Лабораторная работа №6

4 часа

Тема: Анализ структуры условных обозначений средств контроля и управления доступом, способов идентификации.

Цель лабораторной работы: Провести исследование структуры условных обозначений средств контроля и управления доступом, способов идентификации.

Задание №1.

Выполнить классификацию СКУД.

Задание №2.

Провести исследование способов идентификации в СКУД.

Задание №3.

Провести исследование структуры условных обозначений средств контроля и управления доступом.

Отчет по лабораторной работе должен быть выполнен согласно утвержденным на кафедре требованиям и содержать:

1. Тема ЛР.
2. Цель ЛР.

Результаты по каждому выполненному заданию.

3. Выводы по каждому заданию.
4. Заключение.
5. Список использованной литературы.

Методический материал к ЛР (Приложение 1).

Приложение 1.

Методический материал

Классификация систем контроля и управления доступом, принципы их построения и функционирования

Средства контроля и управления доступом подразделяют по:

- функциональному назначению устройств;
- функциональным характеристикам;
- устойчивости к НСД.

На рисунке 3.11 приведена классификация средств контроля и управления доступом по функциональному назначению устройств и функциональным характеристикам .

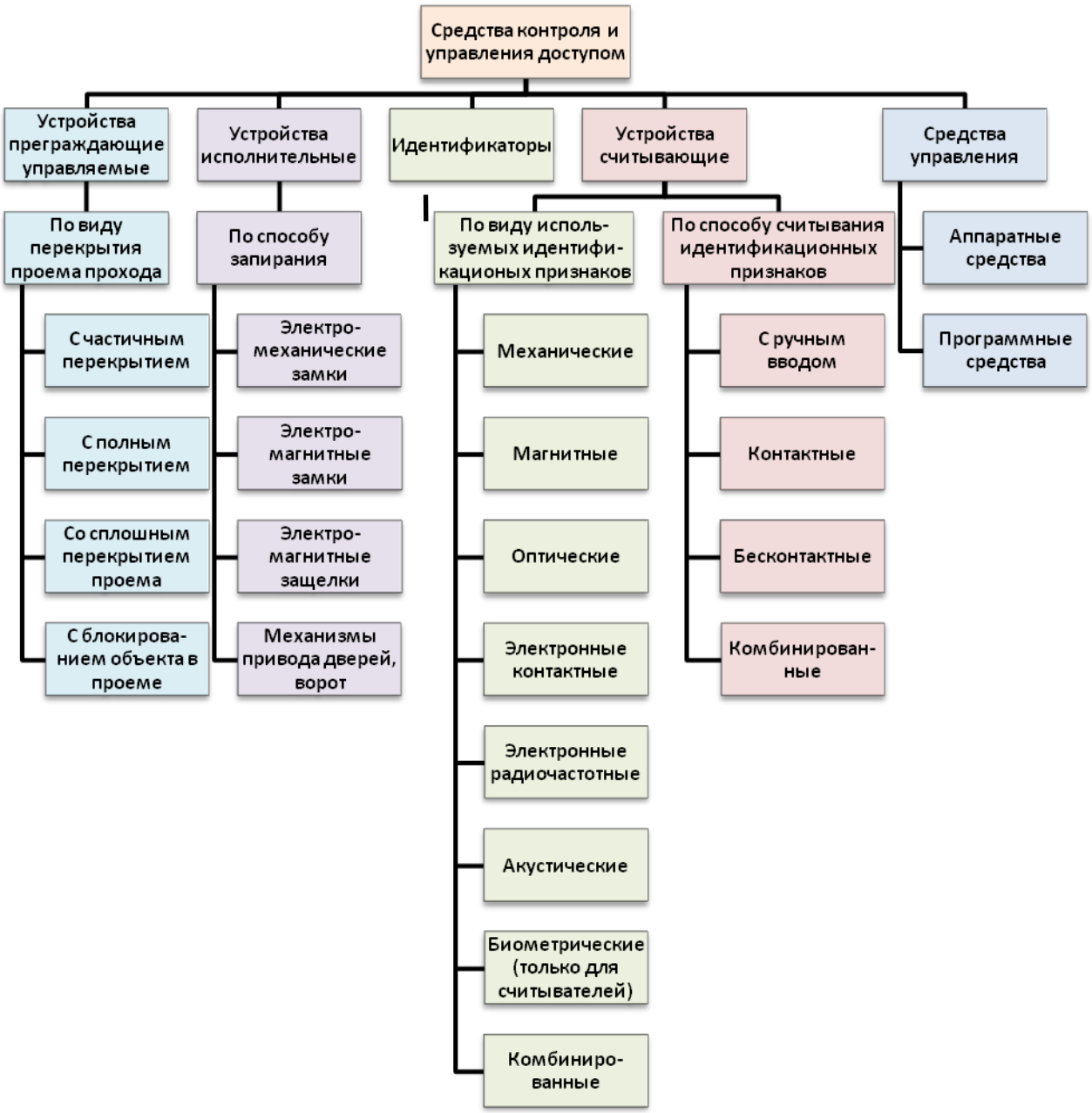

Рисунок 3.11 – Классификация средств контроля и управления доступом по функциональному назначению устройств и функциональным характеристикам

1) По функциональному назначению устройств средства контроля и управления доступом подразделяют на:

- УПУ в составе преграждающих конструкций и исполнительных устройств;
- устройства исполнительные;
- устройства считывающие;
- идентификаторы;

- средства управления в составе аппаратных устройств и программных средств.

2) По функциональным характеристикам средства контроля и управления доступом подразделяют на следующие группы:

а) УПУ – по виду перекрытия проема прохода:

- с частичным перекрытием (турникеты, шлагбаумы);
- с полным перекрытием (полноростовые турникеты, специализированные ворота);
- со сплошным перекрытием проема (сплошные двери, ворота);
- с блокированием объекта в проеме (шлюзы, кабины проходные);

б) Устройства исполнительные – по способу запирания:

- электромеханические замки;
- электромагнитные замки;
- электромагнитные защелки;
- механизмы привода дверей, ворот;

