МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова»)

БГТУ.СМК-Ф-4.2-К5-01

Факультет И (шифр) Информационные и управляющие системы (наименование)

Кафедра И9 (шифр) Систем управления и компьютерных технологий (наименование)

Дисциплина Научно-исследовательская работа в семестре

КУРСОВАЯ РАБОТА

на тему

«Разработка системы контроля управления доступом (СКУД) с максимальной отказоустойчивостью и методы обеспечения ее бесперебойной работы»

Выполнил студент группы И9М31

Густова Д. Р.
Фамилия И.О.

РУКОВОДИТЕЛЬ

Готин С. В. _____
Фамилия И.О. Подпись

Оценка _____

«_____» _____ 2018 г.

САНКТ-ПЕТЕРБУРГ

2018 г.

Содержание

Введение……3

1. Разработка алгоритмов взаимодействия и идентификации элементов СКУД……...4

Заключение……..17

Список использованных источников……18

Введение

Системы контроля и управления доступом (СКУД) прочно заняли свое место в перечне технических систем безопасности, предлагаемых на рынке. Вместе с охранно-пожарной сигнализацией и системами телевизионного наблюдения, они образуют базу для интеграции систем безопасности зданий в единый комплекс.

Любая СКУД предназначена для того, чтобы автоматически пропускать тех, кому это положено, и не пропускать тех, кому это запрещено, контролируя тем самым перемещения сотрудников и посетителей на территории предприятия.

СКУД позволяет в любое время обеспечить контроль над ситуацией, порядок, безопасность персонала и посетителей. Кроме того, СКУД дает возможность контролировать трудовую дисциплину, производить учет использования персоналом своего рабочего времени и многое другое.

Контроллерная СКУД – это совокупность аппаратных, программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта. При их действительном многообразии все они работают по единой схеме: оборудование (запорно-пропускной механизм, будь то турникет, шлагбаум, проходная кабина и любое другое управляемое преграждающее устройство, а также считыватели - устройство, предназначенное для считывания (ввода) идентификационных признаков и др.) подключается к контроллеру, который в свою очередь подсоединяется к компьютеру.

Таким образом, центральным элементом данного класса СКУД является контроллер — устройство, предназначенное для обработки информации, поступающей от считывателей, идентификаторов, для принятия решения и управления исполнительными устройствами. Поэтому его часто называют «сердцем СКУД».

Поскольку тематикой магистерской диссертации была выбрана: «Разработка системы контроля управления доступом (СКУД) с максимальной отказоустойчивостью и методы обеспечения ее бесперебойной работы», первым этапом было выполнить следующие задачи:

- Разработать алгоритмы взаимодействия и идентификации элементов СКУД.
- Подобрать элементную базу.

1 Разработка алгоритмов взаимодействия и идентификации элементов СКУД

Важнейшим аспектом в работе системы контроля управления доступом (СКУД) является гарантированность защищенности информации, территории, имущества, а также безопасности жизнедеятельности.

Для контроля и организации максимально эффективного рабочего процесса необходимо автоматизировать часть процессов, задачами которых являются службы безопасности, отдел охраны труда, а также такие вопросы, как учет рабочего времени, контроль охраняемой территории и прочее.

Следовательно, первостепенной задачей является анализ организационную структуры службы безопасности.

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности предприятия (фирмы, компании и т.д.) за рубежом определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов и мощности организации, деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью. В зарубежных источниках, например, рассматривается следующая структура службы безопасности фирмы. Она возглавляется начальником службы безопасности, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны.

С учетом накопленного зарубежного и отечественного опыта и особенностей рыночной экономики предлагается рабочий вариант службы безопасности предприятия среднего масштаба производства, ее структура и должностные инструкции.

Общие положения

Основными задачами службы безопасности предприятия являются обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации, независимо от ее назначения и форм при всем многообразии возможных каналов ее утечки и различных злонамеренных действий со стороны конкурентов.

Правовые основы деятельности службы безопасности

Основные положения, состав и организация службы безопасности имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах предприятия.

В основу деятельности службы безопасности положены:

- Закон Российской Федерации «О безопасности".
- Законы и регламенты России, обеспечивающие безопасность деятельности и сохранность коммерческой тайны.
- Закон о предприятиях и предпринимательской деятельности.
- Кодекс законов о труде (КЗОТ).

