УДК 336.7 DOI: 10.14451/2.200.41

Эффективность многофакторной аутентификации при финансовых транзакциях: сравнение методов и анализ уязвимостей

© 2025 **Кравец Михаил Юрьевич**
Магистр. Независимый исследователь. Израиль, Тель-Авив.
E-mail: ikravets2008@gmail.com

Ключевые слова: многофакторная аутентификация; финансовые транзакции; биометрия; OTP; фишинг; социальная инженерия.

Статья посвящена исследованию эффективности многофакторной аутентификации (МФА) в финансовом секторе, ее роли в обеспечении безопасности транзакций, защите персональных данных клиентов. Особое внимание уделено анализу двух методов: одноразовых паролей (OTP) и биометрической аутентификации. МФА представляет собой комплексную систему проверки личности, включающую несколько факторов: данные, известные пользователю (пароль), физические носители (смартфон) и уникальные биометрические характеристики (отпечатки пальцев). Использование МФА обеспечивает дополнительную защиту финансовых операций, снижая риск несанкционированного доступа, мошенничества. Исследование выявило, что биометрическая аутентификация достигает 90% снижения случаев мошенничества, значительно превосходя эффективность одноразовых паролей. Однако сложность применения, технические ограничения делают OTP предпочтительным выбором для низкорисковых операций. В статье рассматриваются основные причины неполного устранения мошеннических действий, включая ошибки пользователей, недостаток знаний о методах защиты, внутренние угрозы. Исследование подчеркивает важность образовательных программ, направленных на повышение осведомленности, навыков пользователей для противодействия фишингу, социальной инженерии. Рекомендовано проведение обучающих мероприятий для клиентов, охватывающих правила безопасного использования МФА. Внедрение комплексного подхода, включающего биометрические технологии для высокорисковых транзакций, OTP для низкорисковых операций, обширное обучение пользователей, позволит повысить уровень безопасности, доверия к цифровым финансовым услугам.

Введение

Быстрый рост онлайн-банкинга изменил способы управления финансами, предоставив пользователям небывалые удобство и доступность. Однако вместе с этим цифровым преобразованием возникли и значительные проблемы безопасности, поскольку преступники разрабатывают все более сложные методы для использования уяз-

вимостей в системах онлайн-банкинга. Защита учетных записей пользователей от несанкционированного доступа и финансового мошенничества стала приоритетной задачей как для финансовых учреждений, так и для их клиентов. Для борьбы с этими угрозами необходимо внедрение надежных механизмов аутентификации.

Ранее стандартная аутентификация с помощью логина и пароля считалась достаточной мерой безопасности. Пароль был первой формой аутентификации — секретной фразой или кодом, который обеспечивал доступ к компьютерным ресурсам, таким как программы, файлы, интернет и т.д. Однако люди часто выбирают короткие и простые пароли, так как их легче запомнить. Это делает пароли легкими для подбора и открывает путь для злоумышленников. По данным [9], хакеры могут взломать 20% всех персональных идентификационных номеров (PIN), используя лишь четыре возможные попытки. Более того, они могут получить доступ к учетным записям более 25% пользователей, если будет использовано не более пятнадцати символов. В результате традиционные однофакторные методы аутентификации признаны недостаточно надежными в условиях новых угроз, и популярность стала набирать концепция многофакторной аутентификации (МФА) [3]. МФА требует от пользователей предъявления нескольких факторов для подтверждения личности, обычно включая комбинацию того, что пользователь знает (например, пароль), того, что он имеет (например, физический токен), и того, кем он является (например, биометрические данные). Такой подход добавляет дополнительный уровень защиты.

