Национальный стандарт РФ ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. N 430-ст) (с изменениями и дополнениями)

Access control units and systems. Classification. General technical requirements. Test methods

(ОКПД2) ОК 034-2014 **.30.50.110**

Дата введения - 1 сентября 2009 г.
Взамен ГОСТ Р 51241-98

Предисловие

РАЗРАБОТАН Федеральным казенным учреждением "Научно-исследовательский центр "Охрана" Федеральной службы войск национальной гвардии Российской Федерации (ФКУ "НИЦ "Охрана" Росгвардии)".

Сведения о правилах применения и о порядке опубликования информации об изменениях к стандарту его пересмотре или отмене изложить в новой редакции:

"Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. N 162-ФЗ "О стандартизации в Российской Федерации". Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе "Национальные стандарты", а официальный текст изменений и поправок - в ежемесячном информационном указателе "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru).

1 Область применения

Настоящий стандарт распространяется на средства и системы контроля и управления доступом, предназначенные для предотвращения несанкционированного физического доступа людей, транспорта и других объектов в зону (из зоны) доступа (здания, помещения, территории) в целях обеспечения противокриминальной защиты.

Настоящий стандарт устанавливает классификацию, общие технические требования и методы испытаний средств и систем контроля и управления доступом.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 8.568 Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения

ГОСТ Р 15.301 Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство

ГОСТ Р 27.102 Надежность в технике. Надежность объекта. Термины и определения

ГОСТ Р ИСО/МЭК 7810 Карты индентификационные. Физические характеристики

ГОСТ Р ИСО/МЭК 7811-1 Карты идентификационные. Способ записи. Часть 1. Тиснение

ГОСТ Р ИСО/МЭК 7811-2 Карты идентификационные. Способ записи. Часть 2. Магнитная полоса малой коэрцитивной силы

ГОСТ Р ИСО/МЭК 7811-6 Карты идентификационные. Способ записи. Часть 6. Магнитная полоса большой коэрцитивной силы

ГОСТ Р ИСО/МЭК 7816-1 Карты идентификационные. Карты на интегральных схемах. Часть 1. Карты с контактами. Физические характеристики

ГОСТ Р ИСО/МЭК 7816-2 Карты идентификационные. Карты на интегральных схемах. Часть 2. Карты с контактами. Размеры и расположение контактов

ГОСТ Р ИСО/МЭК 7816-4 Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена

ГОСТ Р ИСО/МЭК 7816-6 Карты идентификационные. Карты на интегральных схемах. Часть 6. Межотраслевые элементы данных для обмена

ГОСТ Р ИСО/МЭК 7816-10-2004 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 10. Электронные сигналы и ответ на восстановление у синхронных карт

ГОСТ Р ИСО/МЭК 10373-1 Карты идентификационные. Методы испытаний. Часть 1. Общие характеристики

ГОСТ Р ИСО/МЭК 10373-2 Карты идентификационные. Методы испытаний. Часть 2. Карты с магнитной полосой

ГОСТ Р ИСО/МЭК 10536-2 Карты идентификационные. Карты на интегральных схемах бесконтактные. Часть 2. Размеры и расположение зон связи

ГОСТ Р ИСО/МЭК 10536-3 Карты идентификационные. Карты на интегральных схемах бесконтактные. Часть 3. Электронные сигналы и процедуры восстановления

ГОСТ Р ИСО/МЭК 11693-1 Карты идентификационные. Карты с оптической памятью. Часть 1. Общие характеристики

ГОСТ Р ИСО/МЭК 11694-1 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 11694-2 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 2. Размеры и расположение оптической зоны

ГОСТ Р ИСО/МЭК 11694-3 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 3. Оптические свойства и характеристики

ГОСТ Р ИСО/МЭК 15693-1 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 15693-2 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 2. Воздушный интерфейс и инициализация

ГОСТ ISO/IEC 15963-1 Информационные технологии. Идентификация радиочастотная для управления предметами. Часть 1. Системы нумерации для уникальной идентификации радиочастотных меток

ГОСТ Р ИСО/МЭК 19794-2 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки

ГОСТ Р 58298 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-5 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ГОСТ Р 58295 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

ГОСТ Р 50009 Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний

ГОСТ Р 50739 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ 34024 Замки сейфовые. Требования и методы испытаний на устойчивость к несанкционированному открыванию

ГОСТ 34593 Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, взрыву и пулестойкость

ГОСТ 31610.0 Взрывоопасные среды. Часть 0. Оборудование. Общие требования

ГОСТ Р 52582 Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому

ГОСТ Р 52931 Приборы контроля и регулирования технологических процессов. Общие технические условия

ГОСТ Р 53560 Системы тревожной сигнализации. Источники электропитания. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 53831 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний

ГОСТ Р 58822 Замки электромагнитные. Классификация. Общие технические требования и методы испытаний

ГОСТ IEC 60065 Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

ГОСТ Р 2.610 Единая система конструкторской документации. Правила выполнения эксплуатационных документов

ГОСТ 12.1.004 Система стандартов безопасности труда. Пожарная безопасность. Общие требования

ГОСТ 12.1.006 Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля

ГОСТ 12.1.019 Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты

ГОСТ 12.2.003 Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности

ГОСТ 12.2.007.0 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

ГОСТ 27.003 Надежность в технике. Состав и общие правила задания требований по надежности

ГОСТ 5089 Замки, защелки, механизмы цилиндровые. Технические условия

ГОСТ 14192 Маркировка грузов

ГОСТ 14254 Степени защиты, обеспечиваемые оболочками (Код IP)

ГОСТ 15150 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды

ГОСТ 16962 Изделия электронной техники и электротехники. Механические и климатические воздействия. Требования и методы испытаний

ГОСТ 19091 Замки, защелки, механизмы цилиндровые. Методы испытаний

ГОСТ 26828 Изделия машиностроения и приборостроения. Маркировка

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **аутентификация**: Процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

3.2 **биометрическая идентификация**: Идентификация, основанная на использовании индивидуальных физических признаков человека.

