СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ (БИОМЕТРИЯ ОТПЕЧАТКА ЛАДОНИ И ГОЛОСОВАЯ АУТЕНТИФИКАЦИЯ)

Студент группы 10306121 Волков И. В.

Научный руководитель – преподаватель-стажер Богданова Е. А.

Белорусский Национальный Технический Университет

Минск, Беларусь

Введение

Определение системы контроля и управления доступом

Система контроля и управления доступом (СКУД) представляет собой комплекс технических и программных средств, предназначенных для организации контроля и регулирования доступа персонала или посетителей на охраняемые объекты или в определенные зоны. Она включает в себя методы аутентификации, контроль прохода через двери, ворота, турникеты и другие точки доступа, а также системы мониторинга и учета.

Значение безопасности и защиты информации

Безопасность и защита информации стали ключевыми аспектами в современном мире, особенно в контексте роста цифровизации и увеличения объема конфиденциальных данных. Системы контроля и управления доступом играют важную роль в обеспечении безопасности, защите конфиденциальной информации, предотвращении несанкционированного доступа и контроле перемещения людей в охраняемых зонах.

Биометрические методы аутентификации

1.1.Сканирование отпечатка ладони

1.1.1. Уникальные особенности ладони

Каждая ладонь имеет уникальные особенности, такие как рисунок линий, папиллярных узоров и точек, которые отличаются у каждого человека. Эти

уникальные характеристики делают отпечаток ладони надежным биометрическим идентификатором.

1.1.2. Принцип работы системы сканирования

Система сканирования отпечатка ладони использует оптические или капаситивные методы для получения изображения ладони. Оптический сканер использует видимый или инфракрасный свет для создания изображения, в то время как капаситивный сканер измеряет электрические свойства кожи. Полученное изображение ладони затем обрабатывается и сравнивается с заранее сохраненными шаблонами для аутентификации.

1.1.3. Преимущества и ограничения сканирования отпечатка ладони

Преимущества сканирования отпечатка ладони включают:

1. Высокую точность и надежность: Отпечатки ладони сложно подделать или скопировать, что делает этот метод аутентификации надежным.

2. Удобство использования: Пользователю необходимо просто поместить ладонь на сканер, что делает этот метод удобным в повседневном использовании.

3. Малая площадь сканирования: Для сканирования отпечатка ладони требуется меньшая площадь, чем для сканирования отпечатка пальца, что позволяет использовать компактные устройства.

Ограничения сканирования отпечатка ладони включают:

1. Возможность изменения отпечатка: Некоторые факторы, такие как повреждения кожи или старение, могут изменить отпечаток ладони и повлиять на процесс идентификации.

2. Дороговизна: Установка и поддержка систем сканирования отпечатка ладони могут быть дорогостоящими, особенно для больших организаций.

3. Чувствительность к грязи и влаге: Системы сканирования отпечатка ладони могут быть чувствительными к грязи, маслу или влаге, что может повлиять на качество сканирования.

1.2. Голосовая аутентификация

1.2.1. Уникальные характеристики голоса

Голос каждого человека имеет уникальные характеристики, такие как тон, частота, ритм, интонация и длительность звуков. Эти уникальные характеристики делают голосовую аутентификацию эффективным методом биометрической идентификации.

1.2.2. Принцип работы системы голосовой аутентификации

Система голосовой аутентификации записывает голосовой образец пользователя и анализирует его особенности. Это может включать измерение частоты голоса, спектрального содержания, ритма речи и других акустических параметров. Полученные данные сравниваются с заранее сохраненными шаблонами голоса для аутентификации.

1.2.3. Преимущества и ограничения голосовой аутентификации

Преимущества голосовой аутентификации включают:

1. Удобство использования: Пользователю необходимо только произнести определенную фразу или предоставить голосовой образец, что делает этот метод удобным в повседневной жизни.

2. Бесконтактность: Голосовая аутентификация не требует физического контакта с устройством, что является удобным и гигиеничным.

3. Высокая точность: Голосовая аутентификация обладает высокой точностью и надежностью, особенно при использовании современных алгоритмов и технологий.

Ограничения голосовой аутентификации включают:

1. Влияние физиологических факторов: Физиологические факторы, такие как простуда, изменение тона голоса или голосовые нарушения, могут повлиять на точность аутентификации.

2. с: в некоторых случаях, голос пользователя может быть записан и воспроизведен злоумышленником для обхода системы аутентификации.

3. Окружающий шум: Шум в окружающей среде может повлиять на качество записи и анализ голосового образца, что может снизить точность аутентификации.

Преимущества и недостатки системы контроля и управления доступом с использованием биометрических методов аутентификации

Преимущества системы контроля и управления доступом с использованием биометрических методов аутентификации:

1. Высокая точность и надежность идентификации: Биометрические методы аутентификации, такие как сканирование отпечатка ладони или голосовая аутентификация, обладают высокой точностью и надежностью при идентификации пользователей. Это значительно снижает возможность несанкционированного доступа к защищенным областям или информации.