Двухфакторная аутентификация помогает устранить недостатки однофакторной аутентификации, добавляя дополнительные атрибуты аутентификации и расширяя возможности для подтверждения данных пользователя [10]. Двухфакторная аутентификация обеспечивает клиентам надежную, гибкую и относительно недорогую защиту. Однако она также уязвима для определенных атак. В теории двухфакторная аутентификация может быть скомпрометирована, если злоумышленник получает доступ к мобильному устройству жертвы [6]. Еще одним дополнительным фактором аутентификации может быть использование стороннего сервиса аутентификации, имеющего более высокую степень доверия к ее уровню защищенности. Например, использование государственных информационных систем [7].

Существует три типа информации, на базе которой можно проводить аутентификацию. Информация о том, что пользователь знает, чем пользователь владеет и сами характеристики пользователя. Уровень сложности аутентификации зависит от комбинации этих знаний. Это значительно затрудняет доступ для ботов или злоумышленников, так как, даже преодолев первые два уровня, им будет практически невозможно пройти третий уровень [5].

Кроме того, современные методы безопасности активно используют искусственный интеллект (ИИ) и машинное обучение (МО), что позволяет проводить непрерывный мониторинг и применять адаптивные меры безопасности на основе анализа поведения пользователей, выявляя потенциально несанкционированные действия [1]. Системы обнаружения мошенничества на базе ИИ становятся неотъемлемой частью борьбы с финансовыми преступлениями, особенно когда хакеры стремятся обойти традиционные меры безопасности [2], а комбинация аутентификационных факторов является основой современных систем безопасности в сфере финансов [4; 8].

Цель данного исследования — оценить влияние многофакторной аутентификации на безопасность финансовых транзакций и выявить лучшие практики её реализации. Особое внимание уделено изучению того, как различные факторы аутентификации могут комбинироваться для создания оптимального уровня защиты и минимизации неудобств для конечных пользователей.

Вопросы исследования включают:

– Насколько эффективно использование многофакторной аутентификации предотвращает

несанкционированный доступ к финансовым транзакциям?
- Каковы практические вызовы при внедрении многофакторной аутентификации в финансовых учреждениях?

Данное исследование фокусируется на анализе современных методов и технологий МФА, применяемых в финансовом секторе, и ограничено рассмотрением их использования в банковских и финансовых транзакциях, осуществляемых через цифровые и мобильные платформы.

Основной вклад этого исследования заключается в комплексной оценке эффективности различных подходов к реализации многофакторной аутентификации в финансовых транзакциях и предоставлении рекомендаций для их практического использования.

Методология

Для достижения целей исследования был использован комплексный подход, включающий анализ данных и изучение практических кейсов внедрения многофакторной аутентификации (МФА) в финансовых транзакциях. В данном разделе подробно описаны используемые методы исследования, выбор данных и технологий, а также процесс анализа полученной информации.

Дизайн исследования

Исследование построено как прикладной анализ методов и практик многофакторной аутентификации, реализуемых в современных финансовых учреждениях. Включение нескольких кейсов позволило провести сравнительный анализ различных технологий МФА, что способствовало более глубокому пониманию их воздействия на безопасность транзакций.

Выборка и подбор данных

Для исследования были отобраны данные о транзакциях и применяемых мерах безопасности в нескольких крупных финансовых учреждениях. Ключевые параметры для отбора включали тип используемой аутентификации, частоту успешных и неудачных попыток входа, а также количество случаев предотвращенного мошенничества. Данные собирались в течение последнего года для обеспечения актуальности и отражения текущих практик в индустрии.

Инструменты и технологии

Для анализа данных использовались инструменты статистической обработки и визуализации, такие как Python с библиотеками Pandas и Matplotlib, а также специализированное программное обеспечение для анализа безопасности. Эти инструменты позволили выявить основные тенденции и зависимости между выбранными параметрами.

Процесс сбора данных

Данные были получены с помощью сотрудничества с финансовыми учреждениями. По их просьбе названия этих учреждений в статье не упоминаются. В процессе сбора данных был соблюден принцип конфиденциальности и анонимности для защиты коммерческой информации и персональных данных клиентов.