3.3 **вещественный код**: Код, записанный на физическом носителе (идентификаторе).

3.4 **взлом**: Действия, направленные на несанкционированное разрушение конструкции.

3.5 **временной интервал доступа (окно времени)**: Временной интервал, в течение которого в данной точке доступа устанавливается заданный режим доступа.

3.6 **вскрытие**: Действия, направленные на несанкционированное проникновение через устройства преграждающие управляемые (УПУ), без их разрушения.

3.7 **доступ**: Перемещение людей (субъектов доступа), транспорта и других объектов (объектов доступа) в (из) помещения, здания, зоны и территории.

3.8 **запоминаемый код**: Код, кодовое слово (пароль), вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

3.9 **зона доступа**: Здание, помещение, территория, транспортное средство, вход и (или) выход которых оборудованы средствами контроля и управления доступом (КУД).

3.10 **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 др. устройства).

3.11 **идентификация**: Процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимают также присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

3.12 **контроллер доступа (КД), прибор приемно-контрольный доступа (ППКД)**: Аппаратное устройство в составе средств управления СКУД.

3.13 **контроль и управление доступом (КУД)**: Комплекс мероприятий, направленных на предотвращения несанкционированного доступа.

3.14 **копирование**: Действия с идентификаторами, целью которых является получение копии идентификатора с действующим кодом.

3.15 **криминальная безопасность**: Состояние объекта защиты, при котором отсутствует недопустимый риск, связанный с причинением ему вреда от реализации криминальной угрозы.

3.16 **манипулирование**: Действия с устройствами контроля доступа, находящимися в рабочем режиме, без их разрушения, с целью получения действующего кода или приведения в открытое состояние УПУ. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия будут незаметны. Манипулирование включает в себя также действия над программным обеспечением и действия по съему информации с каналов связи и интерфейсов устройств доступа.

3.17 **наблюдение**: Действия с устройствами контроля и управления доступом без прямого доступа к ним с целью получения действующего кода.

3.18 **несанкционированные действия (НСД)**: Действия с целью несанкционированного проникновения в зону доступа через УПУ.

3.19 **несанкционированный доступ**: Доступ субъектов или объектов, не имеющих права доступа.

3.20 **пользователь СКУД**: Субъект, в отношении которого осуществляются мероприятия по контролю доступа.

3.21 **правило двух (и более) лиц**: Правило доступа, при котором доступ разрешен только при одновременном присутствии двух или более лиц.

3.22 **принуждение**: Насильственные действия по отношению к лицу, имеющему право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.

3.23 **пропускная способность**: Способность средства или системы КУД пропускать через заданную точку доступа определенное число субъектов или объектов доступа в единицу времени.

3.24 **противокриминальная защита объектов и имущества**: Деятельность, осуществляемая с целью обеспечения криминальной безопасности

3.25 **пулестойкость**: Способность преграды противостоять сквозному пробиванию пулями и отсутствие при этом опасных для человека вторичных поражающих элементов.

3.26 **саботаж**: Преднамеренно созданное состояние системы или ее компонентов, при котором нарушается работоспособность, ухудшаются параметры, происходит повреждение системы.

3.27 **санкционированный доступ**: Доступ субъектов или объектов, имеющих права доступа.

3.28 **система контроля и управления доступом (СКУД)**: Совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.

3.29 **средства управления (СУ)**: Аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации.

3.30 **средства контроля и управления доступом (средства КУД)**: Механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию контроля и управления доступом.

3.31 **точка доступа**: Место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные необходимыми средствами).

3.32 **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.

3.33 **устойчивость к взлому; взломостойкость:** Характеристика конструкции устройства преграждающего управляемого, обеспечивающая его способность выполнять защитную функцию и определяющая класс устойчивости к взлому.

3.34 **устойчивость к взрыву**: Способность конструкции противостоять разрушающему воздействию взрывчатых веществ.

3.35 **устройства преграждающие управляемые (УПУ)**: Устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (турникеты, шлюзы, проходные кабины, двери и ворота, оборудованные исполнительными устройствами СКУД, а также другие подобные устройства).

3.36 **устройства исполнительные (УИ)**: Устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические, электромагнитные замки, электромагнитные защелки, механизмы привода шлюзов, ворот, турникетов и другие подобные устройства).

3.37 **устройство считывающее (УС), считыватель**: Устройство, предназначенное для считывания (ввода) идентификационных признаков.

источник электропитания переменного тока бесперебойный; ИЭПВБ: Источник электропитания переменного тока вторичный с резервом, обеспечивающий электропитание потребителей напряжением, аналогичным по характеристикам напряжению электросети (источника электропитания первичного) при отключении или недопустимом снижении

напряжения электросети.
[ГОСТ Р 53560-2022, статья 3.5]

источник электропитания вторичный с резервом; ИЭПВР: Источник электропитания вторичный постоянного тока для основного и резервного электропитания технических средств охраны, имеющий в своем составе или имеющий возможность подключения элементов накопления (сохранения) электрической энергии (аккумуляторных батарей) для обеспечения функционирования при отключении или недопустимом снижении напряжения электросети переменного тока, и обеспечивающий возможность их заряда.
[ГОСТ Р 53560-2022, статья 3.6]

электросеть: распределительная электрическая сеть по ГОСТ 32144 трехфазного напряжения четырехпроводная или трехпроводная с фазным номинальным напряжением 230 В, частотой 50 Гц по ГОСТ 29322 (IEC 60038:2009)

4 Классификация

4.1 Классификация средств КУД

4.1.1 Средства КУД подразделяют по:
- функциональному назначению устройств;
- функциональным характеристикам;
- устойчивости к НСД.

