ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

ГОСТ Р 51241-2008

Группа П77

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Классификация. Общие технические требования. Методы испытаний

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

ОКС 13.320
ОКП 43 7200

Дата введения 2009-09-01

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения"

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным учреждением Научно-исследовательский центр "ОХРАНА" (ФГУ НИЦ "ОХРАНА") МВД России, Центром оперативного руководства деятельностью вневедомственной охраны (ЦОРДВО) МВД России и Всероссийским научно-исследовательским институтом стандартизации и сертификации в машиностроении (ВНИИНМАШ)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 234 "Системы тревожной сигнализации и противокриминальной защиты"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2008 г. N 430-ст

4 ВЗАМЕН ГОСТ Р 51241-98

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "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

1 Область применения

Настоящий стандарт распространяется на средства и системы контроля и управления доступом, предназначенные для предотвращения несанкционированного доступа людей, транспорта и других объектов в зону (из зоны) доступа (здания, помещения, территории, транспортные средства) 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 8.568-97 Государственная система обеспечения единства измерений. Аттестация испытательного оборудования. Основные положения

ГОСТ Р 15.201-2000 Система разработки и постановки продукции на производство. Продукция производственно-технического назначения

ГОСТ Р ИСО/МЭК 7810-2002* Карты индентификационные. Физические характеристики

---

* На территории Российской Федерации действует ГОСТ Р ИСО/МЭК 7810-2006, здесь и далее по тексту. - Примечание изготовителя базы данных.

ГОСТ Р ИСО/МЭК 7811-1-2003 Карты идентификационные. Способ записи. Часть 1. Тиснение

ГОСТ Р ИСО/МЭК 7811-2-2002 Карты идентификационные. Способ записи. Часть 2. Магнитная полоса малой коэрцитивной силы

ГОСТ Р ИСО/МЭК 7811-3-2003 Карты идентификационные. Способ записи. Часть 3. Расположение рельефных символов на картах формата ID-1

ГОСТ Р ИСО/МЭК 7811-6-2003 Карты идентификационные. Способ записи. Часть 6. Магнитная полоса большой коэрцитивной силы

ГОСТ Р ИСО/МЭК 7816-1-2002 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 7816-2-2002 Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 2. Размеры и расположение контактов

ГОСТ Р ИСО/МЭК 7816-4-2004 Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 4. Межотраслевые команды для обмена

ГОСТ Р ИСО/МЭК 7816-6-2003 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 6. Элементы данных для межотраслевого 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 10373-1-2002 Карты идентификационные. Методы испытаний. Часть 1. Общие характеристики

ГОСТ Р ИСО/МЭК 10373-2-2002 Карты идентификационные. Методы испытаний. Часть 2. Карты с магнитной полосой

ГОСТ Р ИСО/МЭК 10536-2-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Часть 2. Размеры и расположение зон связи

ГОСТ Р ИСО/МЭК 10536-3-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Часть 3. Электронные сигналы и процедуры восстановления

ГОСТ Р ИСО/МЭК 11693-2004 Карты идентификационные. Карты с оптической памятью. Общие характеристики

ГОСТ Р ИСО/МЭК 11694-1-2003 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 11694-2-2003 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 2. Размеры и расположение оптической зоны

ГОСТ Р ИСО/МЭК 11694-3-2003 Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Часть 3. Оптические свойства и характеристики

ГОСТ Р ИСО/МЭК 15693-1-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 1. Физические характеристики

ГОСТ Р ИСО/МЭК 15693-2-2004 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 2. Воздушный интерфейс и инициализация

ГОСТ Р ИСО/МЭК 15963-2005 Автоматическая идентификация. Радиочастотная идентификация для управления предметами. Уникальная идентификация радиочастотных меток

ГОСТ Р ИСО/МЭК 19794-2-2005 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки

ГОСТ Р ИСО/МЭК 19794-4-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ГОСТ Р ИСО/МЭК 19794-5-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ГОСТ Р ИСО/МЭК 19794-6-2006 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

ГОСТ Р 50009-2000 Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний

ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 51053-97 Замки сейфовые. Требования и методы испытания на устойчивость к криминальному открыванию и взлому

