Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:
https://stuservis.ru/kursovaya-rabota/416893

Тип работы: Курсовая работа

Предмет: Информатика (другое)

Введение 3
Глава 1. Теоретические основы системы контроля и управления доступом 5
1.1. Понятие систем контроля и управления доступом 5
1.2. История системы контроля и управления доступом 6
Глава 2. Обзор рынка СКУД 8
2.2 Обзор систем контроля доступа на российском рынке 14
2.2.1 СКУД от компании PERCo 14
2.2.2 СКУД от компании «Сфинкс» 19
2.3 Пример разработанной СКУД для университета 20
2.3.1 Техническое обеспечение 22
Заключение 23
Список использованных источников 25

Магнитные карты – это пластиковые карты, на которых нанесены магнитные полосы. Эти полосы содержат информацию, которая может быть считана специальным устройством, называемым магнитным считывателем.
Магнитные карты являются распространенным видом пластиковых карт и применяются в различных сферах, таких как финансы, транспорт, пропускной режим и т. д. Они используются для хранения и передачи информации о владельце карты, его учетных данных, балансе счета и других данных, необходимых для выполнения определенных операций.
Основным преимуществом магнитных карт является их низкая стоимость производства и использования. Они также просты в использовании и удобны при проведении платежей и других операций. Однако, их недостатком является ограниченная емкость хранения информации и склонность к повреждениям и износу магнитных полос.
С появлением новых технологий, таких как чипы и бесконтактные карты, магнитные карты постепенно вытесняются более продвинутыми и надежными системами.
Использование карты широко распространено в финансовой сфере гораздо больше, чем в охранной. Для считывания информации с карты используется специальное устройство, которое проводит карту через себя. Однако данная технология не нашла широкого применения в системах контроля и управления доступом, так как информация на карте может быть легко стерта и перезаписана. Это не приемлемо для системы контроля и управления доступом. На рисунке 2.3 показано общее изображение магнитных карт.

Рисунок 2.3 – Пример магнитной карты
Штрихкодовая технология – это способ кодирования и идентификации товаров, использующий специальные символы, называемые штрихкодами. Штрихкоды представляют собой чередующиеся широкие и узкие полосы различной ширины, которые представляют определенные числовые или буквенные значения.
Для чтения штрихкода используется устройство, называемое сканером или считывателем штрихкодов. Сканер осуществляет оптическое считывание штрихкода и передает полученную информацию в компьютер или другое устройство, где она обрабатывается.
Штрихкоды широко применяются в розничной торговле, складском хозяйстве, логистике, фармацевтике и других отраслях. Они позволяют автоматизировать процессы учета и инвентаризации товаров, ускоряют скорость обслуживания покупателей, уменьшают вероятность ошибок при выполнении операций с товарами.
Штрихкодовая технология имеет несколько различных стандартов, таких как EAN-13, UPC, QR-код и другие, которые определяют формат и структуру штрихкода. Каждый штрихкод содержит уникальный код, который позволяет идентифицировать товар или услугу, а также может содержать дополнительную информацию, такую как цена, срок годности, страна производства и т. д.
Промежуточным звеном между штриховой и магнитными технологиями, а также бесконтактными, является