Устав предприятия, коллективный договор, трудовые договоры, правила внутреннего трудового распорядка сотрудников, должностные обязанности руководителей, специалистов, рабочих и служащих.

Основные задачи службы безопасности.

Основными задачами службы безопасности предприятия являются:

- Обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной.
- Организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны.
- Организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- Предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну.
- Выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях.
- Обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне.
- Обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности.

- Обеспечение личной безопасности руководства и ведущих сотрудников и специалистов.
- Оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Общие функции службы безопасности.

Служба безопасности предприятия выполняет следующие функции:

- Организует и обеспечивает пропускной и внутри объектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями.
- Руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны.
- Участвует в разработке основополагающих документов с целью закрепления в них требований обеспечение безопасности и защиты коммерческой тайны, в частности, Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих.
- Разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований «ИНСТРУКЦИИ по защите коммерческой тайны".
- Изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнеров, смежников.
- Организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия.
- Разрабатывает, ведет, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации.
- Обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны.

- Осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах условиях по защите коммерческой тайны.
- Организует и регулярно проводит учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход.
- Ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов.
- Ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации.
- Поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

Состав службы безопасности.

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. Организационно служба безопасности состоит из следующих структурных единиц:

- Отдела режима и охраны, в составе сектора режима и сектора охраны.
- Специального отдела в составе сектора обработки секретных документов и сектора обработки документов с грифом «Коммерческая тайна".
- Инженерно-технической группы.
- Группы безопасности внешней деятельности.

Права, обязанности и ответственность сотрудников службы безопасности.

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:

- Требовать от всех сотрудников предприятия, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных

документов или договорных обязательств по защите коммерческой тайны.

- Вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности обязаны:

- Осуществлять контроль за соблюдением «инструкции по защите коммерческой тайны".
- Докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, могущих привести к утечке конфиденциальной информации или утрате документов или изделий.
- Не допускать неправомерного ознакомления с документами и материалами с грифом «Коммерческая тайна» посторонних лиц.

Сотрудники службы безопасности несут ответственность за личное нарушение безопасности коммерческой тайны и за не использование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

Нештатные структуры службы безопасности.

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства предприятия и службы безопасности могут создаваться отдельные комиссии, решающие определенные контрольно-ревизионные функции на временной или постоянной основе, такие как:

- Квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей).
- Комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п..
- Периодические проверочные комиссии для проверки знаний и умений выполнять требования нормативных документов по защите коммерческой тайны, а также по оценке эффективности и надежности защитных мероприятий по обеспечению безопасности предприятия.

Для того, чтобы гарантировать выше перечисленные требования, будущая система должна обладать высокими показателями отказоустойчивости, защищенности от взломов, возможностью

самотестирования на предмет неисправностей, а также наличием способности резервного восстановления основных элементов управления.

Первостепенно, нужно исследовать наиболее критичные узлы дисперсии при взаимодействии элементов системы.

Рассмотрим пример работы охранной сигнализации «СТРАЖ-GSM» как частный случай СКУД.

При взаимодействии данной сигнализации с тревожными датчиками (геркон, датчик дыма, ИК-датчик движения, датчики разбития стекол и т.д.) основная потенциальная угроза заключается в связи, по радиоканалу, с центральной системой управления. Существует большое количество устройств постановки радиочастотной помехи для нарушения взаимодействия и обмена информацией элементов сигнализации, а также для подавления каналов связи и реагирования в случае появления тревожного сигнала.

Данная уязвимость является первым критическим недостатком СКУД.

Для устранения данного недостатка необходимо разработать проводной канал с функцией проверки работоспособности ключевых элементов системы.

Для выявления второго недостатка рассмотрим, в качестве примера, автономную СКУД «Iron Logic Matrix-2».

Поскольку считыватель, выполняющий функцию идентификации личности интегрирован в один корпус с основным контроллером, его необходимо устанавливать за границами контролируемой зоны, что позволяет, демонтировав один элемент не только получить доступ, но и украсть конфиденциальную информацию с полным списком, количеством, идентификационными данными всего персонала, зарегистрированного в данном контроллере, что в последующем максимально критично отразиться на выполнении основных тактико-технических требований.

Соответственно, ***вторым критическим недостатком может являться некорректное расположение центральной системы управления, а также отсутствие резервных тревожных систем***, которые бы позволяли выявлять и сигнализировать о неполадках в центральной системе управления.

