**ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

В настоящем стандарте применяют следующие термины с соответствующими определениями:   
**Доступ**- перемещение людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.   
**Несанкционированный доступ** - доступ людей или объектов, не имеющих права доступа.   
**Санкционированный доступ** - доступ людей или объектов, имеющих права доступа.   
**Контроль и управление доступом (КУД)** - комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.   
**Средства контроля и управления доступом (средства КУД)** - механические, электромеханические, электрические, электронные устройства, конструкции и программные средства, обеспечивающие реализацию контроля и управления доступом.   
**Система контроля и управления доступом (СКУД)** - совокупность средств контроля и управления. обладающих технической, информационной, программной и эксплуатационной совместимостью.   
**Идентификация** - процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимается также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.   
**Биометрическая идентификация** - идентификация, основанная на использовании индивидуальных физических признаков человека.   
**Идентификатор доступа, идентификатор (носитель идентификационного признака)** - уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код Идентификатор, использующий вещественный код - предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и т. д.).   
**Вещественный код** - код, записанный на физическом носителе (идентификаторе).   
**Запоминаемый код** - код, вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.   
**Устройства преграждающие управляемые (УПУ)**- устройства, обеспечивающие физическое препятствие доступу людей, транспорта и других объектов и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т. п. конструкции).   
**Устройства исполнительные** - устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические и электромагнитные замки, защелки, механизмы привода шлюзов, ворот, турникетов и т. д.).   
**Устройства ввода идентификационных признаков (УВИП)**- электронные устройства, предназначенные для ввода запоминаемого кода, ввода биометрической информации, считывания кодовой информации с идентификаторов. В состав УВИП входят считыватели и идентификаторы.   
**Считыватель** - устройство в составе УВИП, предназначенное для считывания (ввода) идентификационных признаков.   
**Устройства управления (УУ)** - устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с УВИП, управление УПУ, отображение и регистрацию информации.   
**Точка доступа** - место, где непосредственно осуществляется контроль доступа (например дверь, турникет, кабина прохода, оборудованные считывателем, исполнительным механизмом, электромеханическим замком и другими необходимыми средствами).   
**Зона доступа**- совокупность точек доступа, связанных общим местоположением или другими характеристиками (например точки доступа, расположенные на одном этаже).   
**Временной интервал доступа (окно времени)** - интервал времени, в течение которого разрешается перемещение в данной точке доступа.   
**Уровень доступа**- совокупность временных интервалов доступа (окон времени) и точек доступа, которые назначаются определенному лицу или группе лиц, имеющим доступ в заданные точки доступа в заданные временные интервалы.   
**Правило двух (и более) лиц** - правило доступа, при котором доступ разрешен только при одновременном присутствии двух или более людей.   
**Пропускная способность**- способность средства или системы КУД пропускать определенное количество людей, транспортных средств и т.п. в единицу времени.   
**Несанкционированные действия (НСД)** - действия, целью которых является несанкционированное проникновение через УПУ.   
**Взлом**-действия, направленные на несанкционированное разрушение конструкции.   
**Вскрытие**- действия, направленные на несанкционированное проникновение через УПУ без его разрушения.   
**Манипулирование**- действия, производимые с устройствами контроля доступа без их разрушения, целью которых является получение действующего кода или приведение в открытое состояние заграждающего устройства. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия не будут заметны. Манипулирование включает в себя также действия над программным обеспечением.   
**Наблюдение**- действия, производимые с устройствами контроля и управления доступом без прямого доступа к ним, целью которых является получение действующего кода.   
**Копирование**- действия, производимые с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.   
**Принуждение**- насильственные действия над лицом, имеющим право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.   
**Саботаж**(состояние саботажа - по ГОСТ Р 50776) - преднамеренно созданное состояние системы, при котором происходит повреждение части системы.   
**Устойчивость к взлому** - способность конструкции противостоять разрушающему воздействию без использования инструментов, а также с помощью ручных и других типов инструментов.   
**Пулестойкость** - способность преграды противостоять сквозному пробиванию пулями и отсутствие при этом опасных для человека вторичных поражающих элементов.   
**Устойчивость к взрыву** - способность конструкции противостоять разрушающему действию взрывчатых веществ.

