Научная статья
УДК 338.2
DOI 10.18101/2304-4446-2025-1-119-126

Важность поведенческих аномалий при выявлении цифровых мошенников на этапе верификации

© Сидоров Арсений Леонидович
аспирант
arseniiy.sidorov@gmail.com

© Винюков Андрей Анатольевич
аспирант
andrey.vinyukov.99@mail.ru

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова (Ленина)
Россия, 197376, г. Санкт-Петербург, ул. Профессора Попова, 5

Аннотация. Цифровое мошенничество становится все более сложным и изощренным, а также растет в объеме, что требует совершенствования механизмов защиты цифровых сервисов. В статье рассматривается значимость поведенческих аномалий для выявления мошенников на этапе верификации. Представлены результаты эксперимента с использованием модели градиентного бустинга (Catboost), проанализированы данные 100 000 пользователей, из которых 2 863 были идентифицированы как мошенники. Ключевыми поведенческими факторами, аномалии в которых свидетельствуют о возможном мошенничестве, являются время загрузки документа, время прохождения этапа биометрии, время заполнения анкеты, количество попыток загрузки документов и биометрии, средняя пауза между заполнением полей формы, а также время реакции на при запуске этапа биометрии. Полученные результаты показывают, что поведение мошенников часто отклоняется от среднего по этим показателям. Такие данные могут быть эффективно использованы для адаптации верификационных систем, чтобы минимизировать потери среди честных пользователей, сохраняя при этом высокий уровень защиты. Ограничения исследования связаны с анализом только этапа верификации, что подчеркивает необходимость дальнейшего изучения поведения пользователей после данного шага. Выводы акцентируют внимание на необходимости комплексного подхода к мониторингу пользовательских действий для борьбы с цифровым мошенничеством.

Ключевые слова: верификация, цифровое мошенничество, поведение пользователя, поведенческие аномалии, градиентный бустинг, биометрия.

Для цитирования
Сидоров А. Л., Винюков А. А. Важность поведенческих аномалий при выявлении цифровых мошенников на этапе верификации // Вестник Бурятского государственного университета. Экономика и менеджмент. 2025. № 1. С. 119–126.

С каждым годом цифровая среда становится более привлекательной для злоумышленников, использующих все более сложные схемы обмана [1]. В условиях растущего объема онлайн-транзакций и множества новых способов взаимодействия с клиентами, а также технологий открытых API компании сталкиваются с

необходимостью защиты не только своих ресурсов, но и данных клиентов [2]. Классические методы, такие как верификация и системы проверки транзакций, больше не всегда могут обеспечить достаточную защиту, поэтому все больше внимания уделяется анализу поведения пользователей для выявления скрытых угроз [3].

Более того, верификация и любые другие проверки пользователя, требующие от последнего активных действий, таких как загрузка документа, прохождение биометрии и так далее, неизбежно приводят к потере части честных пользователей цифровым сервисом [4]. Современный пользователь хочет получить доступ к цифровому сервису за пару кликов и, зачастую, не готов совершать дополнительные действия, которые от него требует верификационная система. В итоге часть честных пользователей просто не заканчивает верификацию и не становится активным пользователем цифрового сервиса. Как следствие, цифровой сервис недополучает прибыль [5]. Таким образом, на первый план выходит скрытый для пользователя мониторинг его действий. Это позволяет сохранить правильный баланс между тщательностью проверки для эффективного отсеивания мошенников и конверсией в платящего пользователя для честных пользователей [6; 7].

В начале необходимо кратко поговорить о верификации и ее современном виде в цифровых сервисах. Верификация — необходимый процесс для многих современных цифровых сервисов, поскольку она способствует обеспечению безопасности пользователей и защищает компании от мошеннических действий [8]. Процесс верификации может включать в себя разные уровни проверки, такие как подтверждение личности, аутентификация по биометрическим данным или многослойная авторизация через SMS-коды или электронную почту. Такие методы позволяют уменьшить риски несанкционированного доступа и повысить доверие клиентов. Для многих цифровых сервисов верификация является регуляторным требованием надзорного органа [9; 10]. В таких случаях самый популярный способ верификации включает два этапа: запрос у пользователя идентифицирующего документа и прохождение этапа биометрии, сравнение лица пользователя с фотографией в документе[1].

