УДК 33(30)

АКТУАЛЬНЫЕ СПОСОБЫ ЗАЩИТЫ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ ОТ УГРОЗ В ЦИФРОВОЙ СРЕДЕ

Элизбарян Элен Арменовна

ФБГОУ ВО «Российский государственный аграрный университет – Московская сельскохозяйственная академия имени К.А. Тимирязева», Москва, Россия (127434, Москва, ул. Тимирязевская, 49), студентка 4 курса института экономики и управления АПК, elizbarelen2003@gmail.com

Аннотация. Современный мир на протяжении многих лет сталкивается с различным видом угроз в цифровой среде - от мошенничества до фишингов. Существуют много способы защиты предпринимательской деятельности от взломов, в том числе и биометрия, которая предлагает революционное решение для повышения безопасности бизнеса. В ходе работы были рассмотрены виды биометрии, риски и способы защиты своих биометрических данных.

Ключевые слова: биометрия; предпринимательство; защита; угрозы.

Научный руководитель: Рахаева Виктория Владимировна

ФБГОУ ВО «Российский государственный аграрный университет – Московская сельскохозяйственная академия имени К.А. Тимирязева», Москва, Россия (127434, Москва, ул. Тимирязевская, 49), к.э.н, доцент кафедры экономической безопасности и права, v_rahaeva@rgau-msha.ru, +74999763941

CURRENT WAYS TO PROTECT BUSINESS ACTIVITIES FROM THREATS IN THE DIGITAL ENVIRONMENT

Elizbaryan Elen Armenovna

Abstract. The modern world has been faced with various types of threats in the digital environment for many years - from fraud to phishing. There are many ways to protect businesses from hacking, including biometrics, which offers a revolutionary solution to improve business security. During the work, types of biometrics, risks and ways to protect one's biometric data were considered.

Key words: biometrics; entrepreneurship; protection; threats.

Rakhaeva Victoria Vladimirovna

Russian State Agrarian University – Moscow Timiryazev Agricultural Academy, Moscow, Russia (127434, Moscow, Timiryazevskaya street 49), candidate of Economic Sciences, Associate Professor of the Department of Economic Security and Law, v_rahaeva@rgau-msha.ru, +74999763941

Введение. В XXI веке все более актуальными становятся вопросы безопасности и идентификации пользователей. Методы защиты как пароли и PIN-коды не так эффективно могут обеспечивать надежный уровень защиты, тем самым уступая места более инновационным технологий – биометрии.

Биометрия – уникальные физиологические и биологические характеристики человека, которые используются для установления или подтверждения личности [6]. Тем самым, в отличие от других способ защиты их тяжелее подделать и взломать. Современные биометрические системы используют отпечатки пальцев, распознание лица и анализ голоса и множество других принципов и технологий,

Биометрические данные давно нашли применение в современных технологий, однако они также используются и в самых различных сферах: медицина, финансовая сфера, правоохранительные органы и так далее.

Биометрия представляет собой новый веток обеспечения безопасности, что делает его опасные инструментов в руках злоумышленников, ведь они осознавая потенциал биометрии ищут способы ее использования в неправомерных мерах. Люде же, к сожалению, не осознают потенциальные угрозы скрывающиеся за этой инновацией.

Цель исследования. Цель исследования – повышение уровня общественного осознания о важности защиты своих биометрических данных и методах их сохранности.

Методы исследования. В процессе исследования были использованы методы: сравнительно-аналитический и эмпирический.

Результаты исследования и их обсуждения. Биометрия – технология, которая использует уникальные биологические и поведенческие характеристики человека для идентификации личности [6]. В России внедрена Единая Биометрическая Система (ЕБС), которая обеспечивает сбор, хранение и использование биометрических данных для аутентификации и идентификации пользователей [3].

Преимуществами ЕБС являются:

• Удобство: ЕБС позволяет проходить идентификацию всего один раз и получать услуги удаленно, что особенно актуально для маломобильных граждан и жителей удаленных регионов.

• Безопасность: Система обеспечивает надежную защиту от взлома, кражи и подделки данных.

• Развитие сервисов: ЕБС позволяет банкам и другим организациям развивать удобные онлайн-сервисы, такие как открытие счетов, получение кредитов, перевод денег.

В наше время биометрии применяется во многих сферах жизни. Так, биометрия укрепляет безопасность платежей и управления учетными записями, особенно в онлайн-банкинге; биометрические паспорта, системы контроля доступа, визовые службы усиливают безопасность и эффективность процессов идентификации и также биометрия обеспечивает удобство

посетителей спортивных организаций и укрепляет безопасность за счет автоматизации регистрации и контроля доступа.

Биометрия может принимать самые различные обличия:

1) Отпечаток пальца: Один из самых распространенных методов.

2) Изображение лица: Используется в системах распознавания лиц.

3) Голос: Анализ голоса для идентификации и аутентификации.

4)Радужная оболочка глаза: Высокоточное и надежное средство идентификации.

5) Рисунок вен ладони: Относительно новый метод, который используется в системах контроля доступа.