ГОСТ Р 51072-2005 Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому, пулестойкость и огнестойкость

ГОСТ Р 51112-97 Средства защитные банковские. Требования по пулестойкости и методы испытаний

ГОСТ Р 51330.0-99 (МЭК 60079-0-98) Электрооборудование взрывозащищенное. Часть 0. Общие требования

ГОСТ Р 52436-2005 Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний

ГОСТ Р 52582-2006 Замки для защитных конструкций. Требования и методы испытаний на устойчивость к криминальному открыванию и взлому

ГОСТ Р 52931-2008 Приборы контроля и регулирования технологических процессов. Общие технические условия

ГОСТ Р МЭК 60065-2005 Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности

ГОСТ 2.601-2006 Единая система конструкторской документации. Эксплуатационные документы

ГОСТ 2.610-2006 Единая система конструкторской документации. Правила выполнения эксплуатационных документов

ГОСТ 12.1.004-91 Система стандартов безопасности труда. Пожарная безопасность. Общие требования

ГОСТ 12.1.006-84 Система стандартов безопасности труда. Электромагнитные поля радиочастот. Допустимые уровни на рабочих местах и требования к проведению контроля

ГОСТ 12.1.019-79 Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты

ГОСТ 12.2.003-91 Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности

ГОСТ 12.2.007.0-75 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения

ГОСТ 27.003-90 Надежность в технике. Состав и общие правила задания требований по надежности

ГОСТ 5089-2003 Замки и защелки для дверей. Технические условия

ГОСТ 14192-96 Маркировка грузов

ГОСТ 14254-96 (МЭК 529-89) Степени защиты, обеспечиваемые оболочками (код IP)

ГОСТ 15150-69 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 16962-71 Изделия электронной техники и электротехники. Механические и климатические воздействия. Требования и методы испытаний

ГОСТ 19091-2000 Замки и защелки для дверей. Методы испытаний

ГОСТ 26828-86 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:** Способность конструкции противостоять разрушающему воздействию.

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.

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:

- с частичным перекрытием (турникеты, шлагбаумы);

- с полным перекрытием (полноростовые турникеты, специализированные ворота);

- со сплошным перекрытием проема (сплошные двери, ворота);

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

4.1.3.2 УИ - по способу запирания:

- 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 классифицируют по устойчивости к разрушающим воздействиям.

Устойчивость УПУ устанавливают по:

1) устойчивости к взлому;

2) пулестойкости (только для УПУ со сплошным перекрытием проема);

3) устойчивости к взрыву.

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

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

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

4.3.4 По устойчивости к неразрушающим воздействиям средства 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 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

4.4.1 Условное обозначение указывают в стандартах и (или) нормативных документах на средства КУД конкретного типа.

Размещение символа условного обозначения средства КУД должно быть осуществлено как часть технической информации и не должно быть совмещено с обозначением торговой марки.

4.4.2 Условное обозначение средств КУД в документации и заказе должно содержать:

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

б) аббревиатуру СКУД;

в) группу символов обозначений в соответствии с 4.4.3;

г) обозначение технических условий (ТУ).

Таблица 1 - Наименование и сокращенное обозначение средств КУД

Наименование средств КУД	Сокращенное обозначение
Устройство преграждающее управляемое	УПУ
Устройство исполнительное	УИ
Устройство считывающее (считыватель)	УС
Идентификатор	ИД

Средства управления - аппаратные устройства: - контроллер доступа - прибор приемно-контрольный доступа Средства управления - программные: программное обеспечение	 КД ППКД ПО

4.4.3 Структура группы символов обозначения для различных средств КУД:

$$X_1X_2 - X_3/X_4X_5,$$

где - классификация по функциональным характеристикам в соответствии с таблицей 2;

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

- порядковый номер разработки средства КУД;

- обозначение конструктивного исполнения;

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

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

Таблица 2 - Обозначение классификации по функциональным характеристикам средств КУД