В любой подобной системе одной из самых важных задач является корректная, безошибочная идентификация пользователя. Как правило, доступ разграничивается с помощью персональных RFID меток, ключей формата Touch Memory, QR-кодов, либо биометрических данных (отпечатки пальцев, сканирование радужной оболочки глаза, сетчатки, распознавание лиц).

Далее необходимо провести сравнительный анализ методов авторизации пользователя, а также рассмотреть возможность двухфакторной аутентификации.

Одним из наиболее распространенных методов идентификации пользователя в СКУД является технология RFID (Radio Frequency IDentification).

RFID - технология автоматической идентификации, в котором посредством радиосигналов считываются и записываются данные. Данные хранятся в так называемой RFID - метке. RFID - система состоит из ридера и метки.

RFID-метки классифицируются по рабочей частоте, типу памяти и источнику питания. Ридеры бывают стационарные и мобильные.

Типы атак, применяемые в технологии RFID

Существует огромное количество различных видов атак. Ниже представлен небольшой список применяемых атак:

- Dos-атака.
- RFID-Zapper.
- Клонирование.
- Подмена содержимого памяти RFID-меток.
- Атаки через RFID-метки.

Dos-атака

Атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён.

Отказ «вражеской» системы может быть и шагом к овладению системой (если в нештатной ситуации ПО выдаёт какую-либо критическую информацию — например, версию, часть программного кода и т. д.). Но чаще это мера экономического давления: потеря простой службы, приносящей доход, счета от провайдера и меры по уходу от атаки ощутимо бьют «цель» по карману.

В настоящее время DoS - атака наиболее популярна, так как позволяет довести до отказа практически любую систему, не оставляя юридически значимых улик.

В настоящее время DoS - атака наиболее популярна, так как позволяет довести до отказа практически любую систему, не оставляя юридически значимых улик.

RFID-Zapper

Электронное устройство, которое может перманентно отключить пассивный RFID чип. В отличие от других методов отключения, не повреждает устройство, к которому подключён. Впервые представлен на выставке Chaos Communication Congress в 2005 году.

Устройство можно собрать из фотовспышки. Вместо ксеноновой лампы-вспышки подключается катушка индуктивности. Между электролитическим конденсатором и катушкой индуктивности встраивается выключатель, при замыкании которого через катушку индуктивности протекает очень большой электрический ток, который создаёт мощное магнитное поле. Согласно закону электромагнитной индукции, в проводниках внутри чипа возбуждается электрический ток, который при высоких значениях может вывести из строя микросхему.

Клонирование

Джонатан Вестхьюз (Jonathan Westhues) — студент, который создал устройство, позволяющее клонировать метки.

Девайс назван «proxmark». Он легко помещался в карман и при достаточно близком расстоянии можно незаметно клонировать метку.

Подмена содержимого памяти RFID-меток

На завершившейся хакерской конференции Defcon немецкий эксперт инфосека Лукас Грюнвальд (Lukas Grunwald) продемонстрировал, как содержимое электронного паспорта может быть легко перенесено на любую другую радиометку. При этом Лукас использовал разработанную вместе с его коллегой Борисом Вольфом (Boris Wolf) еще пару лет назад прогу RFDump, которая умеет считывать, редактировать, записывать (если это возможно) данные RFID-меток. Первой версией данной проги был простенький perl-скрипт, теперь же RFDump представляет собой удобную тулзу, распространяющуюся под лицензией GPL. Существуют пока только версии для Linux. Для работы программы необходим RFID-ридер ACG Multi-Tag Reader или ему подобный. Грюнвальд вносит в софт время от времени кое-какие поправки. Например, сейчас она позволяет задействовать в метке счетчик считываний (функция cookie), планируется введение возможности снятия шифрования данных меток с помощью брутфорса или атаки по словарю, а также проверка на ключи, выставляемые «по умолчанию».

