УДК 004.42

Автор: Уматгериева Хадижат Рамзановна

Преподаватель

ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова»

Россия, г. Грозный

***Соавтор:* Хасбулатов Тамерлан Рустамович**

Магистрант, 2 курс, группа ЗБИН-22М

ФГБОУ ВО «Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова»

Россия, г. Грозный

РАЗРАБОТКА И ИССЛЕДОВАНИЕ БИОМЕТРИЧЕСКИХ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация.

В статье раскрываются методы, цели создания и применения биометрических технологий. Выделяются основные группы биометрических методов, и производится сравнительный анализ методов, входящих в данные группы. На основе проведенного сравнительного анализа выбирается оптимальный метод. Рассматриваются основные области применения, биометрической идентификации. Описывается принципиальная схема биометрической системы, и производится обзор ключевых компонентов, входящих в биометрическую систему.

Приводятся примеры построения структурной и функциональной схемы, для конкретной области применения.

Ключевые слова: биометрическая идентификация, биометрическая система, биометрические методы, биометрические технологии, идентификация личности, области применения отпечатков пальцев, отпечатки пальцев, СКУД.

Структурная схема биометрической системы, функциональная схема биометрической системы.

Author: Umatgerieva Khadizhat Ramzanovna

Teacher

Grozny State Petroleum Technical University named after academician M.D. Millionshchikova"

Russia, Grozny

Co-author: Khasbulatov Tamerlan Rustamovich

Undergraduate, 2nd year, ZBIN-22M group

Grozny State Petroleum Technical University named after academician M.D. Millionshchikova"

Russia, Grozny

DEVELOPMENT AND RESEARCH OF BIOMETRIC METHODS AND INFORMATION SECURITY TOOLS

Annotation.

The article reveals the methods and goals of the creation and application of biometric technologies. The main groups of biometric methods are distinguished, and a comparative analysis of the methods included in these groups is carried out. Based on the comparative analysis, the optimal method is selected. The main areas of application of biometric identification are considered. A schematic diagram of the biometric system is described, and an overview of the key components included in the biometric system is provided.

Examples of building a structural and functional scheme for a specific application are given.

Keywords: biometric identification, biometric system, biometric methods, biometric technologies, identity identification, fingerprint applications, fingerprints, ACS.

Разработка и исследование биометрических методов и средств защиты информации — это важная область, которая постоянно развивается.

Вот несколько ключевых направлений в этой области:

Улучшение алгоритмов распознавания: Исследования направлены на повышение точности и скорости биометрических систем, а также на уменьшение количества ложных срабатываний и пропусков.

Междисциплинарные исследования: Сочетание знаний из различных областей, таких как криптография, машинное обучение и биоинженерия, для создания комплексных решений.

Защита от подделки и мошенничества: Разработка методов, способных обнаруживать попытки подделки биометрических данных, таких как фальшивые отпечатки пальцев или манипулированные изображения лица.

Биометрия на основе поведения: Исследование новых типов биометрических данных, основанных на поведенческих характеристиках, таких как паттерны набора текста или динамика движения.

Интеграция с другими технологиями: Внедрение биометрических систем в широкий спектр приложений, от мобильных устройств до систем контроля доступа.[1]

Эти направления исследований и разработок способствуют созданию более безопасных и эффективных биометрических систем, которые могут найти применение в самых разных сферах, от личной безопасности до национальной обороны.

Основным достоинством биометрии является самостоятельная идентификация человека. На сегодняшний день очевидна необходимость безошибочной идентификации в местах высокой проходимости людей, на контрольно-пропускных пунктах. Остро эта проблема стоит в соблюдении безопасности на транспорте и в местах проведения спортивных и культурно-массовых мероприятий. Нельзя отрицать наличие проблем (сложностей) безопасности в государственных и межгосударственных системах, таких как паспортная, визовая, таможенная, миграционная службы. Уже известных и

[1]Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Из-во Пензенского государственного университета, 2020. – 188 с.
Иванов А.И. Компьютер Вас узнает / А.И. Иванов, И.А. Сорокин, С.Н. Шумкин // Безопас ность, достоверность, информация (БДИ). – № 1. – 996. – С. 18-21.

давно используемых методов контроля явно недостаточно. Прорывом в вопросе системы безопасности является повсеместное использование биометрических технологий.

Биометрическая идентификация — это процесс установления уникальности личности на основе одного или нескольких физиологических или поведенческих признаков. Вот основные элементы, которые могут быть включены в структурную и функциональную схему биометрической системы:

Структурная схема биометрической системы:

Датчик: Устройство для захвата биометрических данных (например, сканер отпечатков пальцев).

Преобразователь сигналов: Преобразует захваченные данные в цифровую форму.

Модуль хранения: База данных для сохранения биометрических шаблонов.

Модуль сравнения: Сравнивает представленные данные с хранящимися шаблонами.

Интерфейс пользователя: Система взаимодействия с пользователем для подтверждения идентификации.[2]

Функциональная схема биометрической системы:

Захват: Сбор биометрических данных с помощью датчика.

Обработка: Преобразование и оптимизация данных для сравнения.

Хранение: Сохранение биометрических шаблонов в базе данных.

Сравнение: Автоматическое сопоставление представленных данных с шаблонами.

Решение: Определение, соответствует ли представленный образец сохраненному шаблону.

Области применения биометрических технологий:

[2]Барсунов В.С. Биометрическая защита информации // Защита информации. Конфидент.-2020. – № 1. – С. 45-52. Тельных А. Идентификация личности. Как это делается / А. Тельных, А. Коган. // Компь ютерра. – 2021 – №10. – С. 39-41.«Наука и образование: новое время» № 2, 2022

Системы контроля доступа (СКУД): Используют отпечатки пальцев или другие биометрические данные для предоставления доступа к защищенным объектам.

