УТВЕРЖДАЮ

Директор ЧУДПО «Ферт-Профи»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Важинская

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2014 г.

ПЛАН – КОНСПЕКТ

проведения занятий по дисциплине «Организация охранных услуг с применением технических средств» повышения квалификации руководителей частных охранных организаций

Тема № 4 «**Системы управления техническими средствами охраны**»

Цель занятия: изучить классификацию систем управления техническими средствами охраны.

Время проведения: 0,5 часа

Метод проведения: лекция

Место проведения: учебный класс

Используемая литература:

1. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. ГОСТ Р 51241-98
2. Выбор и применение систем контроля и управления доступом. Рекомендации. [Р 78.36.005-99](http://bestpravo.ru/rossijskoje/ys-dokumenty/y0o.htm).
3. Организационный момент -5 мин:

Проверка слушателей.

Объявление темы и цели занятия

П. Основная часть – 20 мин.

Объяснение нового материала:

1. Классификация систем управления техническими средствами охраны.
2. Система контроля и правления доступом.

Ш. Заключительная часть – 5 мин

Закрепление нового материала

Задание для самостоятельного изучения.

|  |  |
| --- | --- |
|  |  |
|  |

**Классификация средств контроля и управления доступом**

Средства КУД классифицируют по:

- функциональному назначению устройств;

- устойчивости к НСД.

Средства КУД по функциональному назначению устройств подразделяют на:

- устройства преграждающие управляемые (УПУ) в составе преграждающих конструкций и исполнительных устройств;

- устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;

- устройства управления (УУ) в составе аппаратных и программных средств.

4.1.3. УПУ классифицируют по виду перекрытия проема прохода и по способу управления.

По виду перекрытия проема прохода УПУ могут быть:

- с частичным перекрытием (турникеты, шлагбаумы);

- с полным перекрытием (сплошные двери, ворота);

- с блокированием объекта в проеме (шлюзы, кабины проходные).

По способу управления УПУ могут быть:

- с ручным управлением;

- с полуавтоматическим управлением,

- с автоматическим управлением.

4.1.4. УВИП классифицируют по следующим признакам:

- по виду используемых идентификационных признаков;

- по способу считывания идентификационных признаков.

По виду используемых идентификационных признаков УВИП 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 Виганда 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 и т. д.);

- электронные - идентификационные признаки представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т. д.);

- акустические - идентификационные признаки представляют собой кодированный акустический сигнал;

- 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 УВИП могут быть:

- 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;

- дистанционные (бесконтактные) - считывание кода происходит при поднесении идентификатора на определенное расстояние к считывателю;

- комбинированные.

4.1.5. Классификацию УУ, включающих аппаратные, программные и программно-аппаратные средства, проводят в составе систем КУД.

4.1.6. Средства КУД к информации представляют собой программные, технические и программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации.

К этим средствам относятся также специальные защитные знаки (СЗЗ). СЗЗ представляют собой продукты, созданные на основе физико-химических технологий и предназначенные для контроля доступа к объектам защиты, а также для защиты документов, идентифицирующих личность, от подделки.

**4.2. Классификация систем КУД**

4.2.1. Системы КУД классифицируют по:

- способу управления;

- количеству контролируемых точек доступа;

- функциональным характеристикам;

- виду объектов контроля;

- уровню защищенности системы от несанкционированного доступа к информации.

4.2.2. По способу управления системы КУД могут быть:

- автономные -для управления одним или несколькими УПУ без передачи информации на центральный пульт и без контроля со стороны оператора;

- централизованные (сетевые) -для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны оператора;

- универсальные - 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.

4.2.3. По количеству контролируемых точек доступа системы КУД могут быть:

- малой емкости (менее 16 точек);

- средней емкости (не менее 16 и не более 64 точек);

- большой емкости (64 точки и более).

4.2.4. По функциональным характеристикам системы КУД могут быть трех классов:  
  
1 - системы с ограниченными функциями;

2 - системы с расширенными функциями;

3 - многофункциональные системы.

В системы любого класса могут быть введены специальные функции, которые определяются дополнительными требованиями заказчика.

4.2.5 По виду объектов контроля системы КУД могут быть:

- для контроля доступа физических объектов;

- для контроля доступа к информации.

**4.3. Классификация средств и систем КУД по устойчивости к НСД**

4.3.1. Средства КУД классифицируют по устойчивости к НСД, которая определяется устойчивостью к разрушающим и неразрушающим воздействиям по трем уровням устойчивости:

- нормальной;

- повышенной;

- высокой.

4.3.2. УПУ и УВИП классифицируют по устойчивости к разрушающим воздействиям. Устойчивость УПУ устанавливают по:

- устойчивости к взлому;

- пулестойкости;

- устойчивости к взрыву.

Устойчивость УВИП устанавливают по устойчивости считывателя к взлому. Для УПУ повышенной и высокой устойчивости устанавливают дополнительно 5 классов по показателям устойчивости (1-й класс - низший).

4.3.3. По устойчивости к неразрушающим воздействиям средства и системы КУД 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 УВИП с запоминаемым кодом (клавиатуры, кодовые переключатели и т.п.);

- устойчивости к копированию (для идентификаторов);

- устойчивости защиты средств вычислительной техники УУ от несанкционированного доступа к информации.

