

Мусалимов Марис Наилевич,
курсант 223 учебной группы, 2 факультета,
Филиал ВУНЦ ВВС «ВВА» в г. Челябинск

Попов Юрий Леонидович,
Доцент, кандидат исторических наук,
профессор академии военных наук,
Филиал ВУНЦ ВВС «ВВА» в г. Челябинск

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ: ПРЕИМУЩЕСТВА И РИСКИ

Аннотация: Статья посвящена анализу современных методов биометрической аутентификации, их преимуществам и потенциальным рискам. В работе рассматриваются основные типы биометрических технологий и их эффективность, а также угрозы, связанные с возможностью утечки и подделки биометрических данных. Особое внимание уделяется перспективам развития технологий в контексте обеспечения надежной аутентификации.

Ключевые слова: аутентификация, биометрические технологии, биометрические данные, защита информации, личная информация.

В современном мире биометрические технологии становятся все более распространенными и востребованными, обеспечивая быстрый и удобный доступ к различным сервисам и ресурсам. Биометрическая аутентификация использует уникальные физиологические и поведенческие характеристики человека, такие как отпечатки пальцев, распознавание лиц и голоса, что делает ее привлекательной альтернативой традиционным паролям и кодам. Однако внедрение таких систем вызывает вопросы относительно их надежности, конфиденциальности и безопасности. В данной статье рассматриваются основные преимущества и риски, связанные с использованием биометрической аутентификации, а также влияние на безопасность и приватность пользователей.

Современные методы биометрической аутентификации включают разнообразные технологии, обеспечивающие высокую точность и безопасность подтверждения личности пользователя. Ниже представлены основные современные методы:

1. Отпечатки пальцев: один из наиболее распространенных методов, использующий уникальные детали узоров на пальцах. Современные системы используют сканеры с высоким разрешением и технологии антифальсификации.

2. Распознавание лица: анализирует особенности лица, такие как расстояние между глазами, форма скул, рельеф и другие параметрики. Современные системы используют нейронные сети и 3D-сканирование для повышения точности.

3. Распознавание радужной оболочки глаза: высокоточный метод, использующий уникальные узоры радужной оболочки. Обеспечивает очень высокий уровень безопасности, применяется в специальных сферах.

4. Распознавание голоса: определение личности по голосовым характеристикам, таким как тон, тембр, ритм. Применяется в телефонных приложениях и системах дистанционной идентификации.

5. Биометрия по руке и ладони: анализ формы, размера и структуры кисти и пальцев.

6. Динамическое распознавание поведения: анализирует индивидуальные модели поведения пользователя, такие как нажатия клавиш, использование мыши и другие параметры взаимодействия с устройством [2].



Современные биометрические технологии демонстрируют значительную эффективность благодаря развитию методов идентификации и аутентификации, основанных на уникальных физиологических и поведенческих признаках человека. Вот ключевые аспекты их эффективности:

1. Высокий уровень точности: использование таких технологий, как распознавание лиц, отпечатков пальцев, радужной оболочки глаза и голосовых характеристик позволяет достигать высокой точности распознавания, минимизируя ложные срабатывания и ошибки.

2. Быстрота и удобство: биометрические системы обеспечивают быстрый процесс идентификации, что особенно важно в ситуациях, требующих мгновенного доступа к информации или ресурсам. Они удобны для пользователей, так как исключают необходимость запоминания паролей или носителей.

3. Повышенная безопасность: биометрические данные трудно подделать или украсть по сравнению с традиционными паролями или PIN-кодами, что повышает уровень защиты системы от несанкционированного доступа.

4. Универсальность и интеграция: современные технологии легко интегрируются в различные сферы – банки, аэропорты, системы контроля доступа, мобильные устройства, а также в системы видеонаблюдения и аутентификации пользователей.

5. Обеспечение краткосрочной и долгосрочной аутентификации: биометрические системы могут использоваться для краткосрочной (например, вход в здание) и долгосрочной (например, удостоверения личности) аутентификации.

