Белорусский государственный университет информатики и радиоэлектроники

Кафедра РЭС

РЕФЕРАТ

На тему:

"Общие требования и основные компоненты СКУД"

МИНСК, 2008

## Общие требования к СКУД. Требования к автономным СКУД

Автономные системы определяются как "системы для управления одним или несколькими УПУ без передачи информации на центральный пульт и без контроля со стороны оператора".

Общие требования ко всем автономным системам, а также автономным системам 1-го класса по функциональным характеристикам следующие:

* открывание УПУ при считывании зарегистрированного идентификационного признака;
* запрет открывания при считывании незарегистрированного идентификационного признака;
* запись идентификационных признаков в память системы;
* защита от НСД при записи кодов идентификационных признаков в память системы;
* сохранение признаков в памяти при отказе электропитания;
* ручное, полуавтоматическое или автоматическое открывание УПУ при аварийных ситуациях;
* автоматическое формирование сигнала сброса на УПУ при отсутствии факта прохода;
* выдача сигнала тревоги при использовании системы аварийного открывания для несанкционированного проникновения.

Для 2-го класса автономных систем дополнительно вводятся следующие обязательные требования:

* световая идентификация о состоянии доступа;
* контроль состояния УПУ;
* регистрация и хранение информации о событиях в энергонезависимой памяти, с количеством событий не менее 16.

Для 3-го и 4-го класса обязательны следующие требования (добавляются к уже перечисленным):

* установка уровней доступа;
* установка временных интервалов доступа;
* возможность установки времени открывания УПУ;
* защита от повторного использования идентификаторов для прохода в одном направлении;
* ввод идентификационного признака для открывания под принуждением;
* световое и (или) звуковое оповещение о попытках НСД;
* регистрация и хранение информации о событиях в энергонезависимой памяти, с количеством событий не менее 64;
* введение даты и времени возникновения событий;
* возможность подключения принтера для вывода информации;
* возможность передачи информации на устройства сбора информации или ЭВМ;
* возможность объединения в сеть и обмена информацией с ЭВМ;
* возможность интегрирования на релейном уровне с охранной, пожарной системами или системой видеоконтроля;
* световая индикация состояния доступа.

Основные компоненты СКУД

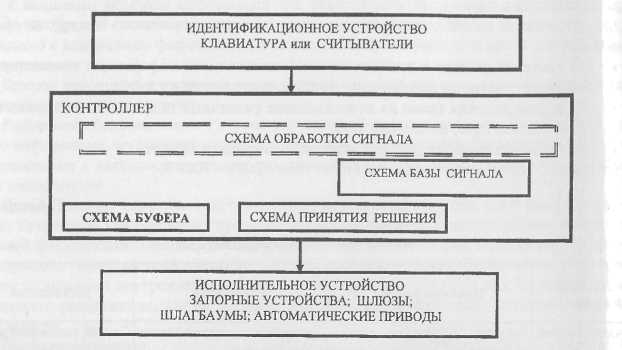


Рис.9.4. Простейшая структура системы контроля и управления доступом

## Идентификационное устройство

Термин идентификация означает - опознавание, поиск по признаку. Идентификация производится по следующим основным принципам:

- по запоминаемому коду, вводимому вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств;

- по вещественному коду - по коду, записанному на физическом носителе (идентификаторе);

- биометрическая идентификация - идентификация, основанная на определении индивидуальных физических признаков личности.

Идентификатор - предмет, в который (на который) с помощью специальной технологии занесена кодовая информация, подтверждающая полномочность прав его владельца, и служащий для управления доступом в охраняемую зону. Идентификаторы могут быть изготовлены в виде карточек, ключей, брелоков и т.п.

Устройства идентификации доступа (идентификаторы и считыватели) считывают и расшифровывают информацию, записанную на идентификаторах соответствующего типа, и устанавливают права людей, имущества, транспорта на перемещение в охраняемой зоне (объекте).