технология Wiegand. В настоящее время она широко распространена во всем мире. Отличительной особенностью Wiegand от магнитных карт является отсутствие магнитной полосы. Вместо этого карта передает сигнал через электромагнитное поле в ответ на сигнал считывателя (карту необходимо поднести очень близко к считывателю). Это означает, что нет необходимости в прямом физическом контакте с считывателем, поэтому карта будет меньше изнашиваться и будет служить дольше. Карты на основе технологии Wiegand могут работать стабильно в температурном диапазоне от -40 до +70 градусов. Кроме карт, идентификатором также может быть брелок или ключ. Эта технология имеет низкую стоимость, устойчивость к помехам, долговечность и высокий уровень защищенности данных.
Wiegand - это технология, которая используется для передачи данных между устройствами без контакта. Она была разработана в 1971 году и с тех пор стала широко применяться в системах безопасности, таких как контроль доступа и системы видеонаблюдения.
Технология Wiegand использует специальные провода или карточки, содержащие магнитные полосы, для передачи информации. Когда карточка или брелок подносится к считывающему устройству, магнитные поля взаимодействуют и передают информацию о коде доступа или идентификаторе.
Преимущества технологии Wiegand включают надежность, высокую скорость передачи данных, защиту от взлома и возможность использования на больших расстояниях. Кроме того, она может быть интегрирована с другими системами безопасности, такими как системы видеонаблюдения или системы контроля доступа. Однако технология Wiegand имеет некоторые ограничения, включая ограниченное количество информации, которое можно передать, и возможность неправильного чтения данных в случае магнитного воздействия.
В целом, технология Wiegand представляет собой надежный и эффективный способ передачи данных без контакта, и она продолжает использоваться в различных системах безопасности по всему миру.
Биометрические технологии - это методы и инструменты, использующие измерения и анализ биологических характеристик человека для идентификации или аутентификации личности. Они основаны на уникальных физиологических и/или поведенческих особенностях каждого человека.
Данная технология предполагает использование индивидуальных биометрических параметров человека. В настоящее время на рынке существует технология, которая определяет личность человека по отпечаткам пальцев, чертам лица, радужной оболочке глаза, голосу, ладони и другим параметрам. Эти системы используют статические средства, которые имеют вероятностный характер. В связи с этим каждое считывание параметра может изменяться и допускать ошибки. Однако такие системы имеют сложные алгоритмы идентификации, их преимуществом является возможность объединения нескольких таких систем в единую систему контроля доступа, что позволяет создать систему контроля доступа, удовлетворяющую самым строгим требованиям безопасности. На рисунке 2.4 показаны основные элементы биометрической СКУД.
Примеры биометрических технологий включают:
1. Сканеры отпечатков пальцев: меряют уникальные детали папиллярных линий на пальцах и используют их для идентификации или аутентификации личности.
2. Сканеры сетчатки глаза: анализируют уникальные характеристики сетчатки глаза для определения личности.
3. Системы распознавания лиц: сканируют и анализируют уникальные особенности лица, такие как расположение глаз, носа и рта, для определения личности.
4. Системы распознавания голоса: анализируют уникальные аспекты звукового профиля голоса, такие как тональность, скорость и интонация, для определения личности.
5. Системы распознавания походки: анализируют уникальные особенности движения и походки человека для идентификации или аутентификации личности.
Биометрические технологии широко применяются в сферах безопасности, контроля доступа, банковского дела и медицинской диагностики. Они обеспечивают высокий уровень защиты и удобство использования, так как не требуют запоминания паролей или использования физических документов. Однако, есть определенные проблемы, связанные с точностью и приватностью при использовании биометрических технологий, которые требуют дальнейших исследований и разработки.

. Лебедев, А. В. Идентификаторы систем контроля доступа: основные принципы и технологии // Материалы IV научно-технической конференции "Современные информационные технологии и IT-общество" (MIT&ITO'2019). – 2019.
2. Грачев, А. И. Системы контроля и управления доступом в информационных системах // Электронные системы управления. – 2018. – № 5. – С. 32-39.

3. Карташова, Н. А. Идентификация и аутентификация в системах контроля доступа // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – № 1(109). – С. 77-82.
4. Кудряшова, А. В. Системы контроля доступа в информационных системах // Инновационная наука. – 2016. – № 4. – С. 44-51.
5. Пимонов, В. В. Особенности реализации систем управления доступом в информационных системах // Вестник международных организаций: образование, наука, новая экономика. – 2015. – № 2. – С. 110-116.
6. Блинов, В. Е. Основные принципы идентификации и аутентификации в системах контроля доступа // Информационные технологии и безопасность. – 2014. – № 1(37). – С. 55-63.
7. Романова, Е. В. Системы контроля доступа в информационных системах и их классификация // Вестник Московского университета имени С.Ю. Витте. Серия 1: Экономика и управление. – 2013. – № 2. – С. 60-64.
8. Федоров, А. Н. Проблемы и перспективы развития систем контроля доступа в информационных системах // Информационные системы и технологии. – 2012. – № 4. – С. 102-107.
9. Дмитриев, В. В. Системы контроля и управления доступом в информационных системах // Восточно-Европейский журнал передовых технологий. – 2011. – № 2/7(56). – С. 65-72.
10. Смирнов, П. В. Развитие систем контроля и управления доступом в информационных системах // Вестник Московского гуманитарного университета имени М.А. Шолохова. Серия 5: Информатика и вычислительная техника. – 2010. – Т. 1. – С. 99-106.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:
https://stuservis.ru/kursovaya-rabota/416893