2. Удобство использования для пользователей: Биометрические методы аутентификации обычно удобны в использовании для пользователей. Вместо необходимости запоминать пароли или носить с собой идентификационные карты, пользователи могут просто использовать свои биометрические характеристики для аутентификации, что упрощает процесс и повышает удобство.

3. Сложность подделки или украдения биометрических характеристик: Биометрические характеристики, такие как отпечаток ладони или голос, сложно подделать или украсть. Это делает системы контроля и управления доступом с использованием биометрических методов более надежными и защищенными от мошенничества.

Недостатки системы контроля и управления доступом с использованием биометрических методов аутентификации:

1. Высокие затраты на установку и поддержку системы: Внедрение и поддержка системы контроля и управления доступом с использованием биометрических методов может быть затратным. Это связано с приобретением специализированного оборудования, разработкой программного обеспечения, обучением персонала и обновлением системы по мере необходимости.

2. Возможность ложных срабатываний или отказа системы: Несмотря на высокую точность и надежность биометрических методов аутентификации, возможны ложные срабатывания или отказы системы. Например, система

может неправильно идентифицировать пользователя из-за изменения его биометрических характеристик (например, из-за повреждения отпечатка ладони или изменения тона голоса). Это может привести к неудобству для пользователей или потенциальным проблемам безопасности.

3. Защита биометрических данных от несанкционированного доступа: Биометрические данные, такие как отпечатки ладони или голосовые образцы, являются конфиденциальной информацией и должны быть защищены от несанкционированного доступа. Системы контроля и управления доступом должны обеспечивать надежную защиту этих данных, что может требовать дополнительных мер безопасности, таких как шифрование и строгий контроль доступа к хранилищам биометрических данных.

Все эти факторы должны быть учтены при выборе и внедрении системы контроля и управления доступом с использованием биометрических методов аутентификации. Необходимо балансировать между удобством использования, надежностью, безопасностью и затратами для достижения оптимального решения.

Применение системы контроля и управления доступом с использованием биометрических методов аутентификации

Банки и финансовые учреждения: Биометрические методы аутентификации могут быть использованы для обеспечения безопасного доступа к банковским счетам и финансовым данным клиентов. Например, сканирование отпечатка пальца или распознавание лица может быть использовано для идентификации клиента при входе в банк или проведении финансовых операций.

Корпоративные офисы и предприятия: Биометрические системы контроля доступа могут быть использованы для ограничения доступа к конфиденциальным помещениям в офисах и предприятиях. Это может включать сканирование отпечатка ладони, распознавание лица или голосовую

аутентификацию для идентификации сотрудников и контроля их доступа к определенным зонам или информации.

Государственные учреждения и организации: Биометрические методы аутентификации могут быть применены в государственных учреждениях и организациях для обеспечения безопасности и контроля доступа. Например, системы сканирования отпечатка пальца или распознавания лица могут использоваться для идентификации сотрудников и контроля доступа к защищенным зонам или базам данных.

Транспортные узлы и аэропорты: Биометрические методы аутентификации могут быть применены на транспортных узлах, таких как железнодорожные станции, автобусные вокзалы и аэропорты, для контроля доступа и обеспечения безопасности. Например, системы сканирования отпечатка пальца или распознавания лица могут использоваться для идентификации пассажиров и контроля доступа к платформам или безопасным зонам.

Умные дома и автомобили: Биометрические методы аутентификации могут быть применены в умных домах и автомобилях для обеспечения безопасности и персонализированного доступа. Например, сканирование отпечатка пальца или распознавание лица может использоваться для разблокировки дверей умного дома или запуска автомобиля только для авторизованных пользователей.

Это лишь несколько примеров применения систем контроля и управления доступом с использованием биометрических методов аутентификации. В целом, такие системы могут быть полезны в любой области, где требуется высокий уровень безопасности и контроля доступа к защищенным зонам или информации.

6 лучших биометрические скуд на 2023 год

Hikvision

Компания входит в число ведущих поставщиков систем безопасности, на рынке присутствует более 20 лет. Головной офис расположен в Китае.

СКУД Hikvision имеет привычную конфигурацию устройств, контроллер базового блока — локальный, то есть все данные хранятся непосредственно на устройствах. Но при необходимости контроллер можно использовать и в рамках сетевой СКУД.

Линейка оборудования включает все необходимое для построения полноценный системы контроля доступа. Поэтому можно подобрать комплектацию и ПО для объекта любого уровня сложности. Для этого на текущий момент компанией предлагается два варианта контроллеров, простой (DS-K2800) и профессиональный (DS-K2600).