в) Идентификаторы и считыватели – по виду используемых идентификационных признаков:

- механические – представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
- магнитные – представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т. д.);
- оптические – представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, топографические метки и т. д.);
- электронные контактные – представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т. д.);

- электронные радиочастотные – считывание кода с электронных идентификаторов происходит путем передачи данных по радиоканалу;
- акустические – представляют собой кодированный акустический сигнал;
- биометрические (только для считывателей) – представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);
- комбинированные – для идентификации используются одновременно несколько идентификационных признаков;

г) Считыватели – по способу считывания идентификационных признаков:

- с ручным вводом – ввод производится с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;
- контактные – ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;
- бесконтактные – считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;
- комбинированные.

д) Средства управления СКУД:

- аппаратные средства (устройства) – контроллеры доступа, приборы приемно-контрольные доступа;
- программные средства – программное обеспечение СКУД.

3) Классификация средств контроля и управления доступом по устойчивости к НСД основана на устойчивости к разрушающим и неразрушающим воздействиям по уровням устойчивости:

- нормальной;
- повышенной;
- высокой.

УПУ классифицируют по устойчивости к разрушающим воздействиям. Устойчивость УПУ устанавливают по:

- устойчивости к взлому;
- пулестойкости (только для УПУ со сплошным перекрытием проема);
- устойчивости к взрыву.

Нормальная устойчивость УПУ обеспечивается механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

Для УПУ повышенной и высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и блокированием объекта в проеме (шлюзы, кабины проходные) устанавливается классификация по устойчивости к взлому, взрыву и пулестойкости как для защитных дверей по ГОСТ Р 51072.

Классификация устройств исполнительных (замки, защелки) по устойчивости к разрушающим воздействиям в зависимости от конструкции – по ГОСТ Р 52582, ГОСТ Р 51053, ГОСТ 19091, ГОСТ 5089.

