***Петров Александр Васильевич***
студент
ФГБОУ ВО «Чувашский государственный
университет им. И.Н. Ульянова»
г. Чебоксары, Чувашская Республика

# ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ И ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ЗАЩИТЫ БАНКОВСКИХ АККАУНТОВ ОТ МОШЕННИЧЕСТВА

***Аннотация****: в статье рассматривается применение биометрических технологий и двухфакторной аутентификации для защиты банковских аккаунтов от мошенничества. Описываются преимущества многофакторной аутентификации, снижение риска утечки данных и соответствие нормативным требованиям. Обсуждаются проблемы и вызовы, связанные с внедрением этих технологий, и предлагаются рекомендации для успешного внедрения и обучения пользователей.*

***Ключевые слова****: двухфакторная аутентификация, биометрические технологии, банковская система, защита от мошенничества, защита от банковских мошенников.*

В современном мире информационная безопасность играет ключевую роль в обеспечении стабильности и функционирования различных сфер деятельности [2]. Биометрические технологии и двухфакторная аутентификация являются одними из наиболее эффективных методов защиты информации и доступа к различным системам [4].

Биометрические технологии – это методы идентификации и аутентификации личности, основанные на уникальных физиологических и поведенческих характеристиках человека [3]. Они включают в себя распознавание отпечатков пальцев, радужной оболочки глаза, голоса, геометрии лица и других параметров.



Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Двухфакторная аутентификация – это процесс подтверждения личности пользователя, основанный на использовании двух независимых факторов: знания (например, пароль) и владения (например, токен или смарт-карта).

Преимущества использования биометрических технологий и двухфакторной аутентификации в банках.

1. Повышение уровня безопасности: биометрические данные и двухфакторная аутентификация обеспечивают более надёжную защиту финансовых средств клиентов от мошенничества и кражи.

2. Удобство для клиентов: использование биометрических данных и двухфакторной аутентификации упрощает процесс идентификации и аутентификации, сокращая время и усилия клиентов при получении банковских услуг.

3. Улучшение качества обслуживания: внедрение биометрических технологий и двухфакторной аутентификации позволяет банкам предоставлять клиентам более удобные и быстрые услуги, что повышает удовлетворённость клиентов и стимулирует их лояльность [5].

Рассмотрим основные виды биометрических технологий и их применение.

1. Отпечатки пальцев:

– один из самых распространённых видов биометрической идентификации;

– используются в системах безопасности (замки с отпечатками пальцев, смартфоны, ноутбуки);

– уникальны для каждого человека и могут быть использованы для идентификации личности.

2. Радужная оболочка глаза:

– распространённый тип биометрической идентификации;

– применяется в системах безопасности аэропортов, военных базах, государственных структурах;

– неповторима для каждого человека и может быть применена для опознания личности.

3. Голос:

– ещё один вид биометрической идентификации;


Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

– используется в системах распознавания речи (мобильные телефоны, смартфоны и другие устройства);

– уникален для каждого человека и может быть использован для идентификации личности.

4. Геометрия лица:

– метод биометрической идентификации, основанный на использовании трёхмерной карты лица для определения личности;

– применяется в различных системах безопасности (банкоматы, системы контроля доступа);

– уникален для каждого человека и может быть использован для идентификации личности.

5. Термограмма лица:

– инновационный способ биометрической идентификации, основанный на использовании инфракрасных изображений черт лица для распознавания личности;

– применяется в сфере безопасности (аэропорты, военные объекты);

– обладает уникальными характеристиками для каждого человека, что делает его эффективным инструментом для определения личности.

Биометрическая аутентификация – это надёжный способ усилить защиту аккаунтов пользователей. Выбор метода аутентификации зависит от предпочтений пользователя, его нужд и возможностей.

1. Одноразовые пароли.

Они создаются специальными приложениями или сервисами и отправляются пользователю на электронную почту или мобильный телефон. При входе в аккаунт пользователь вводит полученный пароль и подтверждает свою личность.

2. Многофакторные токены.

Это физические устройства, такие как USB-ключи, смарт-карты или брелоки. Пользователю необходимо иметь при себе физический токен при каждом входе в систему. Токены генерируют одноразовые пароли, которые нужно вводить для подтверждения личности.



Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

3. Временные коды.

Это одноразовые коды, которые отправляются пользователю через SMS или голосовые сообщения. Пользователю необходимо ввести код в специальное поле на сайте или приложении для подтверждения своей личности.

4. Биометрическая аутентификация.

Она использует уникальные физические характеристики пользователя, такие как отпечатки пальцев, голос, сетчатку глаза или геометрию лица, для подтверждения личности.

5. Аутентификация по PIN-коду.

PIN-код – это цифровой пароль, который пользователь устанавливает самостоятельно. При входе в аккаунт пользователь должен ввести PIN-код для подтверждения своей личности.

6. Аутентификация по кодам восстановления.

Коды восстановления – это резервные коды, которые пользователь получает вместе с одноразовыми паролями или временными кодами. Коды восстановления используются для восстановления доступа к аккаунту в случае потери доступа к основному методу аутентификации.

Биометрические технологии, такие как распознавание отпечатков пальцев, радужной оболочки глаза и голоса, основаны на уникальных физических характеристиках человека. Однако эти технологии могут быть подвержены ошибкам и сбоям, что может привести к несанкционированному доступу к учётным записям.

Сбор и хранение биометрических данных вызывает опасения относительно конфиденциальности пользователей. Кроме того, существует риск утечки данных и их использования в мошеннических целях [1].

Совместимость и интеграция биометрических технологий и двухфакторной аутентификации с различными устройствами и операционными системами может вызвать проблемы. Это может затруднить поддержку разных платформ.

Стоимость и доступность биометрических технологий и двухфакторной аутентификации могут быть проблемой для некоторых пользователей. Не все


Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

люди имеют доступ к современным устройствам и технологиям, что ограничивает их использование.

Наконец, многие пользователи могут быть незнакомы с биометрическими технологиями и двухфакторной аутентификацией. Это может привести к неправильному использованию этих инструментов и снижению их эффективности.

Рекомендации по успешному внедрению и использованию биометрических технологий и двухфакторной аутентификации:

1. Проведите исследование доступных методов аутентификации и выберите наиболее подходящие для ваших нужд.

2. Решите, какие факторы аутентификации будете использовать, например, SMS, Google Authenticator или биометрические данные.

3. Включите многофакторную аутентификацию в настройках выбранного приложения или веб-сайта.

4. Зарегистрируйте дополнительные устройства, если планируете использовать их для аутентификации.

5. Проверьте работу многофакторной аутентификации перед полным использованием.

6. Обучите пользователей правильному использованию MFA, создайте руководство или видеоуроки.

7. Следите за использованием MFA и контролируйте доступ к учётным записям.

Использование биометрических технологий и двухфакторной аутентификации является важным шагом для обеспечения безопасности банковских аккаунтов. Эти методы повышают уровень защиты, снижают риск утечки данных и соответствуют нормативным требованиям.



Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

***Список литературы***

1. Аркадьева О.Г. Формирование модели государственного регулирования развития технологий искусственного интеллекта в финансовом секторе / О.Г. Аркадьева, Н.В. Березина // Oeconomia et Jus. – 2023. – №4. – С. 12–21. DOI 10.47026/2499-9636-2023-4-12-21. EDN RXEYSM

2. Аркадьева О.Г. Влияние парадигмы безопасности на функции управления финансами / О.Г. Аркадьева // Проблемы обеспечения безопасности: Материалы III Междунар. науч.-практ. конф. – Т. 1. – Уфа: Уфимский гос. авиац. техн. ун-т, 2021. – С. 239–242. EDN LULXZW

3. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с.

4. Русскевич Е.А. Мошенничество в сфере компьютерной информации / Е.А. Русскевич, М.Д. Фролов. – М.: Инфра-М, 2020. – 148 с. – EDN NDWYZW

5. Биометрия в финансовой сфере 2020: выгоды для потребителя [Электронный ресурс]. – Режим доступа: https://www.fintechru.org/upload/iblock/b1b/AZ-Biometriya-0806.pdf (дата обращения: 10.09.2024).


Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)