**КЛАССИФИКАЦИЯ**

**4.1. Классификация средств КУД**   
**4.1.1.** Средства КУД классифицируют по: 

* функциональному назначению устройств;
* устойчивости к НСД.

**4.1.2.**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 [I].   
К этим средствам относятся также специальные защитные знаки (СЗЗ) [2]. 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.   
  
**4.4. Условные обозначения средств и систем КУД**   
**4.4.1.** Условные обозначения средств и систем КУД указывают в стандартах и (или) нормативных документах на средства и системы КУД конкретного типа.   
Размещение символа условного обозначения должно быть частью технической информации и не должно быть совмещено с обозначением торговой марки.   
**4.4.2.**Условное обозначение систем КУД в документации и при заказе должно содержать:

а) название "Система";   
б) название класса системы по количеству контролируемых точек доступа и по способу управления;   
в) обозначение КУД;   
г) три символа (первый и второй с точкой), обозначающие:

класс системы по функциональным возможностям;   
степень жесткости по устойчивости к электромагнитным помехам;   
класс защищенности системы от несанкционированного доступа к информации для систем повышенной и высокой устойчивости к НСД или буква "Н" для систем нормальной устойчивости;

д) обозначение настоящего стандарта;   
е) условное обозначение по нормативной документации изготовителя или поставщика.

*Пример условного обозначения системы сетевой малой емкости второго класса по функциональным возможностям, первой категории по устойчивости к электромагнитным помехам и класса ЗА по защищенности системы от несанкционированного доступа к информации:*

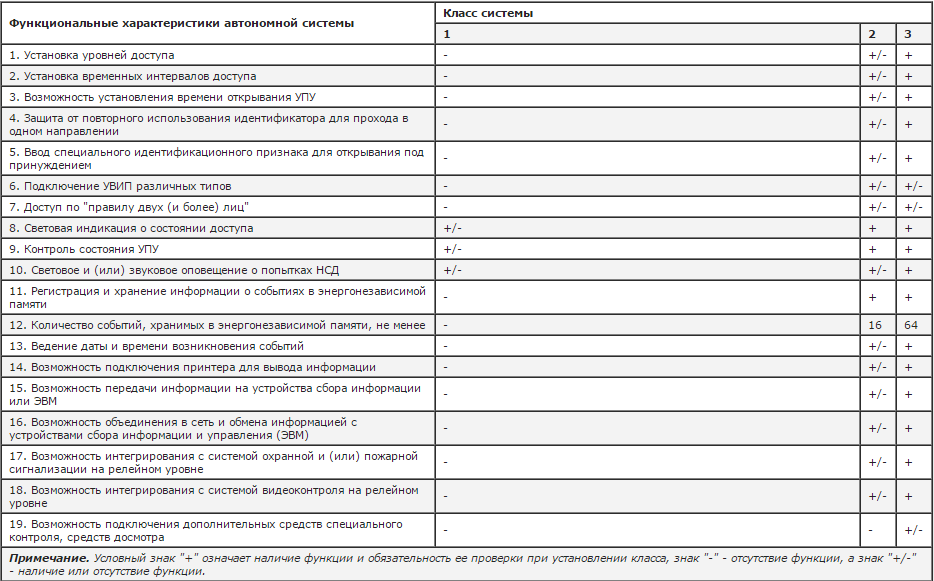
Система малой емкости сетевая **КУД-2.1. Н ГОСТ Р ХКХХХ АБВГ.ХХХХХ ТУ**

**ОБЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**5.1. Общие положения**   
**5.1.1.** Средства и системы КУД должны изготовляться в соответствии с требованиями настоящего стандарта, ГОСТ Р 50775, а также стандартов и других нормативных документов на средства и системы КУД конкретного типа.   
**5.1.2.**Средства и системы КУД должны обеспечивать возможность как круглосуточной, так и сменной работы, с учетом проведения регламентного технического обслуживания.   
**5.1.3.** Средства КУД, предназначенные для построения систем, должны обладать конструктивной, информационной, надежностной и эксплуатационной совместимостью.   
Параметры и требования, определяющие совместимость средств, должны быть установлены в зависимости от назначения и условий применения в нормативных документах на средства и системы КУД конкретного типа.   
**5.1.4.**Требования к средствам контроля доступа вида-специальные защитные знаки (СЗЗ) устанавливают по документу [2].   
  