По устойчивости к неразрушающим воздействиям средства контроля и управления доступом в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию – для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению – для считывателей ввода запоминаемого кода (клавиатуры, кодовые переключатели и т.п.);
- устойчивость к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники и средств управления СКУД от НСД к информации.

Классификацию по устойчивости к неразрушающим воздействиям: вскрытию, манипулированию, наблюдению, копированию устанавливают в стандартах и нормативных документах на средства контроля и управления доступом конкретного типа.

Классификация средств контроля и управления доступом по устойчивости к НСД приведена на рисунке 3.12.

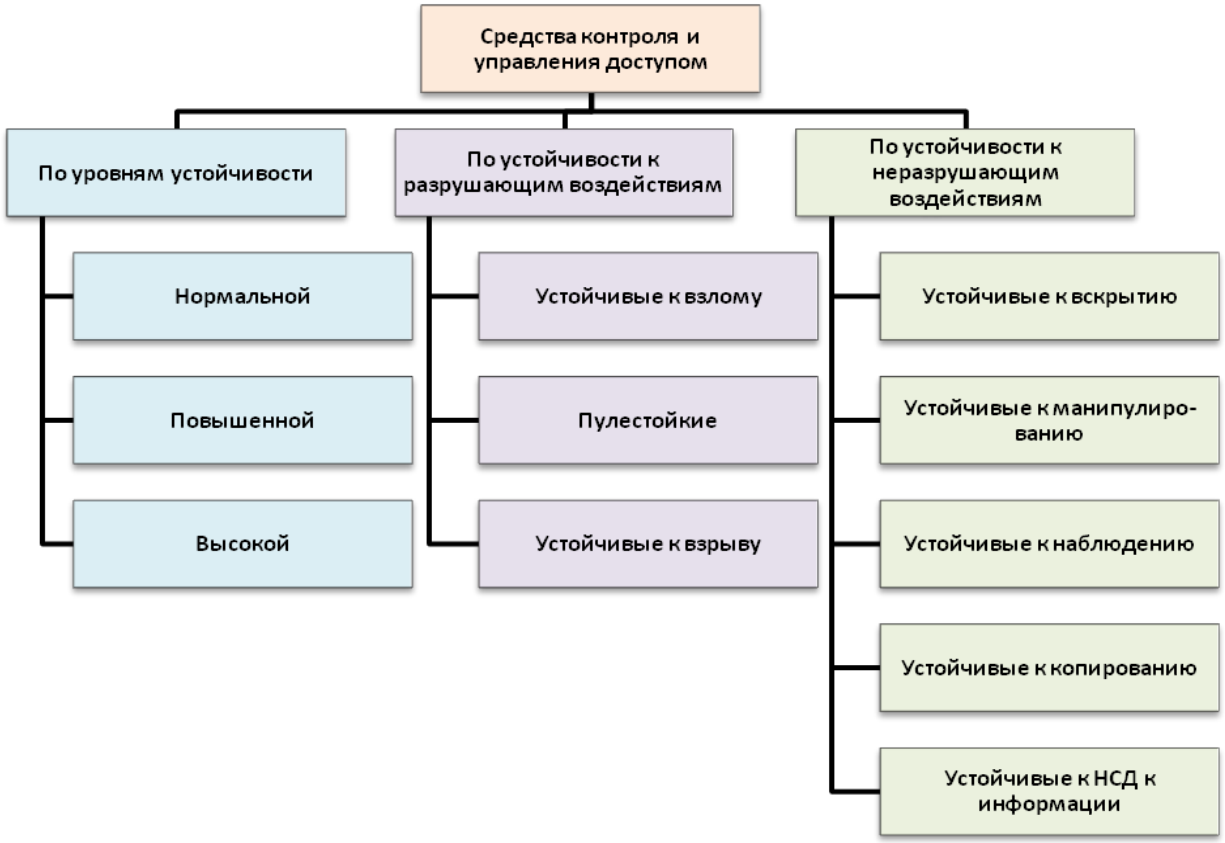

Рисунок 3.12 - Классификация средств контроля и управления доступом по устойчивости к НСД

Общая классификация СКУД

СКУД классифицируются по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- уровню защищенности системы от НСД к информации.