Контролируемые места, где непосредственно осуществляется контроль доступа, например, дверь, турникет, кабина прохода, оборудуются считывателем, устройством исполнительным и другими необходимыми средствами.

Считыватель - электронное устройство, предназначенное для считывания кодовой информации идентификатора и преобразования ее в стандартный формат, передаваемый для анализа и принятия решения в контроллер.

Устройства идентификации доступа (считыватели, идентификаторы) классифицируются по следующим признакам:

- по виду используемых идентификационных признаков;

- по способу считывания идентификационных признаков.

По виду используемых идентификационных признаков устройства идентификации могут быть:

* механические - идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
* магнитные - идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганта и т.д.);
* оптические - идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки);
* электронные - идентификационные признаки представляют собой кодированный электрический, акустический, оптический или радиосигнал;
* биометрические - идентификационные признаки 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.

По способу считывания идентификационных признаков устройства идентификации могут быть:

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

## Идентификация по запоминаемому коду

В качестве считывателей в этом случае чаше всего используется цифровая или алфавитно-цифровая клавиатура (PIN-код - Personal Identification Number). Определение пользователя происходит путем набора персонального кода - последовательности цифр - на клавиатуре кодонаборной панели. Примеры исполнения кодонаборных клавиатур приведены на рис.1. Обычно данный способ идентификации используется также в комбинациях с другими, для повышения надежности систем.

Клавиатурные считыватели, хотя и считаются недостаточно защищенными от манипуляций (подбор кода, наблюдение), имеют определенные достоинства, например, разрядность кода может быть выбрана произвольно, код может устанавливаться самим пользователем и произвольно им изменяться, быть неизвестным оператору системы.

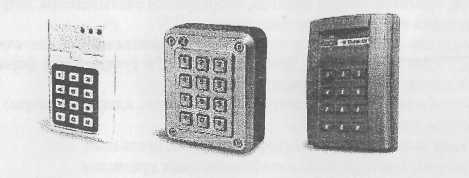


Рис.1. Внешний вид некоторых типов кодонаборных клавиатур

Для исключения возможности подсматривания набираемого кода американская фирма "Hirsch" разработала особую клавиатуру ScramblePad. Она содержит сразу несколько оригинальных технических решений. Во-первых, клавиатура устроена так, что при каждом включении расположение цифр на панели принимает случайный порядок. Во-вторых, угол, в пределах которого видны светящиеся цифры, ограничен. Рассмотреть, какой код набирается на клавиатуре, в данном случае практически невозможно.

## Идентификация по вещественному коду

В настоящее время наибольшее распространение получили СКУД, использующие идентификацию по вещественному коду.

Карточка перфорированная - карточка из двухслойной недеформируемой пластмассы. Информация записывается на ней с помощью пробивки специальных отверстий один раз при изготовлении. Считывание информации осуществляется оптическим или механическим считывателем. Данная карточка является самым простым и дешевым типом идентификатора, однако на практике не обеспечивает секретность кода и легко подделывается.

Срок службы карточки 1-2 года. Механический считыватель перфорированных карточек очень капризен в эксплуатации.

Карточка со штрих-кодом (Barcode Card). В идентификаторах данного класса используется штриховой код. Штрих-код представляет собой группу параллельных линий темного цвета (гораздо темнее чем остальная поверхность) различной ширины, которые наносятся на поверхность карты. Ширина и расстояние между полосками представляют собой кодовую последовательность.

Код карты считывается сканером. При сканировании карточка не контактирует со считывателем физически. Поэтому, считыватель надежен в работе. Карточка со штриховым кодом может быть пропущена через считыватель в любом направлении.

Данная технология обладает низким уровнем секретности, поскольку штрих-код можно легко скопировать. Срок использования карт со штрих-кодом составляет от 18 до 30 месяцев.

Для повышения защищенности карт со штрих-кодом используют ИК считывание. При этом поверхность карты покрывают особой пленкой, непрозрачной в видимом диапазоне, скрывающей штрих-код от человеческих глаз.