Как уже было сказано выше, верификация в современном виде не является совершенной. Основные недостатки: 1. Широкое распространение генеративного искусственного интеллекта приводит к демократизации мошенничества[2]. Создать поддельный документ или дипфейк сейчас — простая задача, а значит не нужно иметь специальных талантов, чтобы начать обманывать цифровые сервисы. Далеко не каждая верификационная система способна выявить подделки такого уровня. Тем более такие подделки практически невозможно выявить на глаз. Человек без помощи машины уже не способен эффективно отличать дипфейки от обычных фотографий [11].

[1] Veriff Identity Fraud Report 2025 — ежегодный отчет о цифровом мошенничестве в процессе верификации от вендора-компании Veriff. URL: https://www.veriff.com/resources/ebooks/veriff-identity-fraud-report-2025 (дата обращения: 13.11.2024). Текст: электронный.

[2] Sumsub Identity Fraud Report 2024 — ежегодный отчет о цифровом мошенничестве в процессе верификации от вендора-компании Sumsub. URL: https://sumsub.com/fraud-report-2024/ (дата обращения: 13.11.2024). Текст: электронный.

2. В эпоху постоянных утечек данных и снижения фокуса внимания у пользователя современные клиенты цифровых сервисов могут или не желать делиться фотографиями своих документов или не закончить верификацию из-за долгого и сложного процесса [12].

3. При этом, даже если документы пользователя настоящие и биометрический шаг не вызывает опасений, многие мошенники просто покупают уже верифицированные аккаунты. Верификация не способна поймать мошенничество такого рода, поскольку изолированная верификационная система не может узнать, что происходит с пользователем после начальной проверки [13; 14].

Как итог, для эффективного предотвращения мошенничества цифровому сервису помимо технологически продвинутой верификационной системы, способной выявлять все современные фейки, созданные с помощью генеративного искусственного интеллекта, необходимо иметь развитую систему мониторинга поведения пользователя после и во время верификации [15; 16]. В данной статье рассмотрим ключевые аспекты пользовательского поведения, которые могут выступать подозрительным маркером мошенничества и указывать на недобросовестного пользователя. Стоит отметить, что в данном эксперименте мы будем рассматривать поведенческие аспекты, которые были собраны только в процессе верификации. Безусловно, выявление мошенничества после этапа верификации — крайне важная практическая задача, но это станет темой для будущих исследований.

За основу эксперимента были взяты реальные анонимизированные и агрегированные данные. По условиям контракта авторы не могут раскрывать цифровой сервис, предоставивший данные. Общий объем выборки пользователей составил 100 000 человек, из которых 2 863 по результатам проверки были признаны мошенниками, остальные — честными пользователями. Все пользователи проходили единый верификационный путь, состоящий из трех основных этапов: заполнение формы с информацией о себе, прохождение верификации идентифицирующего документа и прохождение этапа биометрии.

В рамках эксперимента примем за данность, что система уже сделала выбор правильно, то есть верно определила мошенников и честных пользователей. В реальности, конечно же, существует определенный объем FAR (False Acceptance Rate) и FRR (False Rejection Rate). Это ключевые метрики в биометрических системах и других системах аутентификации, которые показывают качество работы алгоритмов распознавания и верификации. FAR (False Acceptance Rate) — Уровень ложного принятия: показатель, отражающий вероятность того, что система неверно распознает мошенника как честного пользователя. FRR (False Rejection Rate) — Уровень ложного отклонения: показатель, отражающий вероятность того, что система неправильно отклоняет честного пользователя. Оценить данные метрики крайне сложно, поскольку система крайне редко понимает, где она сделала ошибку. Однако в контексте работы определим, что данные показатели являются минимальными и не повлияют на последующие результаты.

