identity Fraud Report 2023 // Sumsub. — 2023. — URL: https://sumsub.com/guides-reports/identity-fraud-report-2023/ (accessed: 07.08.2024).

13. Veriff Fraud Index 2024 // Veriff. — 2024. — URL: https://www.veriff.com/ebooks/veriff-fraud-index-2024 (accessed: 07.08.2024).

14. Westerlund M. The emergence of deepfake technology: A review / M. Westerlund // Technology Innovation Management Review. — 2019. — Vol. 9. — № 11. — P. 39–52. — DOI: 10.22215/timreview/1282.

15. Parate S. Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures / S. Parate, H.P. Josyula, L.T. Reddi // International Research Journal of Modernization in Engineering Technology and Science. — 2023. — Vol. 5. — № 9. — P. 128–137. — DOI: 10.56726/IRJMETS44476.

16. Abdul Rani M.I. A systematic literature review of money mule: Its roles, recruitment and awareness / M.I. Abdul Rani, S.N.F. Syed Mustapha Nazri, S. Zolkaflil // Journal of Financial Crime. — 2024. — Vol. 31. — № 2. — P. 347–361. — DOI: 10.1108/JFC-10-2022-0243.

17. Esoimeme E.E. Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules / E.E. Esoimeme // Journal of Money Laundering Control. — 2021. — Vol. 24. — № 1. — P. 201–212. — DOI: 10.1108/JMLC-05-2020-0053.

18. Junger M. Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits / M. Junger, V. Wang, M. Schlömer // Crime Science. — 2020. — Vol. 9. — № 1. — 13 p. — DOI: 10.1186/s40163-020-00119-4.

19. Doerfler P. Evaluating login challenges as a defense against account takeover / P. Doerfler, K. Thomas, M. Marincenko [et al.] // The World Wide Web Conference. — 2019. — P. 372–382. — DOI: 10.1145/3308558.3313481.

20. Milka G. Anatomy of account takeover / G. Milka // Enigma 2018. — 2018.

21. Personal data leak, music streaming service Deezer // ClaimBack. — URL: https://claimback.de/en/articles/deezer-data-leak-money-back-for-affected-deezer-users (accessed: 16.08.2024).

22. Mauritsius T. Promo abuse modeling in e-commerce using machine learning approach / T. Mauritsius, S. Alatas, F. Binsar [et al.] // 2020 8th International Conference on Orange Technology (ICOT). — IEEE, 2020. — P. 1–6. — DOI: 10.1109/ICOT51877.2020.9468744.

23. Desrousseaux R. Identify Theft Detection on e-Banking Account Opening / R. Desrousseaux, G. Bernard, J.J. Mariage // IJCCI. — 2019. — P. 556–563.

24. Aprisadianti S.N. Promotion Abuse Fraud Detection Application Development using Risk Scoring / S.N. Aprisadianti, L. Dwiyanti // 2023 IEEE International Conference on Data and Software Engineering (ICoDSE). — IEEE, 2023. — P. 208–213. — DOI: 10.1109/ICoDSE59534.2023.1029149.

25. Levi M. Money laundering / M. Levi, P. Reuter // Crime and Justice. — 2006. — Vol. 34. — № 1. — P. 289–375. — DOI: 10.1086/501508.

26. Chen Z. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review / Z. Chen, L.D. Van Khoa, E.N. Teoh [et al.] // Knowledge and Information Systems. — 2018. — Vol. 57. — P. 245–285. — DOI: 10.1007/s10115-017-1144-z.

27. Guo Y. To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce / Y. Guo, Y. Bao, B.J. Stuart [et al.] // Information Systems Journal. — 2018. — Vol. 28. — № 2. — P. 359–383. — DOI: 10.1111/isj.12144.

28. Ahmed M. A semantic rule based digital fraud detection / M. Ahmed, K. Ansar, C.B. Muckley [et al.] // PeerJ Computer Science. — 2021. — Vol. 7. — e649 p. — DOI: 10.7717/peerj-cs.649.

29. Levi M. Assessing the cost of fraud / M. Levi // The SAGE Handbook of Criminological Research Methods. — 2012. — P. 461–474.

30. Anderson R. Measuring the changing cost of cybercrime / R. Anderson, C. Barton, R. Böhme [et al.] // The 18th Annual Workshop on the Economics of Information Security (WEIS 2019). — 2019. — P. 1–25.

31. Cross C. Is online fraud just fraud? Examining the efficacy of the digital divide / C. Cross // Journal of Criminological Research, Policy and Practice. — 2019. — Vol. 5. — № 2. — P. 120–131. — DOI: 10.1108/JCRPP-01-2019-0008.