Методы анализа данных

Для интерпретации данных применялись методы статистического анализа, включая корреляционный анализ и регрессионный анализ, что позволило выявить значимые связи между факторами аутентификации и уровнем безопасности транзакций. Для обработки качественных данных использовался контент-анализ, который позволил обобщить информацию о практических кейсах внедрения МФА и выделить ключевые аспекты успешных и неудачных подходов к реализации.

Эти методы и подходы обеспечили глубокий и структурированный анализ влияния многофакторной аутентификации на безопасность финансовых транзакций и позволили ответить на основные вопросы исследования.

Результаты и обсуждение

Анализ данных продемонстрировал значительное снижение числа мошеннических операций при использовании многофакторной аутентификации (МФА) в финансовых учреждениях, причем степень снижения варьируется в зависимости от выбранного метода аутентификации. На диаграмме «Случаи мошенничества до и после МФА» (рис. 1) представлены данные о количестве мошеннических операций до и после внедрения

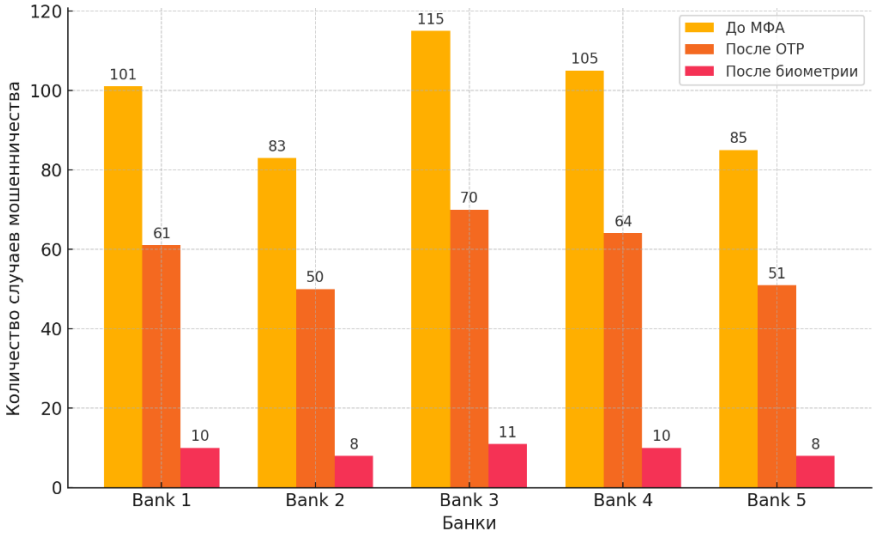

Рис. 1. Случаи мошенничества до и после МФА (OTP vs. Биометрия).

МФА с двумя различными подходами: OTP (одноразовые пароли) и биометрия.

1. **OTP (One-Time Password)**: Внедрение одноразовых паролей (OTP) позволило снизить случаи мошенничества на 39%. Хотя OTP предоставляет ощутимый уровень дополнительной защиты, сохраняются уязвимости, особенно перед атаками социальной инженерии, такими как фишинг. В таких случаях злоумышленники обманом получают одноразовый пароль у пользователя, что делает OTP менее надежным. Однако за счет своей доступности и простоты OTP продолжает оставаться популярным методом защиты при умеренном уровне риска.
2. **Биометрия**: Биометрическая аутентификация, включающая такие данные, как распознавание лица или отпечатков пальцев, обеспечила снижение случаев мошенничества на 90%. Этот результат значительно превосходит эффективность OTP, что объясняется уникальностью биометрических характеристик пользователя, которые практически невозможно подделать или передать. Внедрение биометрии создает дополнительный барьер для злоумышленников, так как биометрические данные привязаны непосредственно к пользователю, что делает их сложными для обхода или подмены.

Причины неполного сокращения мошенничества

Несмотря на высокий уровень защиты, обеспечиваемый МФА, исследование показало, что случаи мошенничества не были полностью устранены. На диаграмме «Причины неполного сокращения мошенничества» (рис. 2) показаны основные факторы, ограничивающие возможности полного искоренения мошеннических операций.