Система верификации цифрового сервиса также зарегистрировала следующие переменные в процессе верификации:

Таблица 1

Описание переменных для эксперимента

Переменная	Описание
Doc_Time	Время, потраченное пользователем на загрузку документа
Selfie_Time	Время, потраченное пользователем на прохождение этапа биометрии
Form_time	Время, потраченное пользователем на заполнение анкеты
Doc_Tries	Количество попыток загрузки документа
Selfie_Tries	Количество попыток загрузки биометрии
Average_Pause	Средняя пауза между полями формы
Selfie_Reaction	Время реакции при запуске этапа биометрии

Ключевая цель данного исследования — понять, какие поведенческие факторы являются важными при предсказании мошенничества, из них — какие наиболее важные. Наконец, чем обусловлена эта важность с точки зрения распределения мошенников, наблюдается ли какой-либо тренд мошеннического поведения внутри каждой переменной. Для этой задачи нам прекрасно подойдут модели градиентного бустинга по следующим причинам: во-первых, градиентный бустинг обычно обеспечивает одну из самых высоких точностей среди моделей машинного обучения. Во-вторых, благодаря методам регуляризации, градиентный бустинг хорошо контролирует переобучение. Наконец, за счет использования «деревьев» решений в качестве базовых моделей градиентный бустинг может эффективно захватывать сложные нелинейные зависимости в данных.

Стоит отметить, что верификационная система может регистрировать гораздо больше признаков. В данную модель мы включим только основные признаки, а также не будем включать булевые переменные, поскольку их эффективность в моделях градиентного бустинга будет ниже, по сравнению с численными переменными, так как их можно будет «разбить» только один раз.

Среди методов градиентного бустинга нами был выбран именно Catboost по следующим причинам: Catboost способен обрабатывать пропущенные значения автоматически, что упрощает подготовку данных и делает его более устойчивым к проблемам с отсутствующими данными и к переобучению.

Как уже было сказано, для эксперимента был взят массив из 100 000 наблюдений, из которых 2 863 пользователя являются мошенниками, а остальные — честными пользователями. Важное достоинство модели Catboost также заключается в том, что модель хорошо работает с несбалансированными выборками.

Построим модель градиентного бустинга по нашим переменным:

Таблица 2

Важность переменных, модель Catboost

Переменная	Важность
Selfie_Reaction	16,34
Doc_Time	16,03
Average_Pause	15,41
Form_time	14,00
Selfie_Time	13,72
Doc_Tries	12,85
Selfie_Tries	11,63

Теперь проинтерпретируем результаты анализа. Важность в правой строке таблицы, по сути, показывает, насколько каждый признак уменьшает ошибку модели на каждой итерации построения деревьев. Чем больше уменьшение ошибки при использовании признака, тем выше его важность. В CatBoost значения важности носят относительный характер. Например, если важность одного признака в два раза выше, чем у другого, это означает, что первый признак примерно в два раза более важен для модели. Сумма всех значимостей признаков обычно равна 100%. Можно использовать это, чтобы понять, какую долю объяснимой значимости каждый признак добавляет в модель.

Следующий аспект, который необходимо обсудить, — это метод отбора переменных. Необходимо выбрать способ, согласно которому мы будем определять переменные в группу важных и в группу менее важных.

Существует несколько основных методов

1. Определение границы по доле кумулятивной важности:

Необходимо рассчитать кумулятивную важность, то есть накопленную важность признаков, и отобрать признаки, покрывающие определенный процент важности (например, 90 или 95%)

2. Отбор признаков на основе порогового значения важности:

Необходимо задать порог, ниже которого признаки считаются малозначимыми (например, 1 или 0.5%).

3. Определение границы по изменению важности:

Необходимо проанализировать распределение важности и выявить резкий спад, где важность признаков начинает резко снижаться.

4. Тестирование производительности модели с разным числом признаков:

Необходимо начать с небольшого числа признаков (например, топ-5), постепенно добавляя новые признаки, пока качество модели перестанет заметно улучшаться.

Чаще всего используется первый метод из-за его простоты и легкости объяснения. В нашем случае, вне зависимости от выбора метода, можно однозначно отметить, что все переменные, включенные в модель, крайне важны для предсказания цифрового мошенничества на этапе верификации. Все эти переменные в случае отклонения от нормы могут считаться красными флагами, на которые система должна обращать внимание. Рассмотрим подробнее каждую переменную и укажем на логический смысл взаимосвязи ее с зависимой переменной.