Биометрия имеет множество преимуществ, так биологические характеристики человека уникальны, соответсвенно подделать и взломать их не так легко, вместе с тем они предлагают высокий уровень безопасности и за счет того что пользователю не нужно запоминать никакие пароли, то биометрии упрощает процесс идентификации и аутентификации. [2]

Вместе с тем у биометрии есть существенные недостатки, которые также следует рассмотреть:

- Стоимость: внедрение биометрических систем может быть дорогостоящим.
- Технические ограничения: точность и эффективность биометрических систем могут быть ограничены техническими факторами, такими как качество оборудования или освещение.
- Риск нарушения приватности: хранение и использование биометрических данных создают риск их неправомерного использования.

Для полной картины нужно рассмотреть процесс работы ЕБС. Представьте, что вы приходите в банк, чтобы снять деньги, но забыли паспорт.

В таком случае если вы зарегистрировали свою биометрию, то возможен такой сценарий:

1. Камера в кассе сфотографирует ваше лицо.
2. Эта фотография преобразуется в уникальный векторный формат с помощью искусственного интеллекта.
3. Вектор отправляется на сервер ЕБС для сравнения с базой данных биометрических шаблонов других клиентов.
4. Если соответствие найдено, система подтвердит вашу личность, и кассир сможет выдать деньги.

Безусловно несмотря на инновационные технологии биометрия не может обеспечить полную защиту, поэтому выделим ряд рисков при использовании биометрии [1]:

- Нарушение конфиденциальности: Утечка биометрических данных может привести к краже личности и доступу к защищенной информации.
- Возможность кражи личности: Злоумышленники

могут использовать украденные биометрические данные для подделки личности.

- Необратимость: В отличие от паролей, биометрические данные нельзя легко изменить или сменить в случае утечки.
- Технические проблемы: Сбои в работе сканеров отпечатков пальцев, распознавания лица или других биометрических технологий могут привести к отказу в доступе.

Вместе с осознанием рисков использования биометрии следует перечислить способы защиты биометрии [4], которые необходимо применять как отдельным лицам, так и государству.

- Безопасное хранение: Биометрические данные хранятся только в виде набора цифр, которые невозможно использовать или расшифровать без специального доступа.
- Многофакторная аутентификация: Использование нескольких методов идентификации (биометрических и не биометрических) увеличивает безопасность.
- Отменяемая биометрия: Разрабатываются технологии, которые искажают биометрические данные при хранении, что делает их бесполезными для злоумышленников.
- Проверка на уровне «окружающей среды»: Современные системы распознавания лица учитывают не только изображение лица, но и окружающую среду, что позволяет отличить поддельные изображения от реальных людей.
- Проверка на уровне цветового спектра: Современные биометрические терминалы анализируют изображение в нескольких спектрах, что делает попытки обмана с помощью поддельных фотографий менее эффективными.
- Алгоритмы Liveness: Эти алгоритмы проверяют, что перед камерой находится живой человек, а не изображение или видео [5].

Выводы. Следуя нижеперечисленным рекомендациям, вы можете минимизировать риски, связанные с использованием биометрии, и обеспечить безопасность своих личных данных в цифровом мире.

Будьте осторожны с кем вы делитесь своими биометрическими данными. Ваши биометрические данные — это личная информация. Никогда не предоставляйте их сайтам, компаниям или людям, которым вы не доверяете.

Используйте двухфакторную аутентификацию. Если данная опция доступна, всегда используйте двухфакторную аутентификацию. Это может добавить дополнительный уровень безопасности к вашим аккаунтам и усложнить задачу мошенникам.

Следите за своими аккаунтами. Регулярно проверяйте свои банковские и кредитные отчеты на предмет необычной активности. Если вы заметите что-то подозрительное, немедленно свяжитесь с вашим банком.

В случае обнаружения махинаций, действуйте быстро. Если вы подозреваете, что ваши биометрические данные были скомпрометированы, немедленно сообщите об этом вашему банку и / или соответствующим властям.

Участвуйте в защите своих данных. Если вы предоставили биометрические данные финансовым институтам или другим организациям, убедитесь, что они входят в реестр аккредитованных организаций, имеющих право работать с биометрическими данными.

Важно помнить: биометрические данные уникальны и их нельзя изменить. Будьте бдительны и защищайте свою биометрию, чтобы избежать потенциальных проблем в будущем.

Список литературы

1. Биометрические данные и риски их утечки // Центр подготовки РКЦТ, [Электронный ресурс]. URL: https://cdto.ranepa.ru/sum-of-tech/materials/49 (дата обращения: 04.07.2024).

2. Все, что вы хотели знать о биометрии и Единой биометрической системе // Росбанк, [Электронный ресурс]. URL: https://www.rosbank.ru/o-banke/biometriya/ (дата обращения: 03.07.2024).

3. Единая биометрическая система // Википедия, [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Единая_биометрическая_система (дата обращения: 02.07.2024).

4. Защита биометрических персональных данных // RTM GROUP, [Электронный ресурс]. URL: https://rtmtech.ru/articles/biodata-protect/ (дата обращения: 05.07.2024).

5. Создавайте мобильные и веб-приложения со встроенной биометрической идентификацией пользователей для себя и своих клиентов// NTECH LAB, [Электронный ресурс]. URL: https://ntechlab.ru/liveness-sdk/ (дата обращения: 06.07.2024).

6. Что такое биометрия // Госуслуги, [Электронный ресурс]. URL: https://www.gosuslugi.ru/help/faq/biometrics/10201 (дата обращения: 01.07.2024).