Золотова Евгения Георгиевна, ФГБОУ ВО «Уфимский государственный нефтяной технический университет», студент,
zolotova.evgeniya2003@mail.ru

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ. УДОБСТВО ИЛИ ДЫРА В БЕЗОПАСНОСТИ

Аннотация. Статья посвящена анализу биометрической аутентификации как перспективного, но противоречивого метода защиты информации. Рассматриваются её ключевые преимущества: удобство, уникальность характеристик, снижение эксплуатационных затрат и интеграция с цифровыми системами. Однако авторы акцентируют риски: уязвимость биометрических данных при утечке, технические ошибки распознавания, этико-правовые вопросы и зависимость от инфраструктуры. Особое внимание уделено регулированию в РФ: Единая биометрическая система (ЕБС) и законодательство (ФЗ № 152, 187) требуют письменного согласия на обработку данных, но сохраняются пробелы в защите. Подчёркивается необходимость баланса между технологическим прогрессом и приватностью: будущее биометрии зависит от усиления шифрования, регуляторных мер и осознанности пользователей. Статья служит основой для дискуссии о безопасном внедрении биометрических решений в условиях цифровизации.

Ключевые слова: биометрическая аутентификация, информационная безопасность, конфиденциальность данных, Единая биометрическая система (ЕБС), нормативное регулирование.

Abstract. The article analyzes biometric authentication as a promising but controversial method of information security. Its key advantages are considered: convenience, unique characteristics, reduced operating costs, and integration with digital systems. However, the authors emphasize the risks: vulnerability of biometric data in case of leakage, technical recognition errors, ethical and legal issues, and dependence on infrastructure. Particular attention is paid to regulation

in the Russian Federation: the Unified Biometric System (UBS) and legislation (Federal Laws No. 152, 187) require written consent for data processing, but gaps in protection remain. The need for a balance between technological progress and privacy is emphasized: the future of biometrics depends on stronger encryption, regulatory measures, and user awareness. The article serves as a basis for a discussion on the safe implementation of biometric solutions in the context of digitalization.

Keywords: biometric authentication, information security, data privacy, Unified Biometric System (UBS), regulatory framework.

В современном мире безопасность информации приобретает все более важное значение. С развитием технологий, системы аутентификации становятся всё более разнообразными и сложными. Одним из наиболее обсуждаемых методов аутентификации является биометрическая, которая основывается на уникальных физических или поведенческих характеристиках человека. Биометрическая аутентификация представляет собой метод идентификации и подтверждения личности пользователей на основе уникальных биологических характеристик, таких как отпечатки пальцев, сканирование радужной оболочки глаза, распознавание лиц и голоса. В последние годы биометрические технологии приобрели огромную популярность благодаря своей способности повышать удобство и безопасность, особенно в эпоху цифровизации, когда традиционные пароли становятся недостаточно надежными. Однако наряду с преимуществами, данный подход также вызывает серьёзные опасения в области безопасности.

Биометрия (от др.-греч. βίος — «жизнь» и μετρέω — «измеряю») — это распознавание личности на основе уникальных биологических и поведенческих характеристик [1]. К основным видам биометрии относятся физическая биометрия (использование уникальных узоров на коже пальцев, анализ уникальных узоров радужной оболочки, распознавание по чертам

лица, измерение размеров и пропорций рук) и поведенческая биометрия (идентификация по особенностям голоса, определение человека по его почерку или способу написания) [2].

Аутентификация – это процесс проверки пользователя, при которой система проверяет и подтверждает действительную подлинность пользователя [3].

На основе двух определениях, описанных выше, можем сделать вывод, что биометрическая аутентификация — это процесс проверки пользователя с целью подтверждения подлинности самого пользователя с помощью распознавания уникальных биологических и поведенческих характеристик [2, 3].

Далее в статье рассмотрим преимущества биометрической аутентификации.

1. Удобство использования. Биометрическая аутентификация, как правило, быстрее и проще в использовании по сравнению с паролями или PIN-кодами. Пользователь может легко идентифицировать себя, прикоснувшись к сканеру отпечатков пальцев или взглянув в камеру.

2. Уникальность характеристик. Биометрические данные труднее подделать по сравнению с традиционными методами аутентификации. Каждый человек имеет уникальные биометрические признаки, что делает эту технологию достаточно надёжной.

3. Снижение количества забытых паролей. Используя биометрию, пользователи избавляются от необходимости запоминать множество паролей, что часто приводит к проблемам с доступом.

4. Снижение затрат на поддержку. Уменьшается количество запросов на сброс паролей, что позволяет сэкономить ресурсы и время IT-отделов.

5. Инклюзивность: Многие биометрические системы могут быть адаптированы для людей с ограниченными возможностями, предоставляя альтернативные способы аутентификации.

6. Интеграция с другими системами. Биометрическую аутентификацию можно легко интегрировать в различные системы, включая мобильные устройства, системы безопасности и банковские приложения.