По способу управления СКУД подразделяются на:

- автономные – для управления одним или несколькими УПУ без передачи информации на центральное устройство управления и без контроля со стороны оператора;
- централизованные (сетевые) – для управления УПУ с обменом информацией с центральным пультом, контролем и управлением системой со стороны центрального устройства управления;
- универсальные (сетевые) – включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и

переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи.

По количеству контролируемых точек доступа СКУД могут быть:

- малой емкости (менее 64 точек);
- средней емкости (не менее 64 и не более 256 точек);
- большой емкости (более 256 точек).

По функциональным характеристикам СКУД могут быть трех классов:

- 1 класс – системы с ограниченными функциями;
- 2 класс – системы с расширенными функциями;
- 3 класс – многофункциональные системы.

По уровню защищенности системы от НСД к информации СКУД классифицируют как для систем с централизованным управлением по защищенности от НСД к информации программного обеспечения СКУД и средств вычислительной техники, входящих в состав сетевых СКУД как для автоматизированных систем.

3.4 Способы идентификации и их характеристика

Все СКУД принято различать по способам идентификации предъявителя.

Существует достаточно большое количество способов идентификации и типов идентификаторов пользователя.

На сегодняшний день для использования в СКУД возможен один из следующих способов идентификации, основанных на предъявлении пользователем:

- вещественного идентификатора (ключ, пропуск);
- идентификатора (магнитная карта, вигант-карта, смарт-карта, проксимити-карта и т.п.);
- биометрических характеристик субъекта.

1) Предъявление вещественного идентификатора

Достоинства:

- простота и дешевизна установки, эксплуатации и обслуживания точки доступа;

- возможность обеспечить контроль и управление доступом организационными мероприятиями;
- идентификаторы просты в эксплуатации и не требовательны к хранению и др.

Недостатки:

- возможность утраты, хищения идентификатора;
- отсутствует секретность кода идентификатора;
- относительная легкость скрытно сделать дубликат идентификатора;
- возможность предъявления чужого идентификатора злоумышленником;
- для карточек – это малый срок службы.

Ключ от механического замка

Ключ от современного замка (накладного или врезного) обеспечивает достаточную надежность и простоту эксплуатации.

Однако если предстоит открывать несколько дверей, то пользователю предстоит носить уже связку ключей. Существует значительный риск утраты ключа. Он снижается, если ключи сдаются владельцем для хранения при выходе с объекта. Вместе с тем для нарушителя при отсутствии должной охраны создаются благоприятные условия для допуска ко всем ключам сразу. При утрате ключа или уходе сотрудника с предприятия необходима замена либо всего замка, либо его секретной части. Существенным недостатком такого средства идентификации является отсутствие возможности протоколизации прохода точки доступа.

Пропуск

Организация пропускной системы, когда идентификация осуществляется контролёром по обычным пропускам (постоянным, временным, разовым), является наиболее распространенной и легко организуемой СКУД.

Однако ей присущ ряд недостатков, снижающих ее эффективность. Такая система требует присутствие контролёра, который решение о допуске принимает на основе субъективных ощущений, что создает предпосылки к проходу несанкционированного лица.

Другими недостатками этой системы являются:

- ежемесячные расходы на содержание штата вахтеров;

- отсутствие возможности объективной протоколизации событий и др.

Карта перфорированная

Представляет собой металлическую или пластмассовую пластину. Информация записывается на ней с помощью пробивки отверстий в определенном порядке один раз при изготовлении.

Считывание информации осуществляется оптическим или механическим считывателями. Такая карточка – самый простой и дешевый идентификатор, но она не обеспечивает секретность кода и легко подделывается.

Как недостаток можно отметить:

- срок службы карточки 1-2 года;
- механический считыватель такой системы очень капризен в эксплуатации.