Средства КУД по функциональному назначению	Классификация по функциональным характеристикам	Обозначение
УПУ - по виду перекрытия прохода	С частичным перекрытием (турникеты, шлагбаумы)	1
	С полным перекрытием (полноростовые турникеты, специализированные ворота)	2
	Со сплошным перекрытием проема (сплошные двери, ворота)	3
	С блокированием объекта в проеме (шлюзы,	4

	кабины проходные)	
УИ	Электромеханические замки	1
- по способу запирания		
	Электромагнитные замки	2
	Электромагнитные защелки	3
	Механизмы привода ворот	4
УС	С ручным вводом	1
- по способу считывания идентификационных признаков		
	Контактные	2
	Бесконтактные	3
	Биометрические	4
	Комбинированные	5
ИД	Механические	1
- по виду идентификационных признаков		
	Магнитные	2
	Оптические	3
	Электронные контактные	4
	Электронные радиочастотные	5
	Акустические	6
	Комбинированные	7
КД, ППКД	Автономный	1
- по способу управления		
	Централизованный	2
	Универсальный	3

Пример условного обозначения

идентификатора КУД электронного радиочастотного, нормальной устойчивости к НСД, порядкового номера разработки 5, конструктивного исполнения 8, модификации А:

*ИД СКУД 5Н - 5/8А ТУ**

---

* Приводится обозначение ТУ.

4.4.4 Условное обозначение систем КУД в документации и при заказе должно состоять из:

а) наименования "Система контроля и управления доступом" или сокращенно СКУД;

в) группы символов в соответствии с 4.4.5;

д) обозначения ТУ.

4.4.5 Структура группы символов обозначения системы КУД:

$$X_1X_2X_3X_4 - X_5/X_6X_7,$$

где - способ управления:

1 - автономное,

2 - централизованное (сетевое);

3 - универсальное (сетевое),

- число контролируемых точек доступа:

1 - система малой емкости,

2 - система средней емкости,

3 - система большой емкости;

- класс по функциональным характеристикам;

- класс защищенности системы от несанкционированного доступа к информации для систем повышенной и высокой устойчивости к НСД или буква "Н" для систем нормальной устойчивости;

- порядковый номер разработки;

- обозначение конструктивного исполнения;

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

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

Пример условного обозначения

системы контроля и управления доступом сетевой, малой емкости, второго класса по функциональным возможностям, нормальной устойчивости к НСД, номера разработки 7, конструктивного исполнения 9, модернизации - Б:

*СКУД - 212Н-7/9Б ТУ**

_____

* Приводится обозначение ТУ.

5 Технические требования

5.1 Общие положения

5.1.1 Разработка и постановка на производство средств и систем контроля управления доступом должны проводиться в соответствии с ГОСТ Р 15.201.

5.1.2 Конструкторская документация на средства и системы КУД должна соответствовать требованиям ЕСКД. Эксплуатационные документы должны быть выполнены в соответствии с ГОСТ 2.601 и ГОСТ 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.

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 УИ

5.2.1.1 УПУ в закрытом состоянии должны обеспечивать физическое препятствие доступу в соответствии с классификацией по виду перекрытия проема:

- частичное перекрытие (турникеты, шлагбаумы);

- полное перекрытие (полноростовые турникеты, специализированные ворота);

- сплошное перекрытие проема (сплошные двери, сплошные ворота);

- блокирование объекта в проеме (шлюзы, кабины проходные).

5.2.1.2 УПУ в рабочем режиме могут быть двух следующих типов:

- тип 1 - нормально открытые;

- тип 2 - нормально закрытые.

Нормально открытые УПУ должны быть оснащены датчиком приближения субъекта и объекта доступа, обеспечивать свободный проход при санкционированном доступе и переходить в закрытое состояние, если доступ не санкционирован.

Нормально закрытые УПУ должны открываться при санкционированном доступе.

5.2.1.3 УПУ с частичным перекрытием проема при необходимости должны быть оснащены средствами сигнализации, срабатывающими при попытке обхода преграждающего устройства.

5.2.1.4 Для УПУ, используемых на проходных или в других местах с большим скоплением людей, в стандартах или ТУ на УПУ конкретного типа должны быть установлены показатели пропускной способности.