- **Ошибка пользователя (например, фишинг)** – 42%. Фишинг и другие формы социальной инженерии являются основными факторами уязвимости, так как пользователи могут по ошибке раскрыть свои данные мошенникам. Это указывает на важность повышения осведомленности пользователей и обучения их основам противодействия таким атакам.
- **Недостаточная осведомленность о безопасности** – 52%.Значительная часть пользователей недостаточно осведомлена о рисках и значимости мер безопасности, таких как МФА. Низкий уровень знаний о безопасности увеличивает вероятность успешных атак, поскольку пользователи могут не осознавать, какие данные можно передавать, а какие – нет. Это подчеркивает необходимость образовательных программ для пользователей, направленных на повышение их компетентности в вопросах безопасности.

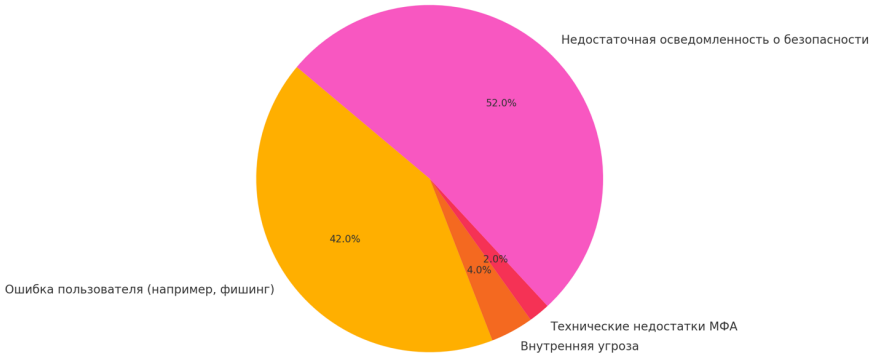

Рис. 2. Причины неполного сокращения мошенничества.

- **Внутренняя угроза** — 4%. Злоупотребление со стороны сотрудников или лиц с доступом к системе представляют незначительную, но всё же реальную угрозу. Хотя такие случаи редки, они требуют усиленного контроля и дополнительных мер безопасности на уровне компании.
- **Технические недостатки** — 2%. Внедрение МФА может сопровождаться техническими сбоями или недостатками в инфраструктуре, что допускает редкие, но возможные случаи обхода системы. Для повышения надежности таких систем необходимы дополнительные инвестиции в тестирование и улучшение инфраструктуры.

Влияние OTP и биометрии на ключевые показатели

Диаграмма «Влияние OTP и биометрии на основные показатели» (рис. 3) представляет собой оценку восприятия безопасности пользователями, а также удобства использования и устойчивости к техническим сбоям для каждого из методов аутентификации

1. **Доверие пользователей**. Биометрия вызывает больше доверия у пользователей (85%), чем OTP (70%). Пользователи считают биометрические методы более надежными и безопасными, поскольку они связаны с уникальными личными характеристиками. Этот фактор играет решающую роль в повышении доверия клиентов к финансовым учреждениям, использующим МФА.
2. **Неудобство использования.** Несмотря на высокую степень доверия, биометрия вызывает больше неудобств для пользователей (25%) по сравнению с OTP (15%). Биометрические системы могут быть сложны в использовании при определенных условиях (например, при плохом освещении для распознавания лица), что может снижать удобство для пользователей.
3. **Технические сбои.** Биометрия имеет более низкий уровень технических сбоев (3%) по сравнению с OTP (7%), поскольку биометрические данные обеспечивают более стабильную и уникальную идентификацию, уменьшая вероятность ошибок, связанных с передачей одноразовых паролей.

Результаты анализа показывают, что биометрические методы аутентификации существенно превосходят OTP по уровню безопасности, что делает их предпочтительным выбором для высокорисковых транзакций. Однако неудобство использования и техническая сложность биометрии делают OTP более приемлемым выбором для транзакций с низким и средним уровнем риска, где необходим баланс между безопасностью и удобством.