Карта со штриховым кодом

Этот идентификатор представляет собой карточку с нанесенными на поверхность одномерным или двумерным рисунком (набор линий или матрица), ширина и расстояние между которыми представляют собой кодовую последовательность. Кодовая последовательность наносится на карточку при ее изготовлении и содержит записанную информацию, которую, как правило, считывается оптическим способом.

Для повышения устойчивости против копирования рисунок часто закрывается пленкой, не пропускающей видимый свет, но прозрачной для ИК диапазона, в котором работает оптический считыватель. Достоинством оптического считывателя является отсутствие движущихся частей.

При сканировании карточки она не нуждается в физическом контакте со считывателем, поэтому считыватель обладает большей надежностью в работе и с успехом может применяться вне помещений. Вероятность подделки карточки достаточно высока (можно сделать копию на ксероксе).

Примером применения такой СКУД является организация прохода пассажиров на платформу железнодорожного вокзала.

2) Предъявление электронного идентификатора

Достоинства:

- достаточно высокая скрытность и секретность кода идентификатора;

- возможность обновления кода (для смарт-карт);
- высокая эффективность контроля и управления доступом при значительной пропускной способности;
- скрытность проведения идентификации (для проксимити-карт);
- достаточно высокая надежность идентификации и долговечность эксплуатации;
- невозможность создания дубликата идентификатора;
- с утратой идентификатора не нужна замена считывателя;
- идентификаторы просты в эксплуатации и (большинство) не требовательны к хранению и др.

Недостатки:

- относительно дорогое оборудование для организации контроля и управления доступом;
- возможность потери и хищения идентификатора;
- возможность предъявления чужого идентификатора злоумышленником и др.

Карта магнитная

Представляет собой карточку с магнитной полосой, на которой записан код (рисунок 3.13). При желании код, записанный на дорожках магнитной полосы, может быть легко перепрограммирован, а при ее утере можно быстро и дешево закодировать новую карточку.

Рисунок 3.13 – Магнитная карта

Код с карточки считывается магнитным считывателем, принцип работы которого аналогичен считывателю обычного магнитофона. Информация считывается при перемещении карточки между магнитными головками считывателя.

Карточки с магнитной полосой являются дешевыми, но не очень надежными, так как существует вероятность их подделки.

К их недостаткам можно также отнести наличие механического контакта при считывании с головками считывателя, который сокращает срок ее службы (средний срок – около года) и необходимость аккуратного обращения, связанного с возможностью искажения или уничтожения записанной информации в магнитных полях.

Виганд-карта

Карта Виганда (рисунок 3.14) содержит внутри себя отрезки тонких металлических проволочек, расположенных в определенном порядке, представляющем собой кодовую комбинацию.

Рисунок 3.14 – Виганд-карта

Расположение проволочек на карте фиксируется специальным клеем, после этого переориентация проволочек не возможна. При перемещении данной карты в магнитном поле считывателя проволочки создают магнитный импульс, несущий индивидуальную информацию, записанную на карте.

Количество отрезков и расстояние между ними определяет идентификационный код карты. Обычно используются 26 битовые коды, что определяет количество отрезков проволоки в карте.

Информационная емкость такой карты определяет 67108864 возможных комбинаций и практически сводит к нулю вероятность приобретения двух карт с одинаковым номером (теоретически вероятность меньше чем $2x10^{-8}$).

Таким образом, эти карты относятся к уровню повышенной устойчивости по отношению к НСД.

Такой тип карт не подвержен воздействию электромагнитных полей и высоких температур окружающего воздуха. Подделка их практически исключена. Считыватели могут работать вне помещений, так как все их электронные компоненты залиты специальным защитным компаундом.

Недостатком этих карт является то, что они очень хрупкие и могут быть повреждены при изгибе. Кроме того, код каждой карты записывается в нее при изготовлении и не может быть изменен. Стоимость карты и считывателя достаточно высока.

Электронные ключи iButton (Touch Memory)

Термин «Touch Memory» (дословно – «касание памяти») можно перевести как «быстрое считывание памяти при касании» (рисунок 3.15).