**5.2. Требования назначения**   
**5.2.1.**Требования к функциональным характеристикам систем КУД   
5.2.1.1. Автономные системы КУД должны обеспечивать: 

* открывание УПУ при считывании зарегистрированного в памяти системы идентификационного признака;
* запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака;
* запись идентификационных признаков в память системы;
* защиту от несанкционированного доступа при записи кодов идентификационных признаков в памяти системы;
* сохранение идентификационных признаков в памяти системы при отказе и 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 формирование сигнала сброса на УПУ при отсутствии факта прохода;
* выдачу сигнала тревоги при использовании системы аварийного открывания УПУ для несанкционированного проникновения.

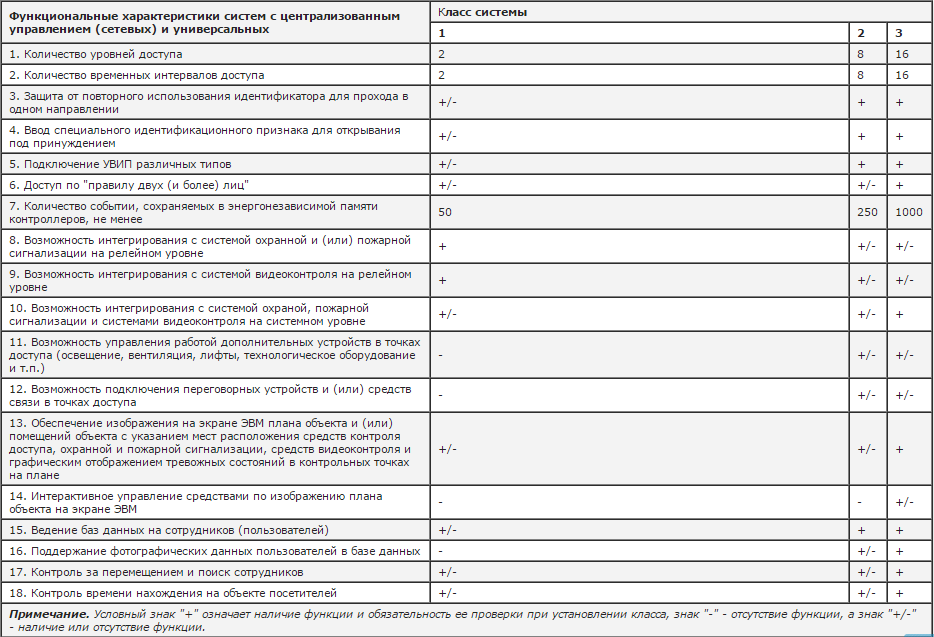
5.2.1.2. Дополнительные характеристики автономных систем в зависимости от класса по функциональным характеристикам приведены в таблице 1.

Функциональные характеристики автономных систем

5.2.1.3. Системы КУД с централизованным управлением и универсальные должны соответствовать требованиям 5.2.1 и дополнительно обеспечивать: 

* регистрацию и протоколирование тревожных и текущих событий;
* приоритетное отображение тревожных событий;
* управление работой УПУ в точках доступа по командам оператора;
* задание временных режимов действия идентификаторов в точках доступа "окна времени" и уровней доступа;
* защиту технических и программных средств от несанкционированного доступа к элементам управления, установки режимов и к информации;
* автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
* возможность автономной работы контроллеров системы с сохранением контроллерами основных функций при отказе связи с пунктом централизованного управления;
* установку режима свободного доступа с пункта управления при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т.п.);
* блокировку прохода по точкам доступа командой с пункта управления в случае нападения;
* возможность подключения дополнительных средств специального контроля, средств досмотра.

5.2.1.4. Дополнительные характеристики систем с централизованным управлением, в зависимости от класса по функциональным характеристикам, приведены в таблице 2.