4.1.2 Средства КУД по функциональному назначению устройств подразделяют на следующие основные средства:
- устройства преграждающие управляемые;
- устройства исполнительные;
- устройства считывающие;
- идентификаторы (ИД);
- средства управления в составе аппаратных устройств и программных средств.

В состав СКУД могут входить другие дополнительные средства: источники электропитания; датчики (извещатели) состояния УПУ; дверные доводчики; световые и звуковые оповещатели; кнопки ручного управления УПУ; устройства преобразования интерфейсов сетей связи; аппаратура передачи данных по различным каналам связи и другие устройства, предназначенные для обеспечения работы СКУД.

В состав СКУД могут входить также аппаратно-программные средства - средства вычислительной техники (СВТ) общего назначения (компьютерное оборудование, оборудование для компьютерных сетей, общее программное обеспечение).

4.1.3 Средства КУД по функциональным характеристикам подразделяют на следующие группы:

4.1.3.1 УПУ по виду перекрытия проема прохода классифицируют по ГОСТ Р 54831.

4.1.3.2 УИ подразделяют по видам запирающих устройств на:
- электромеханические замки;
- электромагнитные замки;
- электромагнитные защелки;
- механизмы привода дверей, ворот.

4.1.3.4 Идентификаторы и считыватели - по следующим признакам:
- виду используемых идентификационных признаков (идентификаторы и считыватели);
- способу считывания идентификационных признаков (считыватели).

По виду используемых идентификационных признаков идентификаторы и считыватели

могут быть:

- механическими - представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);
- магнитными - представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т.д.);
- оптическими - представляют собой нанесенные на поверхность или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т.д.);
- электронными контактными - представляют собой электронный код, записанный в электронной микросхеме идентификатора (дистанционные карты, электронные ключи и т.д.);
- электронными радиочастотными - считывание кода с электронных идентификаторов происходит путем передачи данных по радиоканалу;
- акустическими - представляют собой кодированный акустический сигнал;
- биометрическими (только для считывателей) - представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрию ладони, рисунок сетчатки глаза, голос, динамику подписи и т.д.);
- комбинированными - для идентификации используют одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков считыватели могут быть:

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

4.1.3.5 Классификация средств управления СКУД включает в себя:

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

4.2 Классификация СКУД

4.2.1 СКУД классифицируют по:

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

4.2.2 По способу управления СКУД подразделяют на:

- автономные - для управления одним или несколькими УПУ без передачи информации на центральное устройство управления и контроля со стороны оператора;
- централизованные (сетевые) - для управления УПУ с обменом информацией с центральным пультом и контролем и управлением системой со стороны центрального устройства управления;
- универсальные (сетевые) - включающие в себя 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, центральном устройстве или обрыве связи.

4.2.3 По числу контролируемых точек доступа:

- малой емкости (не более 64 точек);
- средней емкости (от 64 до 256 точек);
- большой емкости (более 256 точек).

4.2.4 По функциональным характеристикам СКУД подразделяют на три класса:
1-й - системы с ограниченными функциями;
2-й - системы с расширенными функциями;
3-й - многофункциональные системы.

4.3 Классификация средств и систем КУД по устойчивости к НСД

4.3.1 Классификация средств КУД по устойчивости к НСД основана на устойчивости к разрушающим и неразрушающим воздействиям по уровням устойчивости:
1) нормальной;
2) повышенной;
3) высокой.
4.3.2 УПУ по устойчивости к разрушающим воздействиям классифицируют по ГОСТ Р 54831.
УПУ повышенной и высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и блокированием объекта в проеме (шлюзы, кабины проходные) классифицируют по устойчивости к взлому, взрыву и пулестойкости как для защитных дверей по ГОСТ 34593.
4.3.3 УИ классифицируют по устойчивости к разрушающим воздействиям в зависимости от конструкции по ГОСТ Р 52582, ГОСТ 34024, ГОСТ 19091, ГОСТ 5089.
Класс устойчивости УИ должен быть не ниже класса устойчивости УПУ.
4.3.4 По устойчивости к неразрушающим воздействиям средства КУД в зависимости от их функционального назначения классифицируют по следующим показателям:
- 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 (СВТ) средств управления СКУД от несанкционированного доступа к информации.
Классификацию по устойчивости к неразрушающим воздействиям: вскрытию, манипулированию, наблюдению, копированию устанавливают в стандартах и нормативных документах на средства КУД конкретного типа.
4.3.5 Классификацию СКУД к НСД определяют как для систем с централизованным управлением по защищенности от несанкционированного доступа к информации ПО СКУД и средств СВТ, входящих в состав сетевых СКУД.
Классификацию систем КУД по защищенности от НСД к информации устанавливают как для автоматизированных систем в соответствии с [1] по приложению А, таблица А.1, с учетом классификации средств СВТ, входящих в состав сетевых СКУД по устойчивости от НСД к информации в соответствии с [2] по приложению Б, таблица Б.1.

4.4 Условные обозначения средств и систем КУД

Исключен с 1 февраля 2025 г. - Изменение N 1

5 Технические требования

5.1 Общие положения

5.1.1 Разработку и постановку на производство средств и систем контроля управления доступом проводят в соответствии с ГОСТ Р 15.301.
5.1.2 Конструкторская документация на средства и системы КУД должна соответствовать

требованиям ЕСКД. Эксплуатационные документы должны быть выполнены в соответствии с ГОСТ Р 2.601 и ГОСТ Р 2.610.