Рисунок 3.15 – Электроный ключ Touch Memory

Разработчик американская фирма Dallas Semiconductor гарантирует, что двух «таблеток» в природе не существует. Длина кода данного идентификатора составляет 48 двоичных разрядов. В 1997 году фирма-производитель переименовала свою продукцию – она стала называться iButton (интеллектуальная таблетка), поэтому сейчас можно встретить оба названия.

Идентификаторы Touch Memory представляют собой специализированную микросхему, размещенную в прочном корпусе из нержавеющей стали. Идентификация (распознание) пользователя производится по уникальному (и неизменяемому в течение жизненного цикла) для каждой карты номеру длиной 48 бит (280 триллионов кодовых комбинаций). Индивидуальный код записан на микросхеме памяти, размещенной в стальном цилиндрическом корпусе.

Питание микросхемы и считывание информации производится обычно посредством двух контактов, расположенных на корпусе. Выпускаются идентификаторы с энергонезависимым ОЗУ, гарантированный срок службы которых составляет 10 лет. Малые размеры устройства позволяют оформлять его в виде брелка, кредитной или таксофонной карточки.

Карта бесконтактная (Proximity)

Внутри proximity-карты (рисунок 3.16) расположена микросхема (чип) с записанной в ней информацией (137 миллиардов кодовых комбинаций). Информация, с таких карточек считывается дистанционно радиочастотным способом на расстоянии от 5 до 90 см (для автомобильных идентификаторов данного типа расстояние считывания достигает 2 м).

Иногда этот тип карт обозначают термином «Hands Free» – «руки свободны». Нередко идентификаторы Proximity изготавливают не в виде карточек, а в виде брелоков.

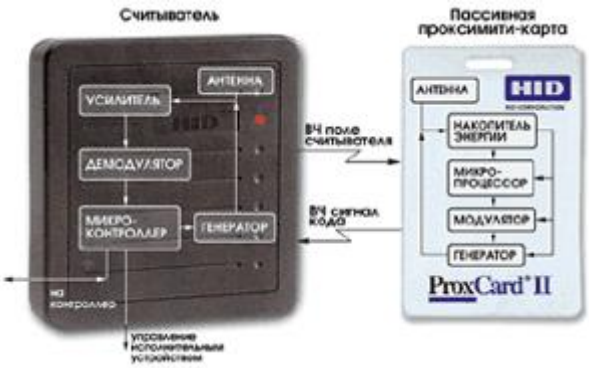

Рисунок 3.16 – Бесконтактная карта

Время считывания информации с карты – не более 0,1 с.

Карты делятся на активные и пассивные. В пассивных картах информация записывается один раз на все время ее действия, а в активных существует возможность вносить изменения информации в микросхеме. Пассивные карты питаются энергией, получаемой от считывателя, срок службы их неограничен и они не могут быть подделаны. Активные – имеют встроенные, незаменяемые батарейки, срок работы которой обычно достаточно велик (до 10 лет).

В надежности эти карты уступают Виганд-картам, но они более удобны в применении. Считыватель может быть скрытно размещен за стеной или в не металлической стене. Эта технология идеально сочетает эффективный контроль со свободой перемещения. Информация с карты может быть считана, даже если она находится в кармане одежды.

Недостатком такой карты является невозможность работы при воздействии сильных электромагнитных полей.

Стоимость пассивных карт составляет 2-8 USD, стоимость считывателя в зависимости от типа составляет 50-1000 USD. Стоимость активных карт приблизительно в 5-10 раз дороже пассивных.

Эта карта незаменима для случаев, когда необходимо обеспечить:

- высокую пропускную способность;
- скрытность места установки считывателя и процесса идентификации;
- дистанционный контроль доступа.

Карты доступа могут быть оформлены в виде пропусков.

Возможно нанесение на такую карту фотографии, названия организации и необходимой информации о владельце (ФИО, должность и др.).

Существует два основных способа оформления карточек:

- цветная печать непосредственно на самой карте;
- применение специальных «паучей».

В «пауч» вкладывается фотография и информация о владельце, он ламинируется, приклеивается к карте, и получается готовый пропуск. При использовании «паучей» возможно переоформление карты на другого сотрудника, например, в случае его увольнения.