Функциональные характеристики систем с централизованным управлением и универсальных

5.2.1.5. Универсальные системы должны обеспечивать автономную работу при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи, а также восстановление режимов работы после устранения отказов и восстановлении связи.   
5.2.1.6. Значения характеристик и требования, приведенные в 5.2.1.1-5.2.1.5, должны быть установлены в стандартах и (или) технических условиях на системы КУД конкретного типа.   
Системы КУД должны также иметь следующие характеристики, значения которых должны быть установлены в стандартах и (или) технических условиях на системы конкретного типа: 

* максимальное количество точек доступа, зон доступа, пользователей, обслуживаемых системой;
* максимальное количество точек доступа, обслуживаемых одним УУ;
* количество и вид временных интервалов доступа (окон времени), уровней доступа;
* количество видов УВИП, используемых в системе;
* время реакции системы на заявку на проход;
* максимальное расстояние от наиболее удаленной точки доступа до пункта управления;
* максимальное расстояние действия считывателя (для бесконтактных считывателей);
* максимальное время хранения информации о событиях в памяти системы;
* максимальная пропускная способность системы в точках доступа;
* вероятность несанкционированного доступа, вероятность ложного задержания (требования обязательны для СКУД с биометрической идентификацией, для остальных допускается не указывать);
* показатели по уровням устойчивости к НСД.

5.2.1.7. По требованиям заказчика допускается устанавливать дополнительные характеристики и показатели в технических условиях на системы конкретного типа.   
  
**5.2.2.** Требования к функциональным характеристикам УПУ   
5.2.2.1. УПУ должны обеспечивать: 

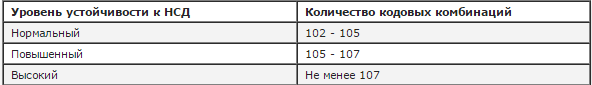
* полное или частичное перекрытие проема прохода;
* ручное, полуавтоматическое или автоматическое управление;
* блокирование человека или объекта для УПУ блокирующего типа.

5.2.2.2. УПУ в дежурном режиме могут быть в нормально открытом или нормально закрытом состоянии.   
УПУ с частичным перекрытием проема прохода могут быть, при необходимости, обеспечены средствами сигнализации, срабатывающими при попытке обхода заграждающего устройства.   
Для УПУ, используемых на проходных или в других местах с большими потоками людей, в стандартах или технических условиях на УПУ конкретного типа должны быть установлены показатели пропускной способности.   
5.2.2.3. УПУ в закрытом состоянии должны обеспечивать физическое препятствие перемещению людей, транспорта и других объектов в (из) помещение, здание, зону или на территорию и открывание запирающего механизма при подаче управляющего сигнала от устройства управления.   
Параметры управляющего сигнала (напряжение, ток и длительность) должны быть указаны в стандартах и (или) нормативных документах на УПУ конкретного типа.   
Нормально закрытые УПУ могут быть оборудованы средствами звуковой сигнализации, которая включается после их открывания и при отсутствии прохода в течение установленного времени, или могут иметь средства для возврата в закрытое состояние.   
5.2.2.4. УПУ при необходимости могут иметь защиту от прохода через них одновременно двух или более человек.   
5.2.2.5. УПУ должны иметь возможность механического аварийного открывания в случае пропадания электропитания, возникновения пожара или других стихийных бедствий. Аварийная система открывания должна быть защищена от возможности использования ее для несанкционированного проникновения.   
5.2.2.6. Умышленное повреждение внешних электрических соединительных цепей и элементов блокировки не должно приводить к открыванию УПУ.   
Должны быть предусмотрены меры по защите внешних электрических соединительных цепей от возможности подачи по ним напряжений, приводящих к нарушению работы или к открыванию УПУ.   
5.2.2.7. УПУ могут иметь дополнительно средства специального контроля, встроенные или совместно функционирующие. Требования к УПУ, в состав которых входят средства специального контроля, устанавливаются в нормативных документах на устройства конкретного типа.   
  