5.2.1.5 УПУ при санкционированном доступе должны переходить в открытое состояние при подаче управляющего сигнала на УИ от устройства управления.

Параметры управляющего сигнала (напряжение, ток и длительность) должны быть указаны в нормативных документах на УПУ конкретного типа.

Нормально закрытые УПУ при необходимости должны быть оборудованы средствами звуковой сигнализации, которая включается после их открывания и при отсутствии прохода в течение установленного времени, и должны иметь средства возвращения в закрытое состояние.

5.2.1.6 УПУ при необходимости должны иметь защиту от прохода через них одновременно двух или более человек.

5.2.1.7 УПУ должны иметь возможность механического аварийного открывания в случае пропадания электропитания, возникновения пожара или других чрезвычайных ситуаций. Аварийная система открывания должна быть защищена от использования ее для несанкционированного проникновения.

5.2.1.8 В конструкции УПУ должны быть предусмотрены меры защиты внешних электрических соединительных цепей УПУ от несанкционированных воздействий (подачи напряжения, обрыва, короткого замыкания), приводящих к открыванию УПУ.

5.2.1.9 УПУ могут иметь дополнительные средства специального контроля (металлодетекторы, обнаружители радиоактивных веществ и др.), встроенные или совместно функционирующие с устройством преграждающим управляемым. Требования к УПУ, в состав которых входят встроенные средства специального контроля, устанавливают в нормативных документах на устройства преграждающие управляемые конкретного типа.

5.2.1.10 УПУ с высоким уровнем устойчивости к НСД и пулестойкости со сплошным перекрытием прохода должны соответствовать требованиям ГОСТ Р 51072.

5.2.1.11 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, электромеханическим защелкам) должны соответствовать ГОСТ Р 52582, ГОСТ 19091, ГОСТ 5089, ГОСТ Р 51053.

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 ИСО/МЭК 19794-6.

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 7811-3, 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, 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 Р ИСО/МЭК 15963.

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.

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.			

В систему любого класса могут быть введены дополнительные характеристики.

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 устойчивости к воздействию электромагнитных помех должны иметь следующие степени жесткости по ГОСТ Р 50009:

- первую или вторую - при нормальной устойчивости;

- третью - при повышенной устойчивости;

- четвертую или пятую - при высокой устойчивости.

Требования по устойчивости к электромагнитным помехам предъявляются к устройствам, имеющим степень жесткости не ниже второй, и должны быть установлены в ТУ на средства и системы КУД конкретного типа.

5.4.2 Уровень допустимых помех при работе средств и систем КУД должен соответствовать ГОСТ Р 50009.

5.5 Требования к устойчивости средств и систем КУД к НСД

5.5.1 Требования к устойчивости к НСД разрушающего действия распространяются на УПУ, за исключением УПУ с частичным перекрытием проема. Требования включают в себя:

- устойчивость к взлому;

- пулестойкость (только для УПУ со сплошным перекрытием проема);

- устойчивость к взрыву.

5.5.2 Нормальная устойчивость УПУ должна обеспечиваться механической прочностью конструкции без оценки по показателям устойчивости к разрушающим воздействиям.

5.5.3 Для УПУ повышенной устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и с блокированием объекта в проеме (шлюзы, кабины проходные) должны обеспечиваться требования по устойчивости к взлому как для защитных дверей по ГОСТ Р 51072.

5.5.4 Для УПУ высокой устойчивости со сплошным перекрытием проема (сплошные двери, ворота) и блокированием объекта в проеме (шлюзы, кабины проходные) должны обеспечиваться дополнительно требования по устойчивости к взрыву и пулестойкости как для защитных дверей по ГОСТ Р 51072.

5.5.5 Замки, защелки, используемые в СКУД, по устойчивости к разрушающим воздействиям в зависимости от конструкции должны соответствовать требованиям ГОСТ Р 52582, ГОСТ Р 51053, ГОСТ 19091, ГОСТ 5089.