После создания своей программы Лукас и Борис занялись активным изучением возможности взлома различных RFID-систем. Первым делом они изучили RFID-систему местного университетского кафе, где данные о сумме

на счете клиента хранились прямо на карточке. Питание там стало для них бесплатным :). Дальше — больше: они останавливались в гостиницах и отелях, в которых для входа в номер использовались proximity-карты. Интересный факт: ни одна из десяти изученных ими RFID-система из не имела шифрования, и Грюнвальд после изучения 2-3 карт мог создать мастер-карту, открывающую любую дверь. Но и системы с шифрованием очень просто обойти: либо ключ подбирался простым перебором, либо стоял выставленный производителем по умолчанию. Уязвимыми оказались и системы супермаркетов, где начали применять RFID как альтернативу штрихкодам. Хакеры получили возможность с помощью карманных компьютеров поменять метки дорогостоящих товарах на менее дорогие, «спасая» таким образом свою наличность. По словам Грюнвальда, 3/4 всех изученных им RFID-систем оказались так или иначе уязвимы.

Атаки через RFID-метки.

На самом деле через редактирование метки можно получить доступ к компьютеру и тем самым совершать различного рода атаки. Уязвимые места RFID-метки: SQL-Injection, web-интерфейсы, где не исключена возможность внедрения вредоносного кода, а также buffer overflow.

Допустим, в RFID-системе используются только метки с объемом памяти 128 байт. Программист, писавший приложение, обрабатывающее содержимое тэгов, пренебрег проверкой на длину этого самого содержимого. В итоге имеется возможность для переполнения буфера, ведь злоумышленник может внедрить в систему метку с большим количеством памяти, чем 128 байт, внедрив туда и шелл-код.

Остановка атак на базу данных

Для того, чтобы избежать атаки типа SQL — Injection следует выполнять тщательную проверку данных, передаваемых SQL — запросом. Так же существует понятие ORM — библиотек, которые являются посредником между базой и программой. Некоторые базы данных предоставляют возможности, которые ограничивают вероятность нападения.

Например, как Oracle и MySQL позволяет только один запрос к исполнению в течение вызовов API, хотя новых версий MySQL позволяют программисту включить несколько запросов.

Клиентские сценарии можно предотвратить с помощью правильной обработки скриптов. Языки, используемые в web-разработке, обычно предоставляют функции, которые могут сделать это за пользователя. PHP может делать это автоматически для каждой строки. Если скриптовый язык не требуется, его отключение позволит избежать любой возможности его злоупотребления. SSI инъекцию можно также избежать использованием надлежащей обработки. Или отключить SSI.

Переполнение буфера (stack overflow) можно также избежать надлежащей проверкой границ буфера. Такие инструменты как Valgrind и Electric Fence помогут осуществить проверку. Конечно использование языка программирования, который выполняет данные проверки, было бы гораздо лучше. Один из таких языков является Java.

Исходя из вышесказанного, метод идентификации (рисунок 1) RFID содержит в себе достаточное количество уязвимостей и не удовлетворяет требованиям будущей системы, следовательно, необходимо найти более надежные способы авторизации пользователей.