**5.2.3.**Требования к функциональным характеристикам УВИП   
5.2.3.1. Считыватели УВИП должны обеспечивать: 

* возможность считывания идентификационного признака с идентификаторов;
* введение биометрической информации (для считывателей биометрической информации);
* преобразование введенной информации в электрический сигнал;
* передачу информации на УУ.

5.2.3.2. УВИП должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды защиты должны быть указаны в стандартах и (или) нормативных документах на УВИП конкретного типа.   
5.2.3.3. Идентификаторы УВИП должны обеспечивать хранение идентификационного признака в течение срока службы и при эксплуатации.   
5.2.3.4. Конструкция, внешний вид и надписи на идентификаторе и считывателе не должны приводить к раскрытию применяемых кодов.   
5.2.3.5. Производитель идентификаторов должен гарантировать, что код данного идентификатора не повторится, или указать условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами.   
5.2.3.6. Считыватели УВИП при взломе и вскрытии, а также в случае обрыва или короткого замыкания подходящих к ним цепей не должны вызывать открывание УПУ. При этом автономные системы могут выдавать звуковой сигнал тревоги, а системы с централизованным управлением сигнал тревоги могут передавать на пункт управления и, при необходимости, выдавать звуковой сигнал   
5.2.3.7. В стандартах и нормативных документах на конкретные виды идентификаторов должен быть определен минимум кодовых комбинаций. Значение кодовых комбинаций приведено в таблице 3.

Значение кодовых комбинаций



Пользователь автономных систем должен иметь возможность сменить или переустановить открывающий код не менее 100 раз. Смена кода должна происходить только после ввода действующего кода.   
  
**5.2.4.** Требования к функциональным характеристикам УУ   
5.2.4.1. Аппаратные средства УУ должны обеспечивать прием информации от УВИП, обработку информации и выработку сигналов управления на исполнительные устройства УПУ.   
5.2.4.2. Аппаратные средства УУ в системах с централизованным управлением и универсальных должны обеспечивать. 

* обмен информацией по линии связи между контроллерами и средствами управления;
* сохранность данных в памяти при обрыве линий связи со средствами централизованного управления, отключении питания и при переходе на резервное питание;
* контроль линий связи между контроллерами, средствами централизованного управления. Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также, при необходимости, защиту информации.

Виды и параметры протоколов и интерфейсов должны быть установлены в стандартах и других нормативных документах на УУ конкретного типа с учетом требований ГОСТ 26139.   
5.2.4.3. Программное обеспечение УУ должно обеспечивать: 

* занесение кодов идентификаторов в память системы;
* задание характеристик точек доступа;
* установку временных интервалов доступа (окон времени);
* установку уровней доступа для пользователей;
* протоколирование текущих событий;
* ведение и поддержание баз данных;
* регистрацию прохода через точки доступа в протоколе базы данных;
* сохранение баз данных и системных параметров на резервном носителе;
* сохранение баз данных и системных параметров при авариях и сбоях в системе;
* приоритетный вывод информации о нарушениях;
* возможность управления УПУ в случае чрезвычайных ситуаций.

5.2.4.4. Программное обеспечение УУ должно быть устойчиво к случайным и преднамеренным воздействиям следующего вида: 

* отключение питания аппаратных средств;
* программный сброс аппаратных средств;
* аппаратный сброс аппаратных средств;
* случайное нажатие клавиш на клавиатуре;
* случайный перебор пунктов меню программы.

После указанных воздействий и перезапуске программы должна сохраняться работоспособность системы и сохранность установленных данных. Указанные воздействия не должны приводить к открыванию УПУ и изменению действующих кодов доступа.   
5.2.4.5. Общие показатели качества программного обеспечения следует устанавливать по ГОСТ 28195.   
  
**5.3. Требования к электромагнитной совместимости**  
**5.3.1.** Средства и системы КУД в зависимости от устойчивости к воздействию электромагнитных помех должны иметь следующие степени жесткости по ГОСТ Р 50009: 

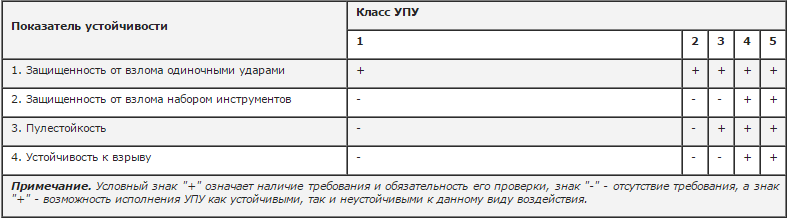
* первая или вторая степень - при нормальной устойчивости;
* третья степень - при повышенной устойчивости;
* четвертая или пятая степень - при высокой устойчивости.