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 средств 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 средств СВТ, входящих в состав СКУД повышенной и высокой устойчивости, требования к защите средств СВТ от несанкционированного доступа к информации

устанавливают по классам в соответствии с [2] и приложением Б.

При этом классы защиты средств 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 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 ТУ на конкретные средства и системы могут быть установлены дополнительные требования к надежности.

5.6.2 Средняя наработка на отказ СКУД на одну точку доступа (без учета УПУ) должна быть не менее 10000 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 Основное электропитание средств и систем КУД должно осуществляться от сети переменного тока частотой 50 Гц номинальным напряжением 220 В.

Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения сети от минус 15% до плюс 10%.

Электропитание отдельных средств КУД допускается осуществлять от других источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на средства КУД конкретных типов.

5.8.2 Средства и системы КУД должны быть снабжены резервным электропитанием при пропадании напряжения основного источника питания. В качестве резервного источника питания может использоваться резервная сеть переменного тока или источники питания постоянного тока.

Номинальное напряжение резервного источника питания постоянного тока выбирают из ряда: 12; 24 В.

Примечание - В технически обоснованных случаях допускается устанавливать напряжение питания по согласованию с потребителем.

Переход на резервное питание должен осуществляться 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% номинального значения.

5.8.3 Резервный источник питания должен обеспечивать выполнение основных функций системы при пропадании напряжений в сети на время не менее 0,5 ч для систем первого и второго классов 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 и системными средствами индикации аварии электропитания.

5.8.4 При использовании в качестве источника резервного питания аккумуляторных батарей должен выполняться их автоматический заряд.

5.8.5 При использовании в качестве источника резервного питания СКУД аккумуляторных или сухих батарей рекомендуется иметь индикацию разряда батареи ниже допустимого предела. Для автономных систем СКУД индикация разряда может быть световой или звуковой, для сетевых систем сигнал разряда батарей может передаваться на пункт управления.

5.8.6 Химические источники питания, встроенные в идентификаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность средств КУД в течение не менее трех лет.

5.9 Требования безопасности

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

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

5.9.7 Уровни излучений средств и систем КУД должны соответствовать нормам и требованиям безопасности, установленным в ГОСТ 12.1.006.

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, [3]-[5].

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 Испытания на устойчивость УПУ к НСД разрушающего воздействия (см. 5.5.2) проводят методами испытаний по ГОСТ Р 51072.

6.2.5 Испытания на устойчивость УИ к НСД разрушающего воздействия (см. 5.5.3) проводят методами испытаний по ГОСТ Р 52582, ГОСТ Р 51053, ГОСТ 19091, ГОСТ 5089.

6.2.6 Испытания на устойчивость средств КУД к НСД неразрушающего воздействия (см. 5.5.4) проводят методами испытаний в соответствии с нормативными документами на средства и системы КУД конкретного типа.

6.2.7 Испытания по защите программного обеспечения СКУД от несанкционированного доступа (см. 5.5.5) систем КУД с централизованным управлением и универсальных от несанкционированного доступа к информации и защите средств СВТ, входящих в состав СКУД, от несанкционированного доступа к информации (см. 5.5.6) 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.

Приложение А (обязательное). Автоматизированные системы. Классификация автоматизированных систем и требований по защите информации

Приложение А
(обязательное)

А.1 Классификация автоматизированных систем

Классификация автоматизированных систем - по [1] и таблице А.1.

Таблица А.1 - Требования к автоматизированным системам по группам

Подсистемы и требования	Группы и классы				
	3		2	1	
	3Б	3А	2Б	1Г	1В
1 Подсистема управления доступом					
1.1 Идентификация, проверка подлинности и контроль доступа субъектов:					
- в систему	+	+	+	+	+
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам	-	-	-	+	+