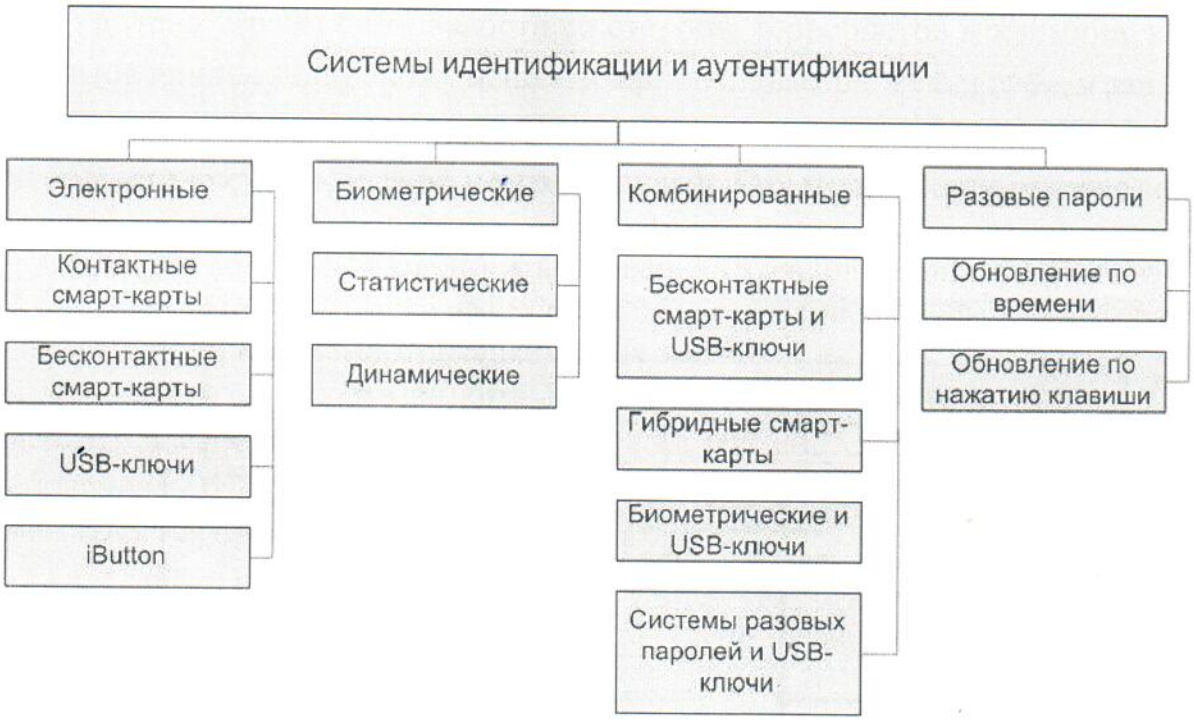

Рисунок 1 – Системы идентификации и аутентификации.

Проблема идентификации личности при допуске к закрытой информации или объекту всегда была ключевой. Магнитные карты, электронные пропуска, кодированные радиосообщения можно подделать, ключи можно потерять, при особом желании даже внешность можно изменить. Но целый ряд биометрических параметров является абсолютно уникальным для человека.

Где применяется биометрическая защита

Современные биометрические системы дают высокую надежность аутентификации объекта (рисунок 2). Обеспечивают контроль доступа в следующих сферах:

- Передача и получение конфиденциальной информации личного или коммерческого характера.
- Регистрация и вход на электронное рабочее место.
- Осуществление удаленных банковских операций.
- Защита баз данных и любой конфиденциальной информации на электронных носителях.
- Пропускные системы в помещения с ограниченным доступом.

Уровень угрозы безопасности со стороны террористов и криминальных элементов привел к широкому использованию биометрических систем защиты и управления контролем доступа не только в государственных организациях или больших корпорациях, но и у частных лиц. В быту наиболее широко такое оборудование применяется в системах доступа и технологиях управления типа «умный дом».