Считыватели способны работать с картами, отпечатками пальцев, есть также возможность работы с набором PIN-а на клавиатуре. Терминалы доступа от Hikvision оснащены также функционалом детекции лица, его распознавания и сохранения снимка.

Так, например терминал распознавания лиц DS-K1T331W способен произвести распознавание на расстоянии от 0,3 до 1,5 м, демонстрируя при этом высокую точность идентификации (более 99%) и скорость — 0,2 сек. Есть модели терминалов, которые способны распознать входящего на расстоянии до 3 метров от устройства. Пример такого терминала — модель DS-K1T672.

Достоинства:

- Возможность комплексной интеграции с системами видеонаблюдения и домофонии на базе единого ПО;
- Предусмотрена интеграция с модулями управления лифтов;
- Простота настройки;
- Большой выбор считывателей;
- Стильный дизайн считывающих устройств;
- Наличие пожарного реле для разблокировки дверей при пожаре.

Недостатки:

- Несовершенная русская речь при озвучке ботов;
- Невозможность подключения стороннего оборудования

ZKTeco

Еще один китайский бренд, который, в первую очередь, специализируется на создании оборудования для биометрических СКУД, однако возможность идентификации по RFID карте или PIN также предусмотрена. Платформа для СКУД от ZKTeco — Windows, есть также оборудование, работающее на ОС Linux.

Контроль доступа предполагает не просто запрещение/разрешение входа, но и возможность контролировать дальнейшее передвижение конкретного объекта. СКУД позволяет отследить до 30 тыс. событий.

Заслуживают, например, внимания терминалы данного бренда, которые способны распознать лицо на расстоянии до 3 метров от считывателя, что делает их эффективными в ситуациях и местах с быстро движущимся людским потоком. Отдельные модели способны осуществлять распознавание под углом до 30 градусов (SpeedFace-V5) в то время, как большинство приборов осуществляют идентификацию под углом не более 15 градусов.

В условиях сложной эпидемиологической ситуации становятся актуальны биометрические терминалы с распознаванием лиц, оснащенные тепловизорной камерой. Так модель RevFace10[TI] поможет в мониторинге и выявлении людей с вирусными заболеваниями, точно измерит температуру, а также определит наличие маски.

Используемый программный комплекс ZKBioTime позволяет вести учет рабочего времени, осуществлять контроль и управление посещениями. Полученные данные в автоматическом режиме заносятся в облачное хранилище ZKBioCloud.

Достоинства:

- Биометрия — основное направление бренда при создании СКУД, имеются патенты на технологии распознавания по лицу, ладоням и т.д.;
- Предусмотрена функция распознавания лица в потоке;

•Наличие удобного оборудования, например дистанционный сканер для снятия отпечатков пальцев сотрудников без необходимости идти к стационарному считывателю;

•Возможность настройки работы оборудования под конкретный объект.

Недостатки:

•Нельзя добавить оборудование другого производителя.

Dahua

Очередной производитель из Поднебесной, входит в число лидеров в мировом масштабе среди поставщиков в сере интеллектуальных систем видеонаблюдения. СКУД от Dahua — это полный набор для создания системы: контроллеры, считыватели, соответствующее ПО. СКУД поддерживает до 100 000 пользователей. Сканеры с функцией биометрического распознавания способны провести идентификацию объекта по лицу или отпечатку пальца. Есть оборудования и для считывания кода с пластиковых карт. Рассмотрим некоторые модели, заслуживающие внимания:

ASI3213G-MW — контроллер доступа с распознаванием лиц, способен распознать лицо на расстоянии от 0,3 до 1,5 метров от видеокамеры, при этом сумеет отличить настоящее лицо от его изображения, характеризуется низким уровне ложного распознавания, хорошей скоростью: 0,3 сек/лицо. Точность распознавания — 99,5%.

ASI8223Y-A-V3 — контроллер с большей дальностью распознавания, до 2 м, способен работать автономно и сохранять до 100 000 лиц, отличается высокой точностью распознавания (99,5%) и скоростью в 0,2 сек/лицо.

Компания предлагает собрать свою СКУД путем подбора подходящего оборудования, а также предлагает уже готовые решения для гостиничного бизнеса, розничной торговли, частного жилого сектора и других.

Контроллеры от бренда позволяют создать как автономную СКУД, так и сетевую. В последнем случае несколько контроллеров будут замыкаться на один основной.

Достоинства:

- Долговечное оборудование;
- Совместимость с техникой других производителей;
- Простота настройки;
- Возможность подбора оборудования под конкретный объект;
- Простота замены комплектующих.

Недостатки:

- Работает только с оборудованием Dahua.

Anviz

Биометрическая СКУД Anviz, страна бренда — США, — это интеграция системы контроля доступа и системы учета времени. Помимо решения проблемы контроля за передвижением сотрудников и посетителей, данное решение позволит строить удобные отчеты по сотруднику в частности или по компании в целом.