Переменная Selfie_Reaction отвечает за время реакции при запуске этапа биометрии. Данная переменная занимает первое место по важности в нашей модели. При детальном рассмотрении данных нами было обнаружено, что время реакции для мошенников в целом гораздо ниже, чем для честных пользователей. Это связано с тем, что мошенники уже знают, какие этапы включает в себя верификация и что от них будет требоваться, в то время как честные пользователи часто проходят данный процесс в первый раз и зачастую в более расслабленном режиме, а значит имеют более низкую скорость реакции от запуска этапа биометрии до прохождения первого задания активного Liveness теста. Также были замечены несколько мошенников, для которых время реакции было слишком долгое. Это может быть связано с тем, что они использовали автоматизированный скрипт

компьютера для прохождения верификации и система просто не могла найти человеческое лицо для прохождения селфи.

Следующая переменная — Doc_Time, отвечает за время, потраченное пользователем на загрузку документа. Данная переменная находиться на втором месте по значимости в модели. При детальном рассмотрении датасета нами была выявлена следующая закономерность. Цифровые мошенники делятся на две группы. Первая группа мошенников в среднем загружает документ сильно быстрее среднего пользователя, поскольку они уже имеют на руках какой-то заготовленный поддельный документ и ознакомлены с процессом. Вторая группа, увидев требования верификации, начинают оперативный поиск какого-то поддельного документа, отчего время до загрузки документа становиться дольше по сравнению со средним честным пользователем цифрового сервиса.

Average_Pause находится на третьем месте по значимости и показывает среднюю паузу между заполнением полей формы-опросника. Форма-опросник обычно является первым этапом верификации и может содержать различные вопросы, от имени пользователя до места жительства и номера идентифицирующего документа. Как и в случае с предыдущей переменной, четко прослеживается тренд на две группы мошенников с разным поведением, одни заполняют поля формы, быстро копируя заранее заготовленные данные, вторые тратят больше времени, чем средний честный пользователь.

Для переменных Form_Time (время, потраченное на заполнение формы) и Selfie_Time (время, потраченное на прохождение селфи шага) в целом наблюдаются схожие две группы мошенников, как уже было упомянуто выше.

Наконец, заключительные по значимости переменные Doc_Tries и Selfie_Tries показывают количество попыток загрузки документа и прохождения этапа селфи соответственно. Замечена четкая позитивная корреляция между тем, является ли пользователь мошенником и количеством попыток прохождения этапов. С первого раза у мошенников что-то может не получиться, и они пытаются еще раз обмануть систему.

Выводы.

С распространением цифровизации, а также с ростом популярности и простоты использования генеративного искусственного интеллекта цифровое мошенничество растет от года к году. Для эффективной борьбы с цифровым сервисом более недостаточно полагаться лишь на верификационную систему. Необходимо уделять внимание поведению пользователей в процессе верификации и в случае обнаружения аномалий принимать необходимые меры, вплоть до блокировки пользователя. Особое внимание необходимо уделять следующим поведенческим аспектам, поскольку они безусловно важны: Время, потраченное пользователем на загрузку документа (Doc_Time), Время, потраченное пользователем на прохождение этапа биометрии (Selfie_Time), Время, потраченное пользователем на заполнение анкеты (Form_Time), Количество попыток загрузки документа (Doc_Tries), Количество попыток загрузки биометрии (Selfie_Tries), Средняя пауза между полями формы (Average_Pause), Время реакции при запуске этапа биометрии (Selfie_Reaction). Показатели мошенников будут отличаться от честных пользователей, они будут смещены и будут во многих случаях принимать значения либо значительно меньше среднего по данной переменной для честных пользователей, либо значительно больше.

Ограничением данной работы является рассмотрение лишь части пути пользователя, система защиты цифрового сервиса от мошенничества не должна ограничиваться лишь верификацией, необходимо мониторить поведение пользователя постоянно. При этом для этапов жизненного цикла пользователя после верификации ключевыми поведенческими показателями будут являться другие переменные. Изучение пути пользователя после верификации будет являться предметом научного интереса авторов для последующих статей.

Литература

1. Donning H., Eriksson M., Martikainen M., & Lehner O. Prevention and detection for risk and fraud in the digital age–the current situation. *ACRN Oxford Journal of Finance and Risk Perspectives*, 2019; 8: 86–97.

2. Дроздов Д. А. Влияние технологии открытых API на развитие рынка финансовых услуг // Вестник Бурятского государственного университета. Экономика и менеджмент. 2024. № 2. С. 57–65. Текст: непосредственный.