5.1.3 Средства и системы КУД должны изготовляться в соответствии с требованиями настоящего стандарта, а также нормативных документов на средства и системы КУД конкретного типа. Техническое обслуживание СКУД в процессе эксплуатации осуществляют в соответствии с эксплуатационной документацией.

5.1.4 Средства и системы КУД должны обеспечивать возможность непрерывной работы с учетом проведения регламентного технического обслуживания.

5.1.5 Системы КУД в рабочем режиме должны обеспечивать автоматическую работу. Режим ручного или автоматизированного управления (с участием оператора) должен обеспечиваться только при возникновении чрезвычайных, аварийных или тревожных ситуаций, а также по требованию заказчика.

5.1.6 Параметры и требования, определяющие совместимость средств КУД, предназначенных для поставки в качестве самостоятельных изделий, должны быть установлены в нормативных документах на средства КУД конкретного типа.

5.1.7 Средства и системы КУД в составе систем противокриминальной защиты объектов должны обеспечивать:

- защиту от несанкционированного доступа на охраняемый объект (помещение, зону) в режиме снятия их с охраны;
- контроль и учет доступа персонала (посетителей) на охраняемый объект (помещение, зону) в режиме снятия их с охраны;
- автоматизацию процессов взятия/снятия охраняемого объекта (помещения, зоны) с помощью средств идентификации СКУД в составе устройств и приборов охранной сигнализации;
- защиту и контроль доступа к компьютерам автоматизированных рабочих мест (АРМ) пультового оборудования систем охранной сигнализации;
- защиту от НСД к информации.

5.2 Требования к функциональным характеристикам средств КУД

5.2.1 Требования к функциональным характеристикам УПУ и ИУ

5.2.1.1 Требования к функциональным характеристикам УПУ - по ГОСТ Р 54831.

5.2.1.2 УПУ с высоким уровнем устойчивости к НСД и пулестойкости со сплошным перекрытием прохода должны соответствовать требованиям ГОСТ 34593.

5.2.1.3 УИ должны обеспечивать приведение УПУ в закрытое или открытое состояние.

УИ могут быть конструктивно законченными изделиями или составлять часть конструкции УПУ.

Требования к конструкции, механическим характеристикам УИ замкового типа (электромеханическим замкам и защелкам, электромагнитным замкам) должны отвечать требованиям ГОСТ Р 51093, ГОСТ Р 52582, ГОСТ Р 58822, ГОСТ 19091, ГОСТ 5089.

5.2.2 Требования к функциональным характеристикам ИД и УС

5.2.2.1 Считыватели должны обеспечивать:

- ввод запоминаемого кода;
- считывание идентификационного признака с идентификаторов;
- введение биометрической информации (для считывателей биометрической информации);
- преобразование введенной информации в электрический сигнал;
- передачу информации на контроллер СКУД.

5.2.2.2 Считыватели должны иметь световую индикацию работоспособности и состояния доступа. Рекомендуемый режим работы:

- непрерывное свечение индикатора красного цвета - доступ закрыт;
- непрерывное свечение индикатора зеленого цвета - доступ открыт.

Допускается в режиме экономии электропитания световую индикацию работоспособности и состояния доступа отображать кратковременными вспышками соответствующего цвета.

При необходимости считыватели должны быть оборудованы звуковым сигнализатором. Параметры звуковых сигналов и события, которые они индицируют, должны быть описаны в документации на ИД и УС.

Допускается отсутствие индикации в считывателе, при этом в документации на УС должно быть указано, что такие считыватели должны использоваться с контроллерами СКУД, которые обеспечивают управление внешними световыми и звуковыми индикаторами.

5.2.2.3 Считыватели должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды и степень защиты должны быть указаны в документации на устройства конкретного типа. Информация, содержащаяся в документации, не должна снижать степень защиты.

5.2.2.4 Считыватели не должны вызывать открывания УПУ в случае взлома или вскрытия, а также при обрыве или коротком замыкании электрических цепей. При этом автономные системы должны выдавать звуковой сигнал тревоги, а системы с централизованным управлением - дополнительно передавать сигнал тревоги на пункт управления.

5.2.2.5 Биометрические считыватели, при их применении в СКУД, должны соответствовать требованиям ГОСТ Р ИСО/МЭК 19794-2, ГОСТ Р ИСО/МЭК 19794-4, ГОСТ Р ИСО/МЭК 19794-5, ГОСТ Р 58295 (ИСО/МЭК 19794-6:2011).

5.2.2.6 Идентификаторы должны иметь уникальный идентификационный признак (код, номер), который не должен повторяться. В случае, если такое повторение возможно, в документации на конкретное изделие должны быть указаны условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами.

5.2.2.7 Идентификаторы должны обеспечивать хранение идентификационного признака в течение всего срока службы при эксплуатации.

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

5.2.2.9 В зависимости от конструктивного исполнения и вида используемого идентификационного признака идентификаторы в части, касающейся их применения в СКУД, должны соответствовать требованиям: ГОСТ Р ИСО/МЭК 7810, ГОСТ Р ИСО/МЭК 7811-1, ГОСТ Р ИСО/МЭК 7811-2, ГОСТ Р ИСО/МЭК 7811-6, ГОСТ Р ИСО/МЭК 7816-1, ГОСТ Р ИСО/МЭК 7816-2, ГОСТ Р ИСО/МЭК 7816-4, ГОСТ Р ИСО/МЭК 7816-6, ГОСТ Р ИСО/МЭК 7816-10, ГОСТ Р ИСО/МЭК 10373-1, ГОСТ Р ИСО/МЭК 10373-2, ГОСТ Р ИСО/МЭК 10536-2, ГОСТ Р ИСО/МЭК 10536-3, ГОСТ Р ИСО/МЭК 11693-1, ГОСТ Р ИСО/МЭК 11694-1, ГОСТ Р ИСО/МЭК 11694-2, ГОСТ Р ИСО/МЭК 11694-3, ГОСТ Р ИСО/МЭК 15693-1, ГОСТ Р ИСО/МЭК 15693-2, ГОСТ ISO/IEC 15963-1.