связи, внешним устройствам ЭВМ					
- к программам	-	-	-	+	+
- к томам, каталогам, файлам, записям, полям записей	-	-	-	+	+
1.2 Управление потоками информации	-	-	-	-	+
2 Подсистема регистрации и учета					
2.1 Регистрация и учет:					
- входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+
- выдачи печатных (графических) выходных документов	-	+	-	+	+
- запуска/завершения программ и процессов (заданий, задач)	-	-	-	+	+
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-	-	+	+
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	-	-	+	+
- изменения полномочий субъектов доступа	-	-	-	-	+
- создаваемых защищаемых объектов доступа	-	-	-	-	+
2.2 Учет носителей информации	+	+	+	+	+
2.3 Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	+
2.4 Сигнализация попыток нарушения защиты	-	-	-	-	+
3 Подсистема обеспечения целостности					
3.1 Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+
3.2 Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+
3.3 Наличие администратора (службы) защиты информации в АС	-	-	-	-	+
3.4 Периодическое тестирование СЗИ НСД	+	+	+	+	+
3.5 Наличие средств восстановления СЗИ НСД	+	+	+	+	+
3.6 Использование сертифицированных средств защиты	-	+	-	-	+

Примечание - Знак "+" означает наличие требований к данному классу, знак "-" - отсутствие требования к данному классу.

А.2 Пояснения к требованиям

А.2.1 Термины и определения к приложению А

А.2.1.1

аутентификация: Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

[6], статья 17

А.2.1.2

безопасность информации: Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз.

[6], статья 21

А.2.1.3

дискреционное управление доступом: Разграничение доступа между поименованными субъектами и объектами; субъект с определенным правом доступа может передать это право любому другому субъекту.

[6], статья 24

А.2.1.4

доступ к информации: Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

[6], статья 1

А.2.1.5

защита от несанкционированного доступа (защита от НСД): Предотвращение или существенное затруднение несанкционированного доступа.

[6], статья 5

А.2.1.6

класс защищенности средств вычислительной техники (автоматизированной системы): Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

[6], статья 32

А.2.1.7

несанкционированный доступ к информации (НСД): Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание - Под "штатными средствами" понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

[6], статья 4

А.2.1.8

объект доступа: Единица информационного ресурса автоматизированной системы доступ к которой регламентируется правилами разграничения доступа.

[6], статья 7

А.2.1.9

пароль: Идентификатор субъекта доступа, который является его (субъекта) секретом.

[6], статья 16

А.2.1.10

правила разграничения доступа: Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

[6], статья 2

А.2.1.11

санкционированный доступ к информации: Доступ к информации, не нарушающий правила разграничения доступа.

[6], статья 3

А.2.1.12

сертификация уровня защиты: Процесс установления соответствия средств вычислительной техники или автоматизированной системы набору определенных требований по защите.

[6], статья 38

А.2.1.13

средство защиты от несанкционированного доступа (средство защиты от НСД): Программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа.

[6], статья 19

А.2.1.14

субъект доступа: Лицо или процесс, действия которого регламентируются правилами разграничения доступа.

[6], статья 3

А.2.1.15

уровень полномочий субъекта доступа: Совокупность прав доступа субъектов доступа.

[6], статья 8

А.2.1.16

целостность информации: Способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения). [6], статья 22

А.3 Подсистема управления доступом

А.3.1 Идентификация, проверка подлинности и контроль доступа субъектов должны осуществляться:

- при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов; при их числе менее шести - система не может классифицироваться по данным требованиям и ее класс может быть только седьмым;

- при доступе к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ по логическим именам и/или адресам;

- при доступе к программам, томам, каталогам, файлам, записям, полям записи по именам;

- к защищенным ресурсам в соответствии с матрицей доступа.

А.3.2 Управление потоками информации должно осуществляться с помощью меток конфиденциальности; при этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

А.4 Подсистема регистрации и учета

А.4.1 Подсистема должна осуществлять регистрацию:

- входа/выхода субъектов доступа в систему/из системы либо регистрацию загрузки и инициализацию операционной системы и ее программного останова;

- выдачи печатных (графических) документов на "твердую" копию с автоматической маркировкой каждого листа (страницы);

- запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;

- попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

- попыток доступа программных средств к дополнительным защищаемым объектам доступа в виде терминалов, узлов сети и внешним устройствам ЭВМ, линиям связи, программам, файлам и т.п.;

- изменений полномочий субъектов доступа и статуса объектов доступа.