Требования по устойчивости к искусственно создаваемым электромагнитным помехам пред являют к устройствам, имеющим степень жесткости не ниже второй, и должны быть установлены в технических условиях на средства и системы КУД конкретного типа.   
**5.3.2.**Уровень допустимых радиопомех при работе средств и систем КУД должен соответствовать ГОСТ 23511 и ГОСТ Р 50009.   
  
**5.4. Требования по устойчивости средств и систем КУД в НСД**  
**5.4.1.** Требования по устойчивости к НСД устанавливают в настоящем пункте и нормативны документах на средства и системы КУД конкретного типа.   
**5.4.2.**Требования по устойчивости к НСД разрушающего действия распространяются на УГП и считыватели УВИП. Требования включают: 

* устойчивость к взлому;
* пулестойкость;
* устойчивость к взрыву.

**5.4.3.** Устойчивость к разрушающим воздействиям устанавливают для средств с повышенным и высоким уровнями устойчивости.   
Нормальная устойчивость обеспечивается механической прочностью конструкции без оценки по показателям устойчивости.   
Повышенную устойчивость определяют по показателям устойчивости к взлому одиночными ударами и (или) набором инструментов.   
Высокую устойчивость определяют по показателям устойчивости к взлому, пулестойкости и (или) взрыву.   
Требования по пулестойкости применяют только к УПУ с полным (сплошным) перекрытием проема прохода.   
Показатели устойчивости по классам приведены в таблице 4.

Классы УПУ по показателям устойчивости



**5.4.4.** Требования по устойчивости к НСД неразрушающего воздействия устанавливаются для средств КУД в зависимости от функционального назначения и включают: 

* устойчивость к вскрытию для УПУ и исполнительных устройств (замков и запорных механизмов);
* устойчивость к манипулированию;
* устойчивость к наблюдению для УВИП с запоминаемым кодом (клавиатуры, кодовые переключатели и т. п.);
* устойчивость к копированию идентификаторов.

Показатели устойчивости по данным требованиям и методы их испытаний должны быть указаны в стандартах и (или) технических условиях на средства КУД конкретного типа.  
**5.4.5.**Автономные СКУД должны быть защищены от манипулирования с целью изменения или подбора кода Вт защиты должен быть указан в технических условиях на системы конкретного типа   
**5.4.6.** Системы КУД повышенной и высокой устойчивости к НСД должны иметь защиту от принуждения и саботажных действий Конкретный метод защиты и показатели защиты должны быть приведены в технических условиях на системы КУД конкретного типа.   
**5.4.7.**Программное обеспечение УУ должно быть защищено от несанкционированного доступа. Требования по защите программного обеспечения УУ от несанкционированного доступа устанавливают по ГОСТ Р 50739.   
**5.4.8.**Программное обеспечение УУ должно быть также защищено от: 

* преднамеренных воздействий с целью изменения опций в системе;
* несанкционированного копирования;
* несанкционированного доступа с помощью паролей.

Рекомендуемые уровни доступа по типу пользователей: 

* первый ("администратор") - доступ ко всем функциям;
* второй ("дежурный оператор") - доступ только к функциям текущего контроля;
* третий ("системный оператор") - доступ к функциям конфигурации программного обеспечения без доступа к функциям, обеспечивающим управление УПУ.