Карточка магнитная (Magnetic Stripe Card, Mag-stripe Card). Часто используются в системах контроля доступа. Цифровые магнитные коды широко применяются в коммерческих кредитных карточках (VISA, STB-card).

Двоичный код наносится на полоску магнитного материала, расположенную параллельно краям карточки. Данные считываются при перемещении карточки вдоль считывающей головки регистрирующего устройства. Не все магнитные карточки и считыватели совместимы, хотя способ записи информации стандартизирован международным стандартом ISO. Согласно указанному стандарту на магнитной полосе может находиться от 1 до 3 дорожек записи, причем положение дорожек, их ширина и глубина строго регламентируются.

В области СКУД и банковских технологий принято использовать вторую дорожку.

К недостаткам карт с магнитной полосой следует отнести:

* возможность изменения кода на карте, тем самым защищенность от несанкционированного доступа невелика;
* системы с магнитными считывателями капризны в эксплуатации, т. к. магнитные головки со временем засоряются и смещаются;
* карты требуют бережного хранения, т. к. магнитная полоса на карте боится действия электромагнитных полей (всю информацию на карте можно стереть, оставив карту недалеко от источника электромагнитного излучения), карта не защищена от механического воздействия;
* быстрый износ карты из-за частых контактов со считывателем (срок службы 1 год);
* малая пропускная способность систем, так как в случае износа магнитной головки, ее засорения или сдвига приходится несколько раз проводить магнитной картой по считывателю, что задерживает поток людей.

Однако для многих пользователей низкая цена считывателей и карт является привлекательным моментом при выборе технологии считывания кода.

Эту технологию рекомендуется использовать при следующих условиях:

* низкий и средний уровень безопасности;
* большое количество используемых карт;
* пользователь хочет использовать уже существующие карты (например, карты учета рабочего времени, кредитные карты) для контроля доступа.

Виганд-карточка (Wiegand). Данная технология была разработана для создания карт не чувствительных к внешним магнитным полям.

Американский ученый John R. Weigand обнаружил, что при наличии магнитного поля сверхкороткие проводники определенного состава вызывают гигантский индукционный отклик в индуктивной катушке. Причем, если магнитное поле направлено в одну сторону, то имеется большой положительный выброс, а в другую - большой отрицательный выброс индукционного тока. Сплав, найденный ученым, имеет практически идеально прямоугольную петлю гистерезиса.

В структуру пластиковой карты вплетены две полоски сверхкоротких проводников (рис.2), расположенных в строго определенной последовательности (различной для разных карт), которые и содержат информацию о персональном коде ее владельца.



Рис.2 Карта Виганда

Считыватель представляет собой индукционную катушку с двумя магнитами противоположной полярности. Когда карта перемещается вдоль считывателя, один магнит детектирует проволочки из одного ряда, а второй из другого. Один ряд дает положительные всплески индукционного тока, которые трактуются как "1", а второй - отрицательные, которые трактуются как "0", т.е. считывается бинарный код карты. Считывание ведется бесконтактным способом.

К основным достоинствам Виганд-карточек можно отнести: высокую надежность; высокую износостойкость; неподверженность электромагнитному излучению и высоким температурам окружающего воздуха; высокую защищенность от подделок (состав сплава хранится в секрете, права на изобретение принадлежат компании); считыватели могут работать вне помещений, так как все их электронные компоненты залиты специальным защитным компаундом.

Недостатком является то, что карточки хрупкие и могут быть повреждены при изгибе. Кроме того, код каждой карточки записывается в нее при изготовлении и не может быть изменен.

В настоящее время Виганд-карточки - один из самых перспективных типов идентификаторов.

## ЛИТЕРАТУРА

1. Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с.
2. Ярочкин В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.
3. Барсуков В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.
4. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия – Телеком, 2000. - 452 с., ил
5. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.] ; под общ. Ред. А.П. Леонова. – Минск: АРИЛ, 2000. – 552 с.