А.4.2 Подсистема должна осуществлять учет:

- создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом;

- всех защищаемых носителей информации с помощью их любой маркировки и регистрацией защищаемых носителей в картотеке с дублированием учета.

А.4.3 Подсистема должна осуществлять очистку двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации.

При регистрации и учете указывают время и дату, характеристики и результаты проведенной операции.

А.4.4 Подсистема должна осуществлять сигнализацию попыток нарушения защиты.

А.5 Подсистема обеспечения целостности

А.5.1 Подсистема должна осуществлять целостность программных средств СЗИ НСД установлением при загрузке системы по контрольным суммам компонент СЗИ и обеспечением использования трансляторов с языками высокого уровня и отсутствием средств модификации объектного кода программ при обработке и/или хранении защищаемой информации.

А.5.2 Физическая охрана средств вычислительной техники должна предусматривать постоянное наличие охраны с помощью технических средств и специального персонала с использованием определенного пропускного режима.

А.5.3 Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

А.5.4 Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводиться не реже одного раза в год.

А.5.5 Средства восстановления СЗИ НСД должны предусматривать ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

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

Приложение Б
(обязательное)

Б.1 Показатели защищенности от НСД к информации

Показатели защищенности от НСД к информации по классам защищенности - по [1] и таблице Б.1.

Таблица Б.1

Наименование показателя	Класс защищенности		
	6	5	4
1 Дискреционный принцип контроля доступа	+	+	+
2 Мандатный принцип контроля доступа	-	-	+
3 Очистка памяти	-	+	+
4 Изоляция модулей	-	-	+
5 Маркировка документов	-	-	+
6 Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+
7 Сопоставление пользователя с устройством	-	-	+
8 Идентификация и аутенфикация	-	=	+
9 Гарантии проектирования	-	+	+
10 Регистрация	-	+	+
11 Целостность КСЗ	-	+	+
12 Тестирование	+	+	+
13 Руководство пользователя	+	=	=
14 Руководство по КСЗ	+	+	=
15 Тестовая документация	+	+	+
16 Конструкторская (проектная) документация	+	+	+
Примечание - Знак "-" означает отсутствие требования к данному классу, знак "+" - наличие новых или дополнительных требований, знак "=" - требования совпадают с требованиями к СВТ предыдущего класса.			

Б.2 Пояснения к требованиям по показателям защищенности

Б.2.1 Дискреционный принцип контроля доступа

Б.2.1.1 Дискреционный принцип контроля доступа по всем классам защищенности

Комплекс средств защиты (КСЗ) должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

Для каждой пары (субъект - объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа ("читать", "писать" и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа (ПРД).

Контроль доступа должен быть применим к каждому объекту и субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможность санкционированного изменения ПРД, в том числе санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

Б.2.1.2 Дополнительно к классу 5 защищенности

Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Б.2.1.3 Дополнительно по классу 4 защищенности

КЗИ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, недопустимого с точки зрения заданного ПРД). Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств - системных макрокоманд, инструкций языков высокого уровня и т.д., а под "скрытыми" - иные действия, в том числе с использованием собственных программ работы с устройствами.

Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

Б.3 Мандатный принцип контроля доступа

Для реализации мандатного принципа каждому субъекту и каждому объекту должны сопоставляться классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление КСЗ классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступах со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его дискреционными и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

Б.4 Очистка памяти

Б.4.1 По классу 5: при первоначальном назначении или перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

Б.4.2 По классу 6: при первоначальном назначении или перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При

перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

Б.5 Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта) от программных модулей других процессов (других субъектов) - т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

Б.6 Маркировка документов

При выводе защищаемой информации на документ в начале и конце проставляют штамп N 1 и заполняют его реквизиты в соответствии с [2].

Б.7 Защита ввода и вывода на отчуждаемый физический носитель информации

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (вывода на "помеченное" устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с "помеченным" каналом связи.

Изменения в назначении и разметке устройств и каналов должны вноситься только под контролем КСЗ.