Специальное оборудование и программное обеспечение позволяют легко оформлять карты-пропуска непосредственно в бюро пропусков.

Смарт-карта

Смарт-карта (рисунок 3.17) содержит встроенный микропроцессор с энергонезависимой памятью и специальной программой, которая управляет обменом данными со считывателем. Считывание информации в этом случае производится с помощью многоконтактной группы.

Рисунок 3.17 – Смарт-карта

Благодаря возможности реализации сложных алгоритмов шифрования данных, большому объему памяти и высокой защищенности от попыток модификации и копирования, смарт-карты справедливо считаются одними из наиболее перспективных идентификаторов.

Некоторые типы карт используют совмещенный тип записи идентификационных признаков. Например, на proximity-карте может быть размещена магнитная полоса или проволоки Виганда. Это позволяет одновременно решать две задачи:

- повысить защищенность карты от копирования;
- использовать одну и ту же карту в разных СКУД с различными типами считывателей.

3) Биометрические способы

Отдельный класс способов идентификации занимают способы, основанные на предъявлении пользователем СКУД анатомических

особенностей своего организма (предъявление знаний и способностей, отдельных характеристик организма) – биометрические способы (рисунок 3.18).

Рисунок 3.18 – Считывание геометрии ладони

Средства биометрической идентификации подразделяют на динамические и статические. Основное отличие их состоит в том, что устройства динамического контроля принимают решение о допуске предъявителя на основании анализа характеристик и параметров его действий. В этом случае идентификаторами могут быть:

- набор PIN-кода на клавиатуре считывателя (кодовая комбинация);
- набор условной фразы на клавиатуре компьютера (динамика набора и сила нажатия клавиш);
- производство подписи (ее форма и динамика написания);
- произношение установленной фразы (параметры голоса: тембр, полоса спектра и т.п.)

Аутентификация пользователя СКУД осуществляется после программной обработки полученной информации и ее сравнения с шаблоном, представленным в системе.

Устройства статического контроля принимают решение о допуске предъявителя на основании анализа анатомических особенностей его организма (частей). Для этого случая идентификаторами пользователя могут быть:

- форма кисти рук;
- форма лица;
- рисунок кожи пальца;
- рисунок сетчатки глаза;
- рисунок радужной оболочки глаза и др.

Аутентификация пользователя СКУД в устройствах статического контроля осуществляется, как правило, считывание информации производится специальными устройствами на основе видеокамер.

Достоинства:

- полное решение задачи контроля доступа – идентифицируется личность человека, а не какой-либо предмет (карточка);
- идентификатор нельзя подделать и передать другому лицу.

Недостатки:

- высокая цена оборудования точки доступа;
- значительная длительность процедуры аутентификации;
- повышенные требования к конфигурации компьютерной техники и программному обеспечению;
- наличие прямой зависимости допуска от физического состояния предъявителя и др.

В виду перечисленных недостатков эти системы применяются редко и в основном в учреждениях с повышенной секретностью. Для повышения быстродействия биометрического контроля обычно совместно с ним используется другой способ идентификации (набор индивидуального PIN-кода).

Применение PIN-кода – основано на использовании набора цифровых комбинаций на клавиатуре.

Условные обозначения средств и систем контроля и управления доступом

Условное обозначение средств и систем контроля и управления доступом указывают в стандартах и (или) нормативных документах на средства и системы контроля и управления доступом конкретного типа.

Размещение символа условного обозначения средства или системы контроля и управления доступом должно быть частью технической информации и не должно быть совмещено с обозначением торговой марки.

Условное обозначение средств контроля и управления доступом в документации и заказе должно содержать:

1) наименование или сокращенное обозначение устройства (средства) в соответствии с таблицей 3.1;

2) аббревиатуру СКУД;
3) группу символов обозначений;
4) обозначение технических условий.

