Реферат

Биометрия

Ильин Андрей Владимирович

Содержание

1 Введение

В современном цифровом мире безопасность данных и контроля доступа к информации становятся все более актуальными задачами. Информационная безопасность является неотъемлемой частью деятельности организаций и государств. Для решения этих задач используется ряд технологий, включая биометрию - область науки и технологии, связанную с использованием уникальных физиологических и поведенческих характеристик человека для идентификации. В данном реферате мы рассмотрим основные аспекты биометрии и ее роль в обеспечении информационной безопасности.

2 Основы биометрии

Основная идея биометрии заключается в том, что каждый человек обладает уникальными физиологическими и поведенческими чертами, которые могут быть использованы для определения личности. Физиологические биометрические характеристики включают в себя отпечатки пальцев, сканирование сетчатки глаза, сканирование лица и другие. Поведенческие биометрические характеристики включают в себя голос, почерк, образцы набора текста и другие параметры.

2.1 Виды биометрии

Биометрия делится на два основных типа: физиологическая и поведенческая.

- Физиологическая биометрия основана на уникальных физических характеристиках человека. К таким характеристикам относятся отпечатки пальцев, сканирование лица, сканирование сетчатки глаза, геометрия руки и многие другие. Физиологическая биометрия широко применяется в системах контроля доступа, банковских учреждениях и других организациях для аутентификации пользователей.
- Поведенческая биометрия основана на характеристиках поведения человека. К ним относятся голос, почерк, образцы набора текста и даже ходьба. Эти характеристики, в отличие от физиологических, могут меняться в зависимости от состояния человека, но они могут добавить дополнительный уровень безопасности при аутентификации.

3 Применение биометрии в обеспечении информационной безопасности

Биометрия играет важную роль в обеспечении информационной безопасности и применяется в различных сферах.

1. Аутентификация: Одним из основных применений биометрии является аутентификация пользователей. Пароли и PIN-коды могут быть украдены или подделаны, в то время как биометрические характеристики трудно подделать. Это обеспечивает более надежный способ определения личности.

2. Контроль доступа: Биометрические системы широко используются для физического и логического контроля доступа. Они могут быть применены в организациях, аэропортах, банках и других местах, где важно обеспечить безопасность.

3. Биометрические платежи: Биометрия применяется в финансовых операциях, таких как мобильные платежи и биометрические кредитные карты. Это усиливает безопасность финансовых транзакций.

4. Государственные идентификационные документы: Многие страны внедряют биометрические технологии в паспорты, водительские удостоверения и другие идентификационные документы. Это помогает бороться с подделками и обеспечивать безопасность национальных границ.

5. Медицинская идентификация: В медицинских учреждениях биометрия применяется для идентификации пациентов. Это позволяет избежать ошибок в лечении и обеспечить безопасность пациентов.

4 Плюсы и минусы биометрии

4.1 Преимущества

Использование биометрии обладает несколькими важными преимуществами:

1. Уникальность: Каждый человек имеет уникальные биометрические характеристики, что делает их надежными для идентификации.
2. Удобство: Биометрические системы более удобны для пользователей, чем пароли и PIN-коды. Пользователи не должны запоминать сложные пароли и могут легко проходить аутентификацию.
3. Невозможность утери: В отличие от паролей и ключей, биометрические характеристики невозможно утерять или забыть.

4.2 Риски и ограничения

Однако, несмотря на множество преимуществ, биометрия также сопряжена с рисками и ограничениями:

1. Несанкционированный доступ: Возможно подделывание биометрических данных. Кража отпечатков пальцев или подслушивание голоса могут использоваться для несанкционированного доступа.

2. Защита данных: Хранение и обработка биометрических данных требуют высоких стандартов безопасности. Утечки биометрических данных могут иметь серьезные последствия.

3. Приватность: Сбор и использование биометрических данных вызывают вопросы приватности. Люди могут быть озабочены тем, как их данные будут использованы и хранены.

4. Временная нестабильность: Некоторые биометрические характеристики, такие как голос, могут изменяться со временем из-за физических или психологических изменений.