Б.8 Сопоставление пользователя с устройствами

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство, как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

Б.9 Идентификация и аутентификация

Б.9.1 По классам защищенности 6 и 5

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации, т.е. осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации

которых при аутентификации не подтвердилась.

Б.9.2 Дополнительно по классу защищенности 4

КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

Б.10 Гарантии проектирования

Б.10.1 По классу защищенности 5

На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.

Б.10.2 Дополнительно по классу защищенности 4

Гарантии проектирования должны включать правила работы с устройствами ввода и вывода информации и каналами связи.

Б.11 Регистрация

Б.11.1 По классу защищенности 5

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;

- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);

- создание и уничтожение объекта;

- действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;

- субъект, осуществляющий регистрируемое действие;

- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);

- успешно ли осуществилось событие (обслужен или нет запрос на доступ).

КСЗ должен содержать средства выборочного ознакомления с регистрационной

информацией.

Б.11.2 Дополнительно по классу 4 регистрация должна включать в себя требование регистрировать все попытки доступа, действия оператора и выделенных пользователей (администраторов защиты и т.п.).

Б.12 Целостность КСЗ

Б.12.1 Целостность КСЗ по классу защищенности 5

В СВТ данного класса защищенности должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

Б.12.2 По классу защищенности 4

В СВТ данного класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться отдельной части оперативной памяти.

Б.13 Тестирование

Б.13.1 По классу защищенности 6 должны тестироваться:

- реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

- успешное осуществление идентификации и аутентификации, а также их средств защиты.

Б.13.2 Дополнительно по классу 5 должны тестироваться:

- очистка памяти в соответствии с Б.4.1;

- регистрация событий в соответствии с Б.11.1, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;

- работа механизма, осуществляющего контроль за целостностью КСЗ.

Б.13.3 По классу 4 должны тестироваться:

- реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными

и мандатными правилами, верное сопоставление меток субъектам и объектам, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);

- невозможность присвоения себе субъектом новых прав;

- очистка оперативной и внешней памяти;

- работа механизма изоляции процессов в оперативной памяти;

- маркировка документов;

- защита ввода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;

- идентификация и аутентификация, а также их средства защиты;

- запрет на доступ несанкционированного пользователя;

- работа механизма, осуществляющего контроль за целостностью СВТ;

- регистрация событий, описанных в Б.11.2, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

Б.14 Руководство пользователя

Руководство пользователя по документации для всех классов должно включать в себя описание способов использования КСЗ и его интерфейса с пользователем.

Б.15 Руководство по КСЗ

Документ адресован администрации защиты.

Б.15.1 По классу 6 руководство по КСЗ должно содержать:

- описание контролируемых функций;

- руководство по генерации КСЗ;

- описание старта СВТ и процедур проверки правильности старта.

Б.15.2 Дополнительно по классам 5 и 4 руководство по КСЗ должно содержать описание процедур работы со средствами регистрации.

Б.16 Тестовая документация

Тестовая документация должна содержать описание применяемых тестов (см. Б.13),

испытаний и результатов тестирования.

Б.17 Конструкторская (проектная) документация

Б.17.1 По классу защищенности 6 конструкторская (проектная) документация должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

Б.17.2 По классу 5 конструкторская (проектная) документация должна содержать описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ, модель защиты, описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

Б.17.3 По классу защищенности 4 конструкторская (проектная) документация должна содержать:

- общее описание принципов работы СВТ;

- общую схему КСЗ;

- описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;

- описание модели защиты;

- описание диспетчера доступа;

- описание механизма контроля целостности КСЗ;

- описание механизма очистки памяти;

- описание механизма изоляции программ в оперативной памяти;

- описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством;

- описание механизма идентификации и аутентификации;

- описание средств регистрации.

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

---

* На территории Российской Федерации действуют "Межотраслевые правила по охране труда (правила безопасности) при эксплуатации электроустановок" (ПОТ Р М-016-2001, РД 153-34.0-03.150-00). - Примечание изготовителя базы данных.

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

[6] Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомисия России. М.: 1992

Электронный текст документа
подготовлен ЗАО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2009