Таблица 3.1 – Наименование и сокращенное обозначение средств контроля и управления доступом

Наименование средств контроля и управления доступом	**Сокращенное обозначение**
Устройство преграждающее управляемое	УПУ
Устройство исполнительное	УИ
Устройство считывающее (считыватель)	УС
Идентификатор	ИД
Средства управления – аппаратные устройства:	
• контроллер доступа	КД
• ПКП доступа	ППКД
Средства управления – программные: программное обеспечение	ПО

Структура группы символов обозначения для различных средств контроля и управления доступом:

$$\boldsymbol{X_1X_2 - X_3/X_4X_5},$$

где X_1 – классификация по функциональным характеристикам в соответствии с таблицей 3.2;

X_2 – уровень устойчивости к НСД (Н – нормальный, П – повышенный, В – высокий);

X_3 – порядковый номер разработки средства контроля и управления доступом;

X_4 – обозначение конструктивного исполнения;

X_5 – обозначение модернизации, русская прописная буква в алфавитном порядке (первая модернизация – А, вторая – Б и т.д.).

Порядковый номер X_3 регистрируется соответствующим государственным органом, ответственным за проведение технической политики в данной сфере.

Таблица 3.2 – Обозначение классификации по функциональным характеристикам средств контроля и управления доступом

Продолжение таблицы 3.2

Средства контроля и управления доступом по функциональному значению	**Классификация по функциональным характеристикам**	**Обозначение**
УПУ X_1 – по виду перекрытия прохода	С частичным перекрытием (турникеты, шлагбаумы)	1
	С полным перекрытием (полноростовые турникеты, специализированные ворота)	2
	Со сплошным перекрытием проема (сплошные двери, ворота)	3
	С блокированием объекта в проеме (шлюзы, кабины проходные)	4
УИ X_1 – по способу запирания	Электромеханические замки	1
	Электромагнитные замки	2
	Электромагнитные защелки	3
	Механизмы привода ворот	4
УС X_1 – по способу считывания идентификационных признаков	С ручным вводом	1
	Контактные	2
	Бесконтактные	3
	Биометрические	4
	Комбинированные	5
ИД X_1 – по виду идентификационных признаков	Механические	1
	Магнитные	2
	Оптические	3
	Электронные контактные	4
	Электронные радиочастотные	5
	Акустические	6
	Комбинированные	7
КД, ППКД X_1 – по способу управления	Автономный	1
	Централизованный	2
	Универсальный	3

Пример условного обозначения идентификатора контроля и управления доступом электронного радиочастотного, нормальной устойчивости к НСД, порядкового номера разработки 5, конструктивного исполнения 8, модификации А (приводится обозначение технических условий):

ИД СКУД 5Н - 5/8А ТУ

Условное обозначение СКУД в документации и при заказе должно состоять из:

1) Наименования «Система контроля и управления доступом» или сокращенно «СКУД».
2) Группы символов.
3) Обозначения технических условий.

Структура группы символов обозначения СКУД:

$$X_1X_2X_3X_4 - X_5/X_6X_7 ,$$

где X_1 – способ управления (1 – автономное, 2 – централизованное (сетевое); 3 – универсальное (сетевое);

X_2 – число контролируемых точек доступа (1 – система малой емкости, 2 – система средней емкости, 3 – система большой емкости);

X_3 – класс по функциональным характеристикам;

X_4 – класс защищенности системы от НСД к информации для систем повышенной и высокой устойчивости к НСД или буква «Н» для систем нормальной устойчивости;

X_5 – порядковый номер разработки;

X_6 – обозначение конструктивного исполнения;

X_7 – обозначение модернизации (обозначается русской прописной буквой в алфавитном порядке, первая модернизация – А, вторая – Б и т.д.).

Порядковый номер X_5 регистрируется соответствующим государственным органом, ответственным за проведение технической политики в данной сфере.

Пример условного обозначения СКУД сетевой, малой емкости, второго класса по функциональным возможностям, нормальной устойчивости к НСД, номера разработки 7, конструктивного исполнения 9, модернизации Б (приводится обозначение технических условий):

СКУД - 212Н-7/9Б ТУ