Биометрические сканеры бренда позволяют осуществлять идентификацию:

- посредством отпечатка пальца;
- По ID сотрудника и отпечатку пальца;
- по ID и набранному паролю;
- по прокси-карте;
- по ID и карте;
- по отпечатку пальца и карте.
- Есть также оборудование с возможностью FACE-идентификации.

Как и большинство СКУД данного обзора программный комплекс от Anviz может функционировать локально, а также в рамках сети, подключаясь к серверу посредством сети Etherent или же через Интернет.

Достоинства:

•Широкий выбор вариантов считывателя по типу идентификатора;

•Стильный дизайн оборудования;

•Возможность работы системы локально или в сети;

•Функциональный блок учета рабочего времени с возможностью контроля и отчетности;

•Среди оборудования имеются биометрические системы контроля температуры и наличия маски;

•Широкий функционал сопровождения.

Недостатки:

•Все сопровождение в основном платное.

Smartec

В линейке российского бренда представлены биометрические считыватели для систем контроля и управления доступа, позволяющие осуществлять идентификацию человека по отпечатку пальца, по рисунку вен на пальце или же по геометрии лица. Последний способ особенно привлекателен, так как является бесконтактным. Можно использовать и классический вариант контроля посредством карты или введения кода. Оборудование позволяет использовать каждый вариант идентификации отдельно или создавать комбинации (например, код+отпечаток пальца).

Есть возможность дополнить СКУД терминалами для учета рабочего времени.

Контроллер можно выбрать автономный или сетевой.

Операционная система — Windows

ПО «Таймекс», на котором строится работа системы, имеет модульную структуру. То есть предполагается наличие базового ядра, к которому подключаются необходимые модули. Например, модуль контроля доступа или учета рабочего времени, видеонаблюдения и т.д. Стоит отметить, что при отсутствии необходимости сложной настройки для реализации

интегрированной системы производитель предлагает бесплатную версию ПО Timex Free, что позволяет не совершать лишних трат.

Достоинства:

- Широкий ассортимент базового и дополнительного оборудования для СКУД;
- Модульность программного комплекса;
- Возможность сетевой и локальной работы;
- Наличие бесплатной версии ПО Timex Free;
- Лицензированная поддержка, рассчитанная на год, позволяет получать обновления до более высокой версии ПО без дополнительны трат;
- Гибкая система лицензирования.

Недостатки:

- Пользователями не отмечены.

Suprema

Южно-Корейский производитель выпускает устройства, позволяющие обеспечивать контроль и учет доступа посредством биометрических данных, карт RFID, введения кода или по смартфону.

Ассортимент оборудования для СКУД включает в себя сканеры и терминалы для распознавания, встраиваемые модули и ПО для управления идентификаторами, модулями контроля и учета. СКУД Suprema отличается гибкостью конфигурации, то есть возможностью настроить все под конкретный объект контроля, а также возможностью расширения базовой системы.

Достоинства:

- Есть решения для мобильной идентификации;
- Смартфон можно использовать и для контроля, удаленного администрирования;
- Широкий ассортимент оборудования для СКУД;

- Надежная схема распознавания;
- Привлекательный дизайн устройств;
- Эргономичность СКУД.

Недостатки:

- Финальная стоимость достаточно высокая.

Заключение

В заключение, системы контроля и управления доступом с использованием биометрических методов аутентификации представляют собой эффективный способ обеспечения безопасности и контроля доступа в различных сферах и организациях. Они обладают рядом преимуществ, таких как высокая точность и надежность идентификации, удобство использования для пользователей и сложность подделки или кражи биометрических характеристик.

Однако, следует учитывать и некоторые недостатки таких систем, включая высокие затраты на установку и поддержку, возможность ложных срабатываний или отказа системы, а также необходимость защиты биометрических данных от несанкционированного доступа.

При выборе и внедрении системы контроля и управления доступом с использованием биометрических методов аутентификации необходимо учесть все эти факторы и достичь баланса между удобством использования, надежностью, безопасностью и затратами. Каждая сфера применения, такая как банки и финансовые учреждения, корпоративные офисы и предприятия, государственные учреждения и организации, транспортные узлы и аэропорты, а также умные дома и автомобили, имеет свои особенности и требования, которые должны быть учтены при выборе соответствующей системы.

В целом, системы контроля и управления доступом с использованием биометрических методов аутентификации являются важным инструментом для обеспечения безопасности и контроля доступа в современном мире. Они помогают защитить конфиденциальную информацию, предотвратить

несанкционированный доступ и обеспечить удобство использования для пользователей. Однако, при их выборе и внедрении необходимо учитывать все преимущества и недостатки, а также особенности конкретной сферы применения.