Особое внимание необходимо уделить образовательной составляющей. На основе выявленных причин уязвимости ясно, что основной вклад в неполное сокращение мошенничества вносит недостаточная осведомленность пользователей и ошибки, связанные с фишингом и социальной инженерией. Финансовым учреждениям рекомендуется проводить регулярные обучающие

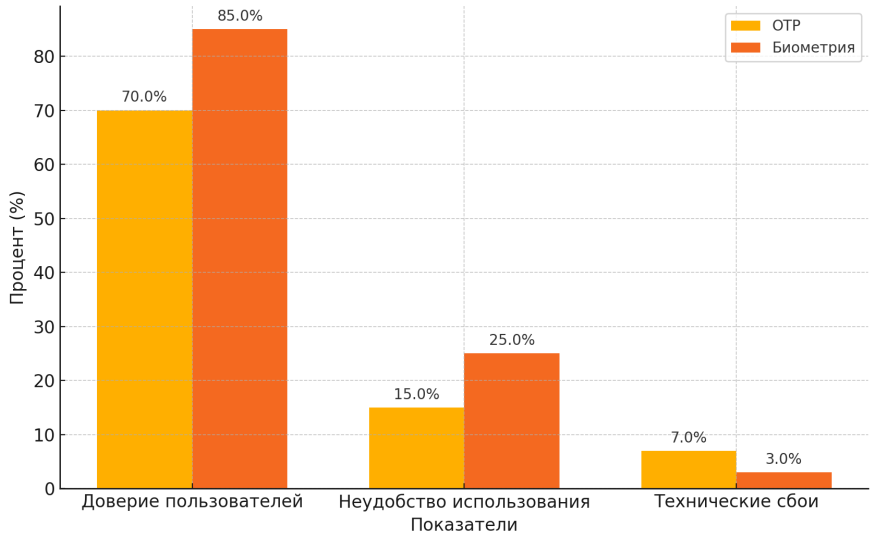

Рис. 3. Влияние OTP и биометрии на основные показатели.

программы, направленные на повышение знаний пользователей о безопасном использовании МФА и способах противодействия социальной инженерии. Такие программы должны включать обучение по следующим аспектам:

1. **Распознавание фишинговых атак** — объяснение пользователям, как определять подозрительные сообщения и запросы, которые могут быть частью фишинга.
2. **Понимание важности МФА** — обучение пользователей значению и роли каждого фактора МФА, чтобы повысить их приверженность к использованию более сложных методов аутентификации.
3. **Безопасное обращение с личной информацией** — указания по защите конфиденциальной информации, которые помогут предотвратить непреднамеренное раскрытие данных мошенникам.

Таким образом, внедрение комплексного подхода, сочетающего биометрические методы для высокорисковых операций, OTP для менее критичных транзакций и обширные образовательные программы для пользователей, позволит значительно повысить уровень защиты финансовых транзакций.

Заключение

Проведенное исследование продемонстрировало значительную эффективность многофакторной аутентификации (МФА) в снижении случаев мошенничества в финансовом секторе. Основной акцент был сделан на сравнении двух подходов к МФА: одноразовых паролей (OTP) и биометрических методов. Результаты показали, что биометрия обеспечивает более высокий уровень безопасности, снижая случаи мошенничества на 90%, тогда как OTP достигает 39%-ного снижения. Эти данные подтверждают, что использование биометрии является предпочтительным выбором для высокорисковых транзакций, в то время как OTP остается эффективным и удобным решением для менее критичных операций.

Ответы на исследовательские вопросы подтверждают важность многослойного подхода к аутентификации, учитывающего специфику использования различных факторов безопасности. Анализ причин, препятствующих полному устранению мошенничества, показал, что основными уязвимостями остаются человеческие ошибки, такие как фишинг, и низкий уровень осведомленности среди пользователей. Также были выявлены ограниченные случаи внутренних угроз и технических сбоев, которые подчеркивают важность постоянного совершенствования систем безопасности.