5.2.3 Требования к функциональным характеристикам СУ

5.2.3.1 Аппаратные средства управления (контроллеры) должны обеспечивать прием информации от считывателей, обработку информации и выработку сигналов управления на исполнительные устройства.

5.2.3.2 Контроллеры в системах с централизованным управлением и универсальных систем должны обеспечивать:

- обмен информацией по линии связи между контроллерами и средствами централизованного управления;

- сохранность данных в памяти системы, при обрыве линий связи со средствами централизованного управления, отключении питания и при переходе на резервное питание;

- контроль линий связи между контроллерами и средствами централизованного управления.

Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также (при необходимости) имитостойкость и защиту информации (для систем повышенной и высокой устойчивости).

Виды и параметры протоколов и интерфейсов должны быть установлены в нормативных документах на контроллеры конкретного типа.

5.2.3.3 Контроллеры должны иметь входы для подключения цепей сигнализации состояния УПУ, кнопки запроса на выход, контакта вскрытия корпуса, контакта отрыва от стены. Контроллеры СКУД дополнительно могут иметь входы для подключения шлейфов охранной сигнализации.

Параметры шлейфов должны соответствовать требованиям ГОСТ Р 52436.

5.2.3.4 Контроллеры должны иметь выходы для подключения цепей управления исполнительными устройствами, выходы управления световой индикацией состояния доступа по каждому направлению, выходы управления световой и звуковой индикацией тревожных состояний.

5.2.3.5 Сетевые СКУД должны иметь средства централизованного управления, в качестве которых могут использоваться СВТ общего назначения (персональные или специализированные компьютеры). Основным компонентом средств управления сетевых СКУД является программное обеспечение (ПО).

В комплект эксплуатационных документов сетевой СКУД должно входить "Руководство по эксплуатации программного обеспечения", в котором должны быть указаны требования к компьютеру и составу общесистемных программ, необходимых для работы ПО СКУД.

5.2.3.6 Программное обеспечение сетевых СКУД должно обеспечивать:

- эргономичный экранный интерфейс с пользователем (оператором СКУД);
- занесение кодов идентификаторов в память системы;
- задание характеристик точек доступа;
- установку временных интервалов доступа (окон времени);
- установку уровней доступа для пользователей;
- протоколирование текущих событий;
- протоколирование тревожных 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.

5.2.3.7 Программное обеспечение должно быть устойчиво к случайным и преднамеренным воздействиям следующего вида:

- отключение питания аппаратных средств;
- программный рестарт аппаратных средств;
- аппаратный рестарт 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.

5.3 Требования к функциональным характеристикам СКУД

5.3.1 Автономные СКУД должны обеспечивать:

- выдачу сигнала на 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 закрытия на УПУ при отсутствии факта прохода;

- выдачу сигнала тревоги при аварийном открывании УПУ для несанкционированного проникновения.

5.3.2 Дополнительные характеристики автономных систем в зависимости от класса по функциональным характеристикам приведены в таблице 3.

В систему любого класса могут быть введены дополнительные характеристики.

Таблица 3 - Функциональные характеристики автономных систем

Функциональная характеристика автономных систем	Класс		
	1	2	3
1 Установка уровней доступа	-	-	+
2 Установка временных интервалов доступа	-	+	+
3 Возможность регулирования времени открывания УИ	-	+	+
4 Возможность идентификации по двум признакам	-	-	+
5 Защита от повторного использования идентификатора для прохода в одном направлении	-	-	+
6 Ввод специального идентификационного признака для открывания под принуждением	-	-	+
7 Подключение считывателей различных типов	-	+	+
8 Доступ по "правилу двух (и более) лиц"	-	-	+
9 Световая индикация о состоянии доступа	+	+	+
10 Контроль состояния УПУ	-	+	+
11 Световое и/или звуковое оповещение о попытках НСД	-	-	+
12 Регистрация и хранение информации о событиях в энергонезависимой памяти	-	+	+
13 Число событий, хранимых в энергонезависимой памяти, не менее	-	64	256
14 Ведение даты и времени возникновения событий	-	+	+
15 Возможность подключения устройства для вывода информации о событиях	-	+	+
16 Возможность передачи информации о событиях на ЭВМ	-	-	+
17 Возможность интегрирования с системой охранной сигнализации на релейном уровне	-	+	+
18 Возможность интегрирования с системой охранного телевидения на релейном уровне	-	-	+
Примечание - Знак "+" означает наличие функции и обязательность ее проверки при установлении класса, знак "-" - отсутствие функции.			

5.3.3 СКУД с централизованным управлением и универсальные должны соответствовать общим функциональным требованиям для автономных систем и дополнительно обеспечивать:

- работу в локальной сети контроллеров СКУД;
- регистрацию и протоколирование тревожных и текущих событий;
- приоритетное отображение на экране управляющего компьютера тревожных событий;
- управление работой УПУ в точках доступа по командам оператора;
- задание временных режимов действия идентификаторов в точках доступа и уровней доступа;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, к установке 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.

5.3.4 Дополнительные характеристики систем с централизованным управлением в зависимости от класса по функциональным характеристикам приведены в таблице 4.

В систему любого класса могут быть введены дополнительные характеристики.