Количество знаков в пароле должно быть не менее шести.   
При вводе пароля в систему вводимые знаки не должны отображаться на средствах отображения информации.   
После ввода в систему пароли должны быть защищены от просмотра средствами операционных систем ЭВМ.   
**5.4.9.**Требования по защите систем КУД с централизованным управлением и универсальных от несанкционированного доступа к информации должны соответствовать для систем нормальной устойчивости к НСД требованиям 5.4.8 данного стандарта, для систем повышенной и высокой устойчивости требования устанавливают по классам в соответствии с документом [3], и они должны соответствовать приложению А.   
При этом класс защиты системы от несанкционированного доступа к информации должен соответствовать: 

* 3А, 3Б, 2Б -для систем повышенной устойчивости;
* 1Г и 1В -для систем высокой устойчивости.

**5.4.10.**Требования по защите средств от несанкционированного доступа к информации устанавливают для средств КУД нормальной устойчивости в соответствии с требованиями настоящего стандарта, для средств КУД повышенной и высокой устойчивости требования устанавливают по классам в соответствии с документом [1], и они должны соответствовать данным приложения Б.   
При этом класс защиты средств КУД от несанкционированного доступа к информации должен соответствовать: 

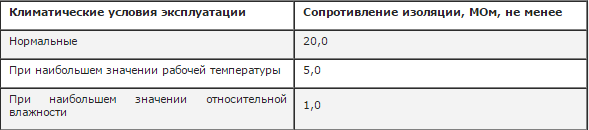
* повышенной устойчивости - классу 5 или 6;
* высокой устойчивости - классу 4.

**5.4.11.** Системы и средства КУД высокой устойчивости подлежат обязательной сертификации по требованиям защиты от несанкционированного доступа к информации.   
    
**5.5. Требования надежности**  
**5.5.1.**В стандартах и (или) технических условиях на средства и системы КУД конкретного типа должны быть установлены следующие показатели надежности в соответствии с ГОСТ 27.002 и ГОСТ 27.003: 

* средняя наработка на отказ, ч;
* среднее время восстановления работоспособного состояния, ч;
* средний срок службы, лет.

При установлении показателей надежности должны быть указаны критерии отказа.   
Показатели надежности средств КУД устанавливают исходя из необходимости обеспечения надежности системы в целом.   
По требованию заказчика в технических условиях на конкретные средства и системы КУД могут быть установлены дополнительно другие требования по надежности.   
**5.5.2.**Средняя наработка на отказ систем КУД с одной точкой доступа (без учета УПУ) - не менее 10000 ч.   
**5.5.3.**Средний срок службы систем КУД - не менее 8 лет с учетом проведения восстановительных работ.   
  
**5.6. Требования по устойчивости к внешним воздействующим факторам**  
**5.6.1.** Требования по устойчивости в части воздействия климатических факторов устанавливают в стандартах и нормативных документах на средства и системы КУД конкретного типа в соответствии с климатическим исполнением и категорией изделий по ГОСТ 15150.   
**5.6.2.** Оболочки средств КУД при необходимости защиты от внешних воздействий должны иметь степени защиты по ГОСТ 14254.   
**5.6.3.** Требования по устойчивости в части воздействия механических факторов должны быть установлены в стандартах и (или) нормативных документах на средства и системы КУД конкретного типа в соответствии с требуемой группой условий эксплуатации по ГОСТ 17516 и степенью жесткости изделий по ГОСТ 16962.   
  
**5.7. Требования к электропитанию**  
**5.7.1.** Основное электропитание средств и систем КУД должно осуществляться от сети переменного тока с номинальным напряжением 220 В, частотой 50 Гц.   
Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения сети от минус 15 до плюс 10 % от номинального значения и частоты (50±1) Гц.   
Электропитание отдельных средств контроля и управления доступом допускается осуществлять от источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на средства КУД конкретного типа.   
**5.7.2.**Средства и системы КУД должны иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервного источника питания допускается использовать резервную сеть переменного тока или источник питания постоянного тока.   
Номинальное напряжение резервного источника питания постоянного тока выбирают из ряда: 12, 24 В.   
Переход на резервное питание должен происходить автоматически без нарушения установленных режимов работы и функционального состояния средств и систем КУД.   
Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения резервного источника от минус 15 до плюс 10 % от номинального значения.   
**5.7.3.** Резервный источник питания должен обеспечивать выполнение основных функций системы КУД при пропадании напряжений в сети на время не менее 0,5 ч для систем первого и второго класса по функциональным характеристикам и не менее 1 ч для систем третьего класса.   
Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы и т.п.). При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания.   
**5.7.4.**При использовании в качестве источника резервного питания аккумуляторных батарей должен выполняться их автоматический заряд.   
**5.7.5.** При использовании в качестве источника резервного питания аккумуляторных или сухих батарей рекомендуется иметь индикацию разряда батареи ниже допустимого предела. Для автономных систем индикация разряда может быть- световая или звуковая, для сетевых систем сигнал разряда батарей может передаваться на пункт управления.   
**5.7.6.** Химические источники питания, встроенные в идентификаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность средств КУД не менее 3 лет.   
  