Однако, несмотря на высокую эффективность, существуют и задачи, связанные с защитой персональных данных, возможностью ошибок в распознавании при изменениях внешнего вида или условий окружающей среды, а также необходимость разработки стандартов и управления безопасностью данных [1].

Угрозы, связанные с возможностью утечки и подделки биометрических данных, представляют серьезную опасность для приватности и безопасности личности. Основными видами таких угроз являются:

1. Утечка биометрической информации:

- кража данных при взломе систем хранения биометрических данных (например, базы данных отпечатков пальцев, лицевых изображений, сетчатки глаза).
- неавторизованный доступ к личным данным через уязвимости в системах хранения или передачи информации.

2. Подделка биометрических данных:

- использование отпечатков пальцев, голосов, изображений лица или другого биометрического признака, созданных мошенником (например, с помощью 3D-или 2D-отпечатков, масок, поддельных голосов).
- внедрение поддельных биометрических образцов для обхода систем аутентификации.

3. Маскировка:

- создание копий биометрических данных другого человека для получения доступа или совершения преступных действий.

4. Социальная инженерия и «фишинг»:

- использование украденных или полученных незаконным путем биометрических данных для обхода систем безопасности.

5. Последствия утечки и подделки:

- потеря конфиденциальности и риска фишинга или мошенничества.
- необратимость биометрических данных: в отличие от паролей, их невозможно изменить, что повышает риск долговременной угрозы при утечке.



Перспективы развития биометрических технологий выглядят весьма многообещающими и обусловлены рядом ключевых факторов и тенденций:

1. Увеличение точности и надежности: современные алгоритмы машинного обучения и обработки изображений позволяют значительно повысить точность распознавания биометрических признаков, что снижает риск ошибок и увеличивает безопасность систем.

2. Расширение областей применения: биометрические технологии находят применение не только в системах безопасности и идентификации (например, биометрический контроль доступа, платежи, паспортные системы), но и в сфере здравоохранения (например, аутентификация пациентов), маркетинга, умных устройств и интернета вещей.

3. Внедрение в мобильные устройства. – Смартфоны и носимые гаджеты активно используют биометрические методы аутентификации (отпечатки пальцев, распознавание лиц, радужной оболочки глаза), что стимулирует развитие более компактных и эффективных решений.

4. Совершенствование инфраструктуры безопасности: биометрические системы интегрируются с многофакторной аутентификацией и криптографическими протоколами, обеспечивая высокий уровень защиты данных и систем.

5. Перспективы развития в области искусственного интеллекта (ИИ): использование ИИ позволяет создавать более сложные и устойчивые системы распознавания.

В целом, можно ожидать, что биометрические технологии будут становиться всё более точными, доступными и интегрированными в повседневную жизнь, способствуя повышению уровня комфорта, безопасности и эффективности в различных сферах [3].

В заключение, биометрическая аутентификация представляет собой современное решение для повышения уровня безопасности и удобства в использовании различных систем. Ее преимущества включают быстрый доступ, сложность подделки и высокую точность идентификации. Однако вместе с тем существуют и существенные риски, связанные с возможностью утечки биометрических данных, их необратимость и угрозами конфиденциальности. Поэтому при внедрении биометрических технологий необходимо тщательно учитывать баланс между безопасностью и защитой прав пользователей, разрабатывать надежные меры защиты и регламентировать использование биометрических данных. Только при ответственном подходе биометрическая аутентификация сможет полностью раскрыть свой потенциал и стать надежным инструментом в современной цифровой среде.

Список литературы:

1. Лебедев, А. С. Информационные технологии и безопасность. – М.: Техническая безопасность, 2020. – 40 с.
2. Кузнецов Д. А. Биометрические системы и средства идентификации. – М.: Защита персональных данных, 2018. – С. 90-103.
3. Терешков И. С. Теория и практика биометрических систем. – М.: Защита информации, 2020. – 56 с.