Таблица 4 - Функциональные характеристики систем с централизованным управлением и универсальных

Функциональные характеристики систем с централизованным управлением (сетевых) и универсальных	Класс системы		
	1	2	3
1 Число уровней доступа, не менее	16	64	256
2 Число временных интервалов доступа, не менее	16	64	256
3 Защита от повторного использования идентификатора для прохода в одном направлении: - локальная - глобальная	 - -	 + -	 + +
4 Возможность двойной идентификации	-	+	+
5 Поддержка биометрической идентификации	-	-	+
6 Ввод специального идентификационного признака для открывания под принуждением	-	+	+
7 Подключение считывателей различных типов	-	+	+
8 Доступ по "правилу двух (и более) лиц"	-	+	+
9 Число событий, сохраняемых в энергонезависимой памяти контроллеров, не менее	1000	5000	10000
10 Возможность интегрирования с системой охранной и пожарной сигнализации на релейном уровне	+	-	-
11 Возможность интегрирования с системой видеоконтроля на релейном уровне	+	-	-
12 Возможность интегрирования с системами охранной и пожарной сигнализации и системами видеоконтроля на системном уровне	-	+	+
13 Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т.п.)	-	-	+
14 Обеспечение изображения на экране ЭВМ плана объекта и (или) помещений объекта с указанием мест расположения средств контроля доступа, охранной и пожарной сигнализации, средств видеоконтроля и графическим отображением тревожных состояний в контрольных точках на плане	-	+	+
15 Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	-	-	+
16 Ведение баз данных на пользователей	-	+	+
17 Поддержание фотографических данных пользователей в базе данных	-	-	+
18 Контроль за перемещением и поиск пользователей	-	-	+
Примечание - Знак "+" означает наличие функции и обязательность ее проверки при			

установлении класса, знак "-" - отсутствие функции.

5.3.5 Универсальные системы должны обеспечивать автономную работу при возникновении отказов в сетевом оборудовании, центральном устройстве или обрыве связи, а также восстановление режимов работы после устранения отказов и восстановлении связи.

5.3.6 СКУД должны иметь характеристики, значения которых должны быть установлены в стандартах и (или) ТУ на системы конкретного типа:

- максимальное число точек доступа, зон доступа, пользователей, обслуживаемых системой;
- максимальное число точек доступа, обслуживаемых одним контроллером;
- максимальное число контроллеров в системе;
- число считывателей на один контроллер системы;
- число и вид временных интервалов доступа, уровней доступа;
- число типов считывателей, используемых в системе;
- время реакции системы на заявку на проход;
- максимальная длина линии связи с контроллерами и допустимые параметры линии связи;
- максимальное расстояние действия считывателя (для бесконтактных считывателей);
- максимальное время хранения информации о событиях в памяти системы;
- максимальная пропускная способность для системы в точках доступа;
- вероятность несанкционированного доступа, вероятность ложного задержания (для СКУД с биометрической идентификацией);
- показатели по уровням устойчивости к НСД.

5.3.8 По требованию заказчика допускается устанавливать дополнительные характеристики и показатели в ТУ на системы конкретного типа.

5.4 Требования к электромагнитной совместимости

5.4.1 Средства и системы КУД, в зависимости от условий эксплуатации, должны обеспечивать помехоустойчивость при воздействии электромагнитных помех следующих степеней жёсткости по ГОСТ Р 50009:

- второй степени жёсткости - для эксплуатации в закрытых помещениях;
- третьей степени жёсткости - для эксплуатации на открытых площадках и периметрах территорий.

5.4.2 Уровни индустриальных радиопомех, создаваемых средствами и системами КУД, должны соответствовать нормам по ГОСТ Р 50009, в зависимости от области применения и условий эксплуатации, установленных в ТУ на средства и системы КУД конкретных типов.

5.5 Требования к устойчивости средств и систем КУД к НСД

5.5.1 Исключен с 1 февраля 2025 г. - Изменение N 1
5.5.2 Исключен с 1 февраля 2025 г. - Изменение N 1
5.5.3 Исключен с 1 февраля 2025 г. - Изменение N 1
5.5.4 Исключен с 1 февраля 2025 г. - Изменение N 1
5.5.5 Исключен с 1 февраля 2025 г. - Изменение N 1

5.5.6 Требования устойчивости к НСД неразрушающего воздействия устанавливают для средств КУД в зависимости от функционального назначения и должны включать в себя:

- требования устойчивости к вскрытию для УПУ и исполнительных устройств (замков и запорных механизмов);
- требования устойчивости к манипулированию;
- требования устойчивости к наблюдению для считывателей с запоминаемым кодом (клавиатуры, кодовые переключатели и т.п.);

- требования устойчивости к копированию идентификаторов.

5.5.7 Программное обеспечение сетевых систем должно быть защищено от несанкционированного доступа. Требования по защите программного обеспечения СКУД должны обеспечиваться средствами ограничения и администрирования доступа операционных систем управляющего компьютера СКУД и разграничением доступа к ПО СКУД. Рекомендуемые уровни защиты доступа к ПО с помощью паролей с разделением 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.

Число 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.

5.5.8 Требования к защите систем КУД с централизованным управлением и универсальных от несанкционированного доступа к информации и к защите СВТ, входящих в состав СКУД от несанкционированного доступа к информации, должны для систем нормальной устойчивости к НСД соответствовать требованиям настоящего стандарта.

Для систем повышенной и высокой устойчивости требования к защите от несанкционированного доступа к информации устанавливают по классам в соответствии с [1] и приложением А.

При этом классы защиты системы от несанкционированного доступа к информации должны соответствовать:

3А, 3Б, 2Б - для систем повышенной устойчивости;

1Г и 1В - для систем высокой устойчивости.