Хотя биометрическая аутентификация предлагает удобство и высокий уровень безопасности, важно тщательно оценить возможность возникновения этих недостатков и рисков при её внедрении. Биометрическая аутентификация обладает множеством преимуществ, но также имеет недостатки и риски:

1. Конфиденциальность и безопасность данных. Биометрические данные являются уникальными и постоянными. В случае их утечки или кражи (например, отпечатков пальцев или образца ДНК) злоумышленники могут использовать эти данные для несанкционированного доступа. Удалить или изменить биометрические данные невозможно, поэтому пользователю может быть сложно защитить себя, если данные были скомпрометированы.

2. Технические ошибки. Системы биометрической аутентификации могут неправильно идентифицировать пользователей, что может привести к ложным отказам (когда система не распознает законного пользователя) или ложным приемам (когда система распознает мошенника). Зависимость от качества сенсоров: недорогие или устаревшие устройства могут снижать точность распознавания.

3. Сложности с доступом. Некоторые пользователи могут испытывать трудности с использованием биометрических систем (например, люди с ограниченными возможностями или различные медицинские состояния, влияющие на биометрию). Выбор некоторых

характеристик, таких как лицо или голос, может быть неэффективен в определённых условиях (например, плохое освещение или фоновый шум).

4. Правовые и этические вопросы. Использование биометрии поднимает вопросы о согласии, особенно если данные собираются без ведома пользователей или используются не по назначению. Законодательство о защите биометрических данных может варьироваться в зависимости от страны, что создаёт сложности для пользователей и компаний.

5. Выход из строя. В случае повреждения или подделки биометрических данных пользователю может быть сложно восстановить доступ к своим устройствам или аккаунтам. Например, если у пользователя повреждён палец, который использовался для аутентификации, это создаёт трудности.

6. Большая зависимость от технологий. Внедрение биометрических систем требует значительных инвестиций в оборудование и программное обеспечение, а также в обучение персонала. Сбои в системе могут привести к серьёзным последствиям для бизнеса или государственных учреждений.

Единая биометрическая система (ЕБС), запущенная в России в 2018 году по инициативе Центрального банка и Министерства цифрового развития, использует передовые технологии распознавания лиц и голоса для идентификации пользователей. Эта система призвана расширить возможности использования цифровых услуг в различных сферах, от розничной торговли до государственных сервисов. Примерами использования ЕБС являются оплата по лицу в магазинах и оплата проезда в московском метро [4].

Как на территории РФ обстоят дела с защитой биометрических данных? Организация и защита биометрических персональных данных должны соответствовать требованиям, изложенным в следующих

нормативных и правовых документах: Федеральный закон (ФЗ) «О персональных данных» от 27.07.2006 № 152-ФЗ, ФЗ "О связи" от 07.07.2003 N 126-ФЗ, ФЗ 149-ФЗ «Об информации, информационных технологиях и защите информации», ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ, Статья 23 Конституции РФ гарантирует каждому право на неприкосновенность частной жизни, личную и семейную тайну [5]. Биометрические данные человека могут быть обработаны только при наличии его письменного разрешения. Нельзя заставлять кого-либо предоставлять эти данные, кроме случаев, предусмотренных законом. Также запрещено собирать и обрабатывать биометрическую информацию, полученную без предварительного согласия человека, например, с камер видеонаблюдения. Исключения составляют случаи, когда это необходимо для осуществления правосудия, исполнения судебных решений, а также при проведении обязательной дактилоскопической или геномной регистрации [6].

Биометрическая аутентификация — это не однозначное «удобство» или «угроза», а технология, требующая грамотной реализации. Её преимущества неоспоримы, но массовое внедрение без должных мер защиты создает риски для приватности. Будущее биометрии зависит от развития технологий шифрования, ужесточения регуляторных норм и осознанности пользователей.

Литература

1. Биометрия [Электронный ресурс] – Режим доступа https://ru.wikipedia.org/wiki/Биометрия (дата обращения 03.04.2024)

2. Степенко В.Е., Богдановская А.Д. Биометрические персональные данные // Евразийский Союз Учёных. 2020. № 4-10 (73). С. 15-19.

3. Комеков Э.А. Системы аутентификации // Вестник науки и образования. 2022. № 11 (131). С. 21-25.

4. Биометрическая идентификация [Электронный ресурс] – Режим доступа: http://www.sberbank.ru/ru/person/kibrary/vocabulary/ biometricheskaya_identifikaciya (дата обращения 09.04.2024)

5. Макарова Д. В., Докучаев В. А. Основные методы сбора и защиты биометрических персональных данных // REDS: Телекоммуникационные устройства и системы. 2019. Т. 9. № 1. С. 7-12.

6. Бурлака С.Н., Бельдина О.Г. Защита биометрических персональных данных: проблемы правового регулирования // Право и государство: теория и практика. 2023. № 10(226). С. 277-279.