**5.8. Требования безопасности**  
**5.8.1.** Средства и системы КУД должны соответствовать требованиям безопасности ГОСТ 12.2.007.0, ГОСТ 12.2.006 и ГОСТ 27570.0.   
**5.8.2.** Материалы, комплектующие изделия, используемые для изготовления средств и систем КУД, должны иметь токсико-гигиенический паспорт, гигиенический паспорт и гигиенический сертификат.   
**5.8.3.**Монтаж и эксплуатация средств и систем КУД должны соответствовать требованиям безопасности ГОСТ 12.2.003.   
**5.8.4.** Средства и системы КУД должны соответствовать требованиям пожарной безопасности ГОСТ 12.1.004.   
**5.8.5.**Электрическое сопротивление изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должно быть не менее значений, указанных в таблице 5.

Требуемые значения сопротивления изоляции



**5.8.6.** Электрическая прочность изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должна соответствовать требованиям ГОСТ 12997.   
**5.8.7.** Сопротивление изоляции и электрическая прочность средств и систем КУД, предназначенных для бытового и аналогичного общего применения, должны соответствовать требованиям ГОСТ 12.2.006 и ГОСТ 27570.0.   
**5.8.8.** Для средств КУД, работающих при напряжениях не выше 12 В переменного тока и 36 В постоянного тока, допускается не приводить значение электрической прочности изоляции и ее сопротивления в нормативных документах на конкретные средства.   
**5.8.9.**Конкретные значения сопротивления изоляции и электрическая прочность изоляции должны быть указаны в технических условиях на средства и системы КУД конкретного типа.   
**5.8.10.** Уровни излучений средств и систем КУД должны соответствовать требованиям безопасности, установленным в ГОСТ 12.1.006.   
**5.8.11.**Средства и системы КУД, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям ГОСТ 12.1.010, других стандартов и нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.   
    
**5.9. Требования к конструкции**  
**5.9.1.**Габаритные размеры средств КУД и их отдельных функционально и конструктивно оформленных устройств, блоков должны обеспечивать транспортирование через типовые проемы зданий, сборку, установку и монтаж - на месте эксплуатации.   
**5.9.2.**Конструкции средств КУД должны быть построены по модульному и блочно-агрегатному принципу и обеспечивать: 

* взаимозаменяемость сменных однотипных составных частей;
* удобство технического обслуживания, эксплуатации и ремонтопригодность;
* исключение возможности несанкционированного доступа к элементам управления параметрами;
* доступ ко всем элементам, узлам и блокам, требующим регулирование или замену в процессе эксплуатации.

**5.9.3.**Конструкционные и электроизоляционные материалы, покрытия и комплектующие изделия должны обеспечивать: 

* механическую прочность;
* требуемую надежность;
* устойчивость к несанкционированным действиям по категориям и классам устойчивости;
* безопасную работу в заданных условиях эксплуатации.

**5.10. Требования к маркировке**  
**5.10.1.** Маркировка средств и систем КУД должна быть выполнена по ГОСТ Р 50775 и содержать: 

* товарный знак и (или) другие реквизиты предприятия-изготовителя;
* условное обозначение средств и систем КУД;
* серийный номер;
* дату изготовления;
* знак сертификата соответствия (при его наличии).

**5.10.2.**Номер сертификата или реквизиты заключения (при их наличии), фирменный знак и (или) другие реквизиты организаций, проводивших сертификационные или экспертные испытания, должны быть указаны в сопроводительной документации.