Для СВТ, входящих в состав СКУД повышенной и высокой устойчивости, требования к защите СВТ от несанкционированного доступа к информации устанавливают по классам в соответствии с [2] и приложением Б.

При этом классы защиты СВТ, входящих в состав СКУД от несанкционированного доступа к информации, должны соответствовать:

5 или 6 - для систем повышенной устойчивости;

4 - для систем высокой устойчивости.

5.6 Требования к надежности

5.6.1 В стандартах и (или) ТУ на средства и системы КУД конкретного типа должны быть установлены следующие показатели надежности в соответствии с ГОСТ Р 27.102 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 ТУ на конкретные средства и системы могут быть установлены дополнительные требования к надежности.

5.6.2 Значение средней наработки на отказ СКУД на одну точку доступа (без учета УПУ) выбирают из ряда: 10 000, 15 000, 20 000, 30 000 ч.

5.6.3 Средний срок службы систем КУД должен быть не менее восьми лет с учетом проведения восстановительных работ.

5.7 Требования устойчивости к внешним воздействующим факторам

5.7.1 Требования устойчивости в части воздействия климатических факторов устанавливают в стандартах и нормативных документах на средства и системы контроля и управления доступом конкретных видов в соответствии с климатическим исполнением и категорией изделий по ГОСТ 15150.

5.7.2 Степени защиты оболочек средств КУД при необходимости защиты от внешних воздействий должны соответствовать требованиям ГОСТ 14254.

5.7.3 В зависимости от условий применения в части воздействия механических нагрузок средства и системы КУД должны обеспечивать требования к прочности и устойчивости при воздействии этих нагрузок. К средствам и системам, не предназначенным для функционирования в условиях воздействия механических нагрузок, предъявляют требования только по прочности при воздействии этих нагрузок.

Требования устойчивости воздействию механических факторов устанавливают в нормативных документах на средства и системы контроля и управления доступом конкретных видов в соответствии с условиями эксплуатации и группами исполнения изделий по ГОСТ 16962.

5.8 Требования к электропитанию

5.8.1 Электропитание средств и систем КУД допускается осуществлять от:

- электросети;
- ИЭПВ, ИЭПВБ или ИЭПВР по ГОСТ Р 53560;
- технических средств охраны, имеющих специально предназначенные для этого выходы;
- автономных источников электропитания.

5.8.2 Средства и системы КУД, электропитание которых осуществляется от электросети или ИЭПВБ, должны сохранять работоспособность при отклонении напряжения электропитания в диапазоне от минус 20% до плюс 10% от номинального значения.

5.8.3 Средства и системы КУД, электропитание которых осуществляется от ИЭПВР, должны сохранять работоспособность при отклонении напряжения электропитания в диапазоне от минус 15% до плюс 15% от номинального значения.

5.8.4 Средства и системы КУД, электропитание которых осуществляется от электросети, должны быть оснащены встроенным резервным источником электропитания, обеспечивающим сохранение работоспособности средств и систем КУД на время не менее 1 ч при отключении напряжения электросети.

5.8.5 Средства и системы КУД, электропитание которых осуществляется от электросети, и имеющие в качестве встроенного резервного источника электропитания аккумуляторные батареи, при электропитании от электросети должны обеспечивать их заряд.

5.8.6 При электропитании средств или систем КУД от аккумуляторных батарей (при отсутствии напряжения электросети) или от химических источников тока (сухих гальванических элементов) должна обеспечиваться индикация или выдача соответствующего сигнала при разряде аккумуляторных батарей (сухих гальванических элементов) до уровня, не позволяющего средствам или системам КУД обеспечивать выполнение своих функций.

Примечание - Формирование индикации или сигнала о разряде аккумуляторных батарей (сухих гальванических элементов) может осуществляться как отдельными средствами в составе СКУД, так и передаваться на КД, ППКД или автоматизированное рабочее место в составе СКУД.

5.8.7 Средства и системы КУД должны обеспечивать сохранение и восстановление системных настроек, режимов работы и функционального состояния после восстановления напряжения электропитания.

5.8.8 Допускается не применять резервирование электропитания для УПУ, имеющих в режиме включенного состояния электромагнитных элементов, электродвигателей, и иных типов

потребителей паспортную мощность, равную или превышающую 100 ВА.

5.8.9 Идентификаторы или контроллеры, оснащенные встроенными неперезаряжаемыми химическими источниками тока (сухими гальваническими элементами), должны сохранять работоспособность от одного комплекта источников тока в течение не менее трех лет со дня ввода в эксплуатацию.

5.9 Требования безопасности

5.9.1 Средства и системы КУД должны соответствовать общим требованиям безопасности по ГОСТ 12.2.007.0, ГОСТ IEC 60065, ГОСТ 12.2.003.

5.9.2 Материалы, комплектующие изделия, используемые для изготовления средств и систем КУД, должны быть экологически безопасны.

5.9.3 Средства и системы КУД должны соответствовать общим требованиям пожарной безопасности по ГОСТ 12.1.004.

5.9.4 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.

Таблица 5 - Сопротивление изоляции

Климатические условия эксплуатации	Сопротивление изоляции, МОм, не менее
Нормальные	20,0
При наибольшем значении рабочей температуры	5,0
При наибольшем значении относительной влажности	1,0

5.9.5 Сопротивление изоляции и электрическая прочность средств и систем КУД, предназначенных для бытового и аналогичного общего применения, должны соответствовать требованиям ГОСТ IEC 60065, ГОСТ Р 52931.

5.9.6 Конкретные значения сопротивления изоляции и электрическая прочность изоляции должна быть указана в ТУ.