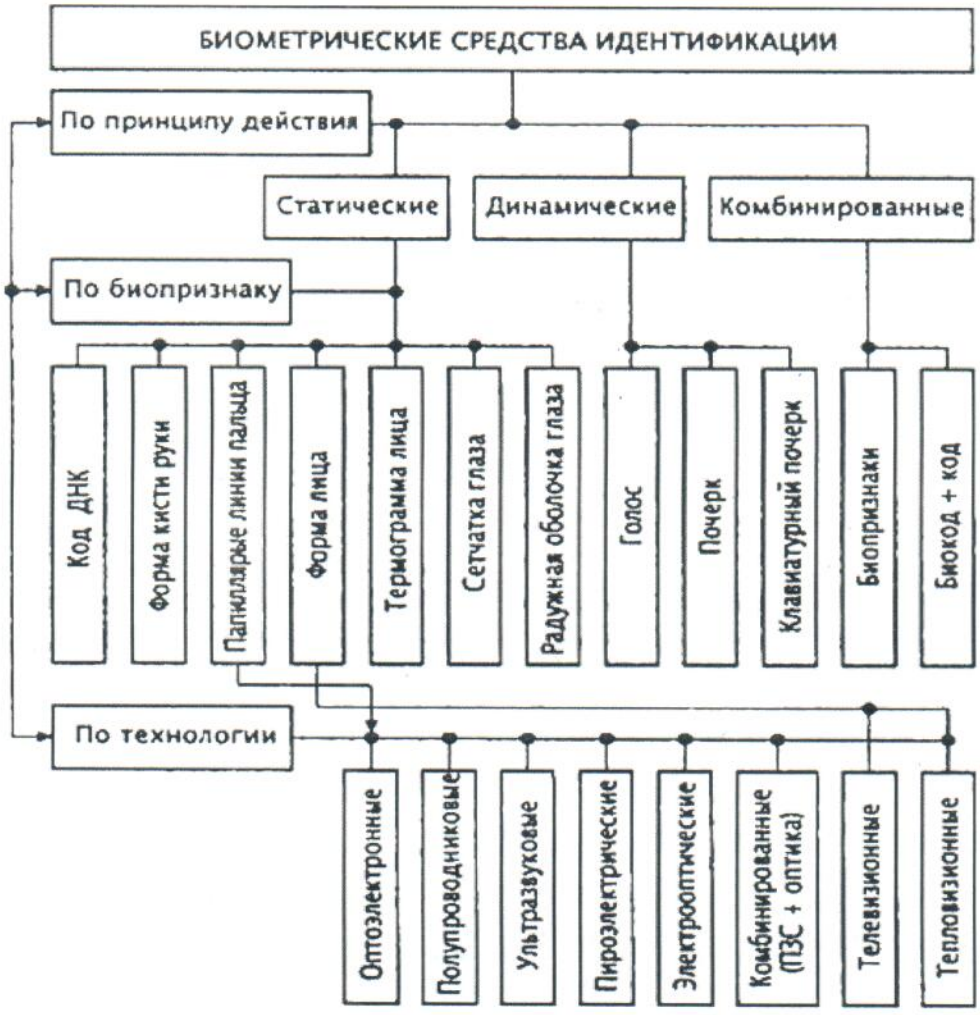

Рисунок 2 – Биометрические средства идентификации.

Биометрические характеристики являются очень удобным способом аутентификации человека, так как обладают высокой степенью защиты (сложно подделать) и их невозможно украсть, забыть или потерять.

Дактилоскопия (распознавание отпечатков пальцев) — наиболее разработанный на сегодняшний день биометрический метод идентификации личности. Катализатором развития метода послужило его широкое использование в криминалистике 20 века.

Каждый человек имеет уникальный папиллярный узор отпечатков пальцев, благодаря чему и возможна идентификация. Обычно алгоритмы используют характерные точки на отпечатках пальцев: окончание линии узора, разветвлении линии, одиночные точки. Дополнительно привлекается информация о морфологической структуре отпечатка пальца: относительное положение замкнутых линий папиллярного узора, «арочных» и спиральных линий.

Особенности папиллярного узора преобразовываются в уникальный код, который сохраняет информативность изображения отпечатка. И именно «коды отпечатков пальцев» хранятся в базе данных, используемой для поиска и сравнения. Время перевода изображения отпечатка пальца в код и его идентификация обычно не превышает 1 секунды, в зависимости от размера базы. Время, затраченное на поднесение руки – не учитывается.

Преимущества и недостатки метода

Преимущества метода. Высокая достоверность — статистические показатели метода лучше показателей способов идентификации по лицу, голосу, росписи. Низкая стоимость устройств, сканирующих изображение отпечатка пальца. Достаточно простая процедура сканирования отпечатка.

Недостатки метода. Папиллярный узор отпечатка пальца очень легко повреждается мелкими царапинами, порезами. Люди, использовавшие сканеры на предприятиях с численностью персонала порядка нескольких сотен человек заявляют о высокой степени отказа сканирования. Многие из сканеров неадекватно относятся к сухой коже и не пропускают стариков. Так же присутствует недостаточная защищённость от подделки изображения

отпечатка, отчасти вызванная широким распространением метода. Для некоторых людей с «неподходящими» пальцами (особенности температуры тела, влажности) вероятность отказа в доступе может достигать 100%. Количество таких людей варьируется от долей процентов для дорогих сканеров до десяти процентов для недорогих. Конечно, стоит отметить, что большое количество недостатков вызвано широкой распространённостью системы, но эти недостатки имеют место быть и проявляются они очень часто.

Исходя из выше изложенного, в разрабатываемой системе контроля управления доступом будет использоваться дактилоскопия для идентификации пользователя.

Заключение

В результате курсовой работы была выполнена задача разработки алгоритма взаимодействия и идентификации элементов СКУД.

Были изучены технологии RFID, их особенности и недостатки.

Были рассмотрены системы идентификации и аутентификации. Подробно рассмотрены средства биометрической идентификации.

Для разрабатываемой СКУД был выбран метод дактилоскопической идентификации пользователя, который будет являться основным.

Список использованных источников

1. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2001.
2. Барсуков В.С. Интегральная защита информации // Системы безопасности. – М., 2002.
3. Гинце А. Новые технологии в СКУД // Системы безопасности, 2005.
4. Горлицин И. Контроль и управление доступом - просто и надежно КТЦ "Охранные системы", 2002.
5. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия - Телеком, 2000.
6. Сабынин В.Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Информост радиоэлектроники и телекоммуникации, 2001.