4.3.4. Классификация по устойчивости к вскрытию, манипулированию, наблюдению, копированию должна быть указана в стандартах и других нормативных документах на средства КУД конкретного типа.

4.3.5. Класс защищенности от несанкционированного доступа к информации должен быть указан в нормативных документах на средства или системы КУД конкретного типа.

4.3.6. Классификацию систем КУД по защищенности от несанкционированного доступа к информации проводят по таблице А.1 приложения А.

4.3.7. Классификацию средств КУД по устойчивости от несанкционированного доступа к информации проводят по таблице Б.1 приложения Б.

**СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ**

7.1. Система контроля и управления доступом (СКУД) предназначена для:

обеспечения санкционированного входа в здание и в зоны ограниченного доступа и выход из них путем идентификации личности по комбинации различных признаков: вещественный код (виганд-карточки, ключи touch-memory и другие устройства), запоминаемый код (клавиатуры, кодонаборные панели и другие устройства), биометрические признаки (отпечатки пальцев, сетчатка глаз и другие признаки);

предотвращения несанкционированного прохода в помещения и зоны ограниченного доступа объекта.

7.2. Согласно ГОСТ Р 51241-98 СКУД должна состоять из:

устройств преграждающих управляемых (УПУ) в составе преграждающих конструкций и исполнительных устройств;

устройств ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;

устройств управления (УУ) в составе аппаратных и программных средств.

7.3. Считывателями и УПУ следует оборудовать:

главный и служебные входы;

КПП;

помещения, в которых непосредственно сосредоточены материальные ценности;

помещения руководства;

другие помещения по решению руководства объекта.

7.4. Пропуск сотрудников и посетителей на объект через пункты контроля доступа следует осуществлять:

в здание и в служебные помещения - по одному признаку;

входы в зоны ограниченного доступа (хранилища ценностей, сейфовые комнаты, комнаты хранения оружия) - не менее чем по двум признакам идентификации.

7.5. СКУД должна обеспечивать выполнение следующих основных функций:

открывание УПУ при считывании идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение) в заданный временной интервал или по команде оператора СКУД;

запрет открывания УПУ при считывании идентификационного признака, доступ по которому не разрешен в данную зону доступа (помещение) в заданный временной интервал;

санкционированное изменение (добавление, удаление) идентификационных признаков в УУ и связь их с зонами доступа (помещениями) и временными интервалами доступа;

защиту от несанкционированного доступа к программным средствам УУ для изменения (добавления, удаления) идентификационных признаков;

защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;

сохранение настроек и базы данных идентификационных признаков при отключении электропитания;

ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;

автоматическое закрытие УПУ при отсутствии факта прохода через определенное время после считывания разрешенного идентификационного признака;

выдачу сигнала тревоги (или блокировку УПУ на определенное время) при попытках подбора идентификационных признаков (кода);

регистрацию и протоколирование текущих и тревожных событий;

автономную работу считывателя с УПУ в каждой точке доступа при отказе связи с УУ.

7.6. На объектах, где необходим контроль сохранности предметов, следует устанавливать СКУД, контролирующие несанкционированный вынос данных предметов из охраняемых помещений или зданий по специальным идентификационным меткам.

7.7. УПУ с устройствами исполнительными должно обеспечивать:

частичное или полное перекрытие проема прохода;

автоматическое и ручное (в аварийных ситуациях) открывание;

блокирование человека внутри УПУ (для шлюзов, проходных кабин);

требуемую пропускную способность.

7.8. Считыватели УВИП должны обеспечивать:

считывание идентификационного признака с идентификаторов;

сравнение введенного идентификационного признака с хранящимся в памяти или базе данных УУ;

формирование сигнала на открывание УПУ при идентификации пользователя;

обмен информацией с УУ.

УВИП должны быть защищены от манипулирования путем перебора или подбора идентификационных признаков.

Идентификаторы УВИП должны обеспечить хранение идентификационного признака в течение:

всего срока эксплуатации - для идентификаторов без встроенных элементов электропитания;

не менее 3 лет - для идентификаторов со встроенными элементами электропитания.

Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.

7.9. УУ должно обеспечивать:

прием информации от УВИП, ее обработку, отображение в заданном виде и выработку сигналов управления УПУ;

ведение баз данных сотрудников и посетителей объекта с возможностью задания характеристик их доступа (кода, временного интервала доступа, уровня доступа и другие);

ведение электронного журнала регистрации проходов сотрудников и посетителей через точки доступа;

приоритетный вывод информации о тревожных ситуациях в точках доступа;

контроль исправности и состояния УПУ, УВИП и линий связи с ними.

7.10. Конструктивно СКУД должны строиться по модульному принципу и обеспечивать:

взаимозаменяемость сменных однотипных технических средств;

удобство технического обслуживания и эксплуатации, а также ремонтопригодность;

исключение возможности несанкционированного доступа к элементам управления;

санкционированный доступ ко всем элементам, узлам и блокам, требующим регулирования, обслуживания или замены в процессе эксплуатации.

7.11. Выбор оборудования СКУД, места его установки на объекте следует проводить в соответствии с [Р 78.36.005-99](http://bestpravo.ru/rossijskoje/ys-dokumenty/y0o.htm).