5.9.7 Исключен с 1 февраля 2025 г. - Изменение N 1

5.9.8 Средства и системы КУД, предназначенные для эксплуатации в зонах с взрывоопасной средой должны соответствовать требованиям ГОСТ Р 51330.0 и нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.

5.10 Требования к конструкции

5.10.1 Габаритные размеры средств КУД и их отдельных функционально и конструктивно законченных устройств, блоков должны обеспечивать транспортирование через типовые проемы зданий, сборку, установку и монтаж на месте эксплуатации.

5.10.2 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 регулирования или замены в процессе эксплуатации.

5.10.3 Конструкционные, электроизоляционные материалы, покрытия и комплектующие

изделия должны обеспечивать:

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

5.11 Требования к маркировке

5.11.1 Маркировка средств и систем КУД должна быть выполнена в соответствии с ГОСТ 26828 и содержать:

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

5.11.2 Маркировка средств и систем КУД при транспортировании в упаковке должна соответствовать ГОСТ 14192.

6 Методы испытаний

6.1 Общие положения

6.1.1 Испытания средств и систем КУД проводят методами, приведенными в настоящем стандарте, а также по методикам испытаний в соответствии с действующими нормативными документами на конкретные типы испытаний и ТУ на конкретные средства и системы КУД.

Объем и последовательность испытаний устанавливают в программе испытаний на конкретные средства и системы контроля и управления доступом.

6.1.2 Приборы и оборудование, применяемые при проведении испытаний, должны быть поверены и аттестованы в соответствии с ГОСТ Р 8.568 и обеспечивать требуемую точность измерений.

6.1.3 При проведении испытаний средств и систем контроля и управления доступом должны быть обеспечены требования техники безопасности и другие условия в соответствии с требованиями используемых нормативных документов.

Безопасность проведения работ, использования приборов, инструментов и оборудования должна обеспечиваться выполнением требований ГОСТ 12.1.006, ГОСТ 12.1.019.

Помещения для проведения испытаний должны соответствовать необходимому уровню безопасности работ, а приборы и оборудование - использоваться в соответствии с предусмотренными инструкциями.

6.1.4 Образцы средств и систем контроля и управления доступом, предназначенные для проведения испытаний, должны иметь техническую документацию в объеме, необходимом для проведения испытаний, и быть полностью ею укомплектованы.

6.1.5 Все испытания средств и систем контроля и управления доступом, кроме климатических, проводят в нормальных климатических условиях испытаний по ГОСТ 15150.

6.2 Испытания на соответствие средств и систем КУД техническим требованиям

6.2.1 Испытания на соответствия средств и систем КУД техническим требованиям к функциональным характеристикам (см. 5.2, 5.3) проводят по методикам испытаний, приведенным в

стандартах и ТУ на средства и системы КУД конкретного типа.

6.2.2 Испытания устойчивости средств и систем КУД к требованиям электромагнитной совместимости (см. 5.4) проводят по ГОСТ Р 50009.

6.2.4 Исключен с 1 февраля 2025 г. - Изменение N 1

6.2.5 Исключен с 1 февраля 2025 г. - Изменение N 1

6.2.6 Исключен с 1 февраля 2025 г. - Изменение N 1

6.2.7 Испытания по защите программного обеспечения СКУД от несанкционированного доступа систем КУД с централизованным управлением и универсальных от несанкционированного доступа к информации и защите СВТ, входящих в состав СКУД, от несанкционированного доступа к информации 5.5.7 проводят проверкой на соответствие ГОСТ Р 50739, [1] и [2].

6.2.8 Испытания средств и систем КУД на соответствие требованиям надежности (см. 5.6) проводят по методикам, разработанным с учетом положений и требований ГОСТ 27.003.

6.2.9 Испытания средств и систем КУД на устойчивость к внешним воздействующим факторам (см. 5.7) проводят по ГОСТ Р 52931.

6.2.10 Испытания средств и систем КУД на соответствие требованиям к электропитанию (см. 5.8) проводят по методикам в соответствии с ТУ на средства и системы КУД конкретного типа.

6.2.11 Испытания средств и систем КУД на соответствие требованиям безопасности (см. 5.9) проводят по ГОСТ Р МЭК 60065, ГОСТ 12.2.003 и ТУ на средства и системы КУД конкретного типа.

6.2.12 Проверку конструкции (см. 5.10) и маркировки (см. 5.11) проводят по ТУ на средства и системы КУД конкретного типа.

---

* Приводится обозначение ТУ.

Приложение А (обязательное)

Автоматизированные системы. Классификация автоматизированных систем и требований по защите информации

Исключено с 1 февраля 2025 г. - Изменение N 1

Приложение Б (обязательное)

Средства вычислительной техники (СВТ). Показатели защищенности от НСД к информации по классам защищенности

Исключено с 1 февраля 2025 г. - Изменение N 1

Библиография

[1] Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России). Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г., М.: 1992

[2] Руководящий документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности

от несанкционированного доступа к информации". Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России). Утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г., М.: 1992

[3] ПУЭ-76 Правила устройства электроустановок, утверждены Главным техническим управлением по эксплуатации энергосистем и Государственной инспекцией по энергонадзору Министерства энергетики и электрификации СССР. 6-е и 7-е издания. Издательство ДЕАН. М.: 2008

[4] Правила техники безопасности при эксплуатации электроустановок потребителей. Утверждены Главгосэнергонадзором 21.12.1984 г. Издание 4-е. Издательство АОЗТ "Энергосервис". М.: 1994

[5] Единые правила безопасности при взрывных работах. Утверждены Госгортехнадзором 24 марта 1992 г. Издательство НПО ОБТ, Москва, 1992

[6] Исключен с 1 февраля 2025 г. - Изменение N 1