5 Будущее биометрии

Биометрия продолжает развиваться и находить новые области применения. В будущем мы можем ожидать следующих изменений:

1. Улучшение технологий: Технологии биометрии будут развиваться и становиться более точными и надежными.
2. Расширение области применения: Биометрия будет активно внедряться в мобильные устройства, облачные вычисления и интернет вещей.
3. Использование в медицине: Биометрия будет активно применяться для медицинской идентификации пациентов и мониторинга их состояния.

5.1 Новые технологии и развитие биометрии

1. Генетическая биометрия: Одним из перспективных направлений развития биометрии является использование генетической информации для идентификации. Геном человека уникален, и технологии секвенирования ДНК могут стать мощным инструментом в борьбе с мошенничеством и обеспечении безопасности.
2. Биометрия в интернете вещей: С развитием интернета вещей (IoT) возникает потребность в надежных методах аутентификации устройств. Биометрия может быть встроена в умные устройства, такие как смарт-двери или смарт-автомобили, для обеспечения безопасности.

3. Эмоциональная биометрия: Изучение человеческих эмоций через анализ голоса, выражений лица и других параметров становится актуальным. Эмоциональная биометрия может использоваться в медицинских приложениях и в области клиентского обслуживания.

5.2 Этические и правовые аспекты

С развитием биометрии возникают серьезные вопросы о приватности и правах человека. Сбор и хранение биометрических данных требуют строгих правовых норм и нормативных актов, чтобы защитить интересы граждан. Органы власти и организации должны разработать стратегии для обеспечения соблюдения приватности и этики.

6 Биометрия и информационная безопасность

1. Многофакторная аутентификация: Биометрия эффективно используется в системах многофакторной аутентификации. Вместе с другими методами, такими как пароли или токены, биометрия повышает безопасность. Это особенно важно в корпоративной среде, где защита данных является приоритетом.

2. Борьба с киберугрозами: Киберугрозы становятся все более изощренными, и биометрия может помочь в предотвращении несанкционированного доступа. Технологии, такие как сканирование лица и сканирование сетчатки глаза, не позволяют злоумышленникам проникнуть в систему с использованием украденных паролей.

3. Приложения для мобильных устройств: Биометрические методы аутентификации, такие как сканер отпечатков пальцев или распознавание лица, активно используются в смартфонах и планшетах. Это обеспечивает безопасный доступ к данным и приложениям, хранящимся на устройствах.

4. Государственная безопасность: Во многих странах биометрия используется для обеспечения национальной безопасности. Это включает в себя идентификацию национальных документов, контроль доступа на границах и борьбу с преступностью.

7 Заключение

Биометрия играет ключевую роль в обеспечении информационной безопасности. Её использование позволяет надежно идентифицировать личность и обеспечить контроль доступа к данным и ресурсам. Однако, необходимо учитывать риски и соблюдать высокие стандарты безопасности и приватности. С развитием технологий и новых направлений исследований биометрии, она будет продолжать оставаться важным инструментом в обеспечении информационной безопасности и защите данных в будущем.

Список литературы

1. БИОМЕТРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [Электронный ресурс]. ВГУ. URL: https://cyberleninka.ru/article/n/biometriya-v-informatsionnoy-bezopasnosti.
2. Биометрическая аутентификация [Электронный ресурс]. URL: https://rt-solar.ru/events/blog/3616/.
3. Проблемы и угрозы биометрической идентификации [Электронный ресурс]. URL: https://habr.com/ru/companies/trendmicro/articles/469533/.
4. Аутентификация [Электронный ресурс]. URL: https://cisoclub.ru/autentifikacija/.
5. Нейросетевые технологии биометрической аутентификации пользователей открытых систем [Электронный ресурс]. URL: https://www.dissercat.com/content/neirosetev tekhnologii-biometricheskoi-autentifikatsii-polzovatelei-otkrytykh-sistem.
6. ИСПОЛЬЗОВАНИЕ БИОМЕТРИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ [Электронный ресурс]. URL: https://web.snauka.ru/issues/2023/09/100808.