3. Dharmavaram V. G., & Mishra O. KYC Fraud: A New Means to Conduct Financial Fraud–How to Tackle It?. *In Cybersecurity Issues, Challenges, and Solutions in the Business World*. 2023: 81–94.

4. Сидоров А. Л. Слабо структурированные проблемы при регистрации пользователей в цифровых сервисах и способы их решения // Системный анализ в проектировании и управлении. 2024. № 27(2). С. 381–386. Текст: непосредственный.

5. Сидоров А. Л. Актуальность внедрения дополнительных защитных мер для цифровых сервисов при регистрации пользователей // Актуальные аспекты модернизации российской экономики. Санкт-Петербург, 2022. С. 282–287. Текст: непосредственный.

6. Hilal W., Gadsden S. A., & Yawney J. Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*. 2022; 193.

7. Pourhabibi T., Ong K. L., Kam B. H., & Boo Y. L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*. 2020; 133.

8. Parate S., Josyula H. P., & Reddi L. T. Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*. 2023. 5(9). 128–137.

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

10. Rafiq M., & Sohail M. K. Anti-Money Laundering (AML) and Regulatory Technology: A Systematic Literature Review. Journal of Asian Development Studies. 2023; 12(3): 949–965.

11. Kadyshevitch D. Generative AI has democratised fraud and cybercrime. *Computer Fraud & Security*. 2024; 5.

12. Mansoor N., Antora K. F., Deb P., Arman T. A., Manaf A. A., & Zareei M. A review of blockchain approaches for kyc. IEEE Access. New Delhi, 2023.

13. Rani M., Zolkaflil S., & Nazri S. The money mule red flags in anti-money laundering transaction monitoring investigation. *International Journal of Business and Economy*. 2022; 4(1): 150–163.

14. Rani M. I. A., Zolkaflil S., & Nazri S. Money mule risk assessment: an introductory guidance for financial crime compliance officers. *Asian Journal of Research in Business and Management*. 2022; 4(1): 208–217.

15. Bello O. A., & Olufemi K. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*. 2024; 5(6): 1505–1520.

16. Khare P., & Srivastava S. AI-Powered Fraud Prevention: A Comprehensive Analysis of Machine Learning Applications in Online Transactions. 2023; 10: 518–525.

Статья поступила в редакцию 24.12.2024; одобрена после рецензирования 23.01.2025; принята к публикации 24.01.2025.

Importance of Behavioral Anomalies in Detecting Digital Fraudsters at the Verification Stage

Arseny L. Sidorov
Research Assistant
arseniiy.sidorov@gmail.com

Andrey A.Vinyukov
Research Assistant
andrey.vinyukov.99@mail.ru

Ulyanov (Lenin) Saint Petersburg State Electrotechnical University "LETI"
5 Professora Popova St., Saint Petersburg 197376, Russia

Abstract. Digital fraud is becoming increasingly complex and sophisticated, and is also growing in volume, which requires improving the mechanisms for protecting digital services. The article discusses the importance of behavioral anomalies for identifying fraudsters at the verification stage. It presents the results of an experiment using the gradient boosting model (Catboost). While analyzing the data of 100,000 users, we have identified 2863 of them as fraudsters. The key behavioral factors, anomalies in which indicate possible fraud, are document loading time, time to complete the biometrics stage, time to fill out the questionnaire, the number of attempts to load documents and biometrics, the average pause between filling in the form fields, and the reaction time when starting the biometrics stage. The results show that the behavior of fraudsters often deviates from the average for these indicators. These data can be effectively used for adapting verification systems in order to minimize losses among honest users, maintaining at that a high level of protection. The limitations of the study are associated with the analysis of only the verification stage, which emphasizes the need for further study of user behavior after this step. The findings emphasize the need for a comprehensive approach to monitoring user behavior to combat digital fraud.
Keywords: verification, digital fraud, user behavior, behavioral anomalies, gradient boosting, biometrics.

For citation
Sidorov A. L., Vinyukov A. A. Importance of Behavioral Anomalies in Detecting Digital Fraudsters at the Verification Stage. *Bulletin of Buryat State University. Economy and Management.* 2025; 1: 119–126 (In Russ.).

The article was submitted 24.12.2024; approved after reviewing 23.01.2025; accepted for publication 24.01.2025.