Вклад данного исследования заключается в понимании того, какие факторы МФА являются наиболее эффективными и удобными для пользователей, а также в выявлении ключевых причин, препятствующих полному устранению угроз. Эти данные представляют ценность для финансовых учреждений, стремящихся повысить защиту транзакций и улучшить взаимодействие с клиентами.

Для дальнейшего повышения безопасности финансовых операций рекомендуется внедрять комплексные программы обучения пользователей, которые помогут противостоять фишингу и другим видам социальной инженерии. Повышение осведомленности, обучение распознаванию угроз и правилам безопасного использования МФА станут важными мерами для уменьшения человеческого фактора в уязвимостях.

В будущем целесообразно продолжить исследования, направленные на интеграцию МФА с инновационными технологиями, такими как машинное обучение и блокчейн, чтобы адаптировать системы безопасности к новым угрозам и потребностям пользователей.

Библиографический список

1. *Довгаль В. А.*, *Довгаль Д. В.* Анализ перспективных методов поведенческой биометрии для аутентификации пользователей // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2017. — 3 (206). — URL: https://cyberleninka.ru/article/n/analiz-perspektivnyh-metodov-povedencheskoy-biometrii-dlya-autentifikatsii-polzovateley (дата обр. 13.11.2024).
2. *Нестерова В. А.*, *Рыбакова В. А.* Обзор использования искусственного интеллекта в обнаружении финансового мошенничества // Экономика и парадигма нового времени. — 2024. — 1 (22). — URL: https://cyberleninka.ru/article/n/obzor-ispolzovaniya-iskusstvennogo-intellekta-v-obnaruzhenii-finansovogo-moshennichestva (дата обр. 13.11.2024).
3. A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure / S. P. Otta [et al.] // Future Internet. — 2023. — Apr. — Vol. 15, no. 4. — P. 146. — ISSN 1999-5903. — DOI: 10.3390/fi15040146.
4. *Aburbeian A. M.*, *Fernández-Veiga M.* Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning // AI. — 2024. — Jan. — Vol. 5, no. 1. — P. 177–194. — ISSN 2673-2688. — DOI: 10.3390/ai5010010.
5. *Chauhan E. V.*, *Parekh D. C.*, *Joshi P. V.* Three Factor Authentication Novel Framework through Improve System Privacy and Data Security // International Journal of Scientific Research in Science, Engineering and Technology. — 2021. — May. — P. 183–190. — ISSN 2395-1990. — DOI: 10.32628/ijsrset218324.
6. *Kabir M. S.*, *Olanrewaju O. M.*, *Mukhtar A.* RatHole: Authentication Algorithm for Controling Access to Mobile Phone File Management System // Journal of Basics and Applied Sciences Research. — 2024. — May. — Vol. 2, no. 1. — P. 35–45. — ISSN 3026-9091. — DOI: 10.33003/jobasr-2024-v2i1-29.
7. *Kravets M.* Using national identification systems to reduce banks' operational costs. — 2024. — DOI: 10.5281/ZENODO.11312089.
8. *Lomba E.*, *Severino R.*, *Vilas A. F.* Work In Progress: Towards Adaptive RF Fingerprint-based Authentication of IIoT devices // 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA). — IEEE, 09/2022. — P. 1–4. — DOI: 10.1109/etfa52439.2022.9921575.
9. Understanding Human-Chosen PINs: Characteristics, Distribution and Security / D. Wang [et al.] // Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security. — ACM, 04/2017. — P. 372–385. — (ASIA CCS '17). — DOI: 10.1145/3052973.3053031.
10. User authentication on mobile devices: Approaches, threats and trends / C. Wang [et al.] // Computer Networks. — 2020. — Apr. — Vol. 170. — P. 107118. — ISSN 1389-1286. — DOI: 10.1016/j.comnet.2020.107118.