Банковские операции: Биометрическая аутентификация для подтверждения транзакций и доступа к банковским услугам.

Мобильные устройства: Распознавание отпечатков пальцев или лица для разблокировки телефонов и подтверждения покупок.

В последние годы в области биометрии наблюдаются следующие тенденции и направления исследований:

Мультифакторная аутентификация: Интеграция нескольких биометрических методов для повышения безопасности и точности идентификации.

Современные технологии защиты биометрических данных включают использование шифрования и биометрического шаблонирования. Это помогает обезопасить данные на случай их утечки. Также разрабатываются методы, которые позволяют проводить аутентификацию без хранения самих биометрических данных, например, с помощью одноразовых биометрических шаблонов.

Последние достижения в области мультифакторной аутентификации:

Мультифакторная аутентификация (MFA) становится всё более сложной и надёжной. Одним из новых подходов является адаптивная MFA, которая анализирует контекст доступа пользователя и требует дополнительных факторов аутентификации в случае обнаружения необычной активности.

Биометрические платежные системы: Внедрение биометрических данных для упрощения и безопасности платежных операций.

Искусственный интеллект и машинное обучение: Применение AI и машинного обучения для улучшения алгоритмов распознавания и снижения ложных срабатываний.

Конфиденциальность и защита данных: Усиление мер по защите биометрических данных от несанкционированного доступа и злоупотреблений.

Эти направления отражают стремление к созданию более надежных, удобных и безопасных систем идентификации.

Конфиденциальность и защита данных являются ключевыми аспектами в области биометрической идентификации. Вот несколько направлений, которые способствуют усилению защиты биометрических данных:

Биометрическое шифрование: Использование шифрования для защиты биометрических данных на всех этапах их обработки и хранения.

Анонимизация биометрических данных: Применение техник, которые позволяют использовать биометрические данные без раскрытия личности.

Блокчейн для биометрических данных: Использование блокчейн-технологий для создания децентрализованной и надежной системы хранения биометрических данных.

Одноразовые биометрические шаблоны: Разработка систем, которые не требуют постоянного хранения биометрических данных, а используют временные или одноразовые шаблоны.[3]

Многофакторная аутентификация: Комбинирование биометрических данных с другими факторами аутентификации, такими как пароли или электронные ключи.

Эти меры направлены на минимизацию рисков несанкционированного доступа и злоупотреблений, обеспечивая при этом удобство и эффективность биометрических систем идентификации.

Многофакторная аутентификация (MFA) играет ключевую роль в обеспечении безопасности информационных систем. Комбинирование биометрических данных с другими факторами, такими как пароли, PIN-коды, электронные ключи или одноразовые парольные коды (OTP), значительно

[3]Уиллес Д. Шесть биометрических устройств идентификации отпечатков пальцев. / Д. Уиллес, М. Ли. // Сети и системы связи. – 2020. – №9(31). – СЛ46-155.
Филлипс П. Дж. Введение в оценку биометрических систем / П. Дж. Филлипс, Э. Мартин, С.Л. Пржибоски // Открытые системы. – 2021. – №3. – С. 21-27.

повышает уровень защиты от несанкционированного доступа. Вот несколько преимуществ MFA:

Усиленная безопасность: Использование нескольких независимых каналов аутентификации затрудняет злоумышленникам получение контроля над аккаунтом.

Гибкость и масштабируемость: Системы MFA могут быть настроены с различными уровнями сложности в зависимости от требований безопасности конкретной организации.

Снижение рисков: Даже если один из факторов аутентификации скомпрометирован, наличие дополнительных слоев защиты помогает предотвратить несанкционированный доступ.

Удобство пользователя: Современные решения MFA стремятся минимизировать неудобства для пользователей, например, через использование биометрических данных, которые не требуют запоминания сложных паролей.

Тем не менее, при внедрении MFA важно учитывать баланс между безопасностью и удобством использования, чтобы не создавать излишние трудности для пользователей. Кроме того, необходимо обеспечить защиту биометрических и других чувствительных данных, используемых в процессе аутентификации.

Сегодня мы видим, что текущее развитие биометрических технологий на основе современных технических средств привело к тому, что практически каждый человек так или иначе соприкоснулся с биометрией, например при доступе к смартфону с помощью изображения лица или отпечатка пальца.

Эти выводы подчеркивают значимость биометрических систем в обеспечении безопасности и управлении доступом, а также их потенциал для дальнейшего развития и интеграции в различные сферы жизни.

Использованные источники:

1. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: Из-во Пензенского государственного университета, 2020. – 188 с.
2. Иванов А.И. Компьютер Вас узнает / А.И. Иванов, И.А. Сорокин, С.Н. Шумкин // Безопасность, достоверность, информация (БДИ). – № 1. – 996. – С. 18-21.
3. Барсунов В.С. Биометрическая защита информации // Защита информации. Конфидент.-2020. – № 1. – С. 45-52.
4. Тельных А. Идентификация личности. Как это делается / А. Тельных, А. Коган. // Компьютерра. – 2021 – №10. – С. 39-41.«Наука и образование: новое время» № 2, 2022
5. Уиллес Д. Шесть биометрических устройств идентификации отпечатков пальцев. / Д. Уиллес, М. Ли. // Сети и системы связи. – 2020. – №9(31). – СЛ46-155.
6. Филлипс П. Дж. Введение в оценку биометрических систем / П. Дж. Филлипс, Э. Мартин, С.Л. Пржибоски // Открытые системы. – 2021. – №3. – С. 21-27.