ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Классификация
Общие технические требования
Методы испытаний

Издание официальное

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН Научно-исследовательским центром «Охрана» (НИЦ «Охрана») Главного управления вневедомственной охраны (ГУВО) МВД России с участием рабочей группы специалистов научно-исследовательского института спецтехники (НИИСТ) МВД России, Государственного унитарного предприятия (ГУП) специального Научно-производственного объединения (СНПО) «Элерон», войсковой части 31600, Гостехкомиссии России, Всероссийского научно-исследовательского института стандартизации и сертификации в машиностроении (ВНИИНМАШ) Госстандарта России

ВНЕСЕН Техническим комитетом по стандартизации ТК 234 «Технические средства охраны, охранной и пожарной сигнализации»

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 29 декабря 1998 г. № 472

3 ВВЕДЕН ВПЕРВЫЕ

4 ПЕРЕИЗДАНИЕ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Классификация
Общие технические требования
Методы испытаний

Access control systems and units.
Classification. General technical requirements. Methods of tests

Дата введения 2000—01—01

1 Область применения

Настоящий стандарт распространяется на технические системы и средства контроля и управления доступом, предназначенные для контроля и санкционирования доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

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

Настоящий стандарт распространяется на вновь разрабатываемые и модернизируемые средства и системы контроля и управления доступом.

Требования, изложенные в 5.3, 5.4, 5.8, являются обязательными.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 8.568—99/ГОСТ Р 8.571—98 Государственная система обеспечения единства измерений. Термометры сопротивления платиновые эталонные 1-го и 2-го разрядов. Методика поверки

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 12.1.010—76 Система стандартов безопасности труда. Взрывобезопасность. Общие требования

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 20.57.406—81 Комплексная система контроля качества. Изделия электронной техники, квантовой электроники и электротехнические. Методы испытаний

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 12997—84 Изделия ГСП. Общие технические условия

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

Издание официальное

ГОСТ 16962—71 Изделия электронной техники и электротехники. Механические и климатические воздействия. Требования и методы испытаний

ГОСТ 16962.1—89 (МЭК 68-2-1—74) Изделия электротехнические. Методы испытаний на устойчивость к климатическим внешним воздействующим факторам

ГОСТ 16962.2—90 Изделия электротехнические. Методы испытаний на стойкость к механическим внешним воздействующим факторам

ГОСТ 17516—72 Изделия электротехнические. Условия эксплуатации в части воздействия механических факторов внешней среды

ГОСТ 17516.1—90 Изделия электротехнические. Общие требования в части стойкости к механическим внешним воздействующим факторам

ГОСТ 21552—84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение

ГОСТ 23773—88 Машины вычислительные электронные цифровые общего назначения. Методы испытаний

ГОСТ 24686—81 Оборудование для производства изделий электронной техники и электротехники. Общие технические требования. Маркировка, упаковка, транспортирование и хранение

ГОСТ 26139—84 Интерфейс для автоматизированных систем управления рассредоточенными объектами. Общие требования

ГОСТ 27570.0—87 (МЭК 335-1—76) Безопасность бытовых и аналогичных электрических приборов. Общие требования и методы испытаний

ГОСТ 28195—89 Оценка качества программных средств. Общие положения

ГОСТ 30109—94 Двери деревянные. Методы испытаний на сопротивление взлому

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 50775—95 (МЭК 839-1-1—88) Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения

ГОСТ Р 50776—95 (МЭК 839-1-4—89) Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию

ГОСТ Р 50862—96 Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость

ГОСТ Р 50941—96 Кабина защитная. Общие технические требования и методы испытаний

ГОСТ Р 51072—97 Двери защитные. Общие технические требования и методы испытаний на устойчивость к взлому и пулестойкость

ГОСТ Р 51112—97 Средства защитные банковские. Требования по пулестойкости и метод испытаний

ГОСТ Р 51317.4.2—99 (МЭК 61000-4-2—95) Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний

ГОСТ Р 51317.4.3—99 (МЭК 61000-4-3—95) Совместимость технических средств электромагнитная. Устойчивость к радиочастотному электромагнитному полю. Требования и методы испытаний

ГОСТ Р 51317.4.4—99 (МЭК 61000-4-4—95) Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Требования и методы испытаний

ГОСТ Р 51317.4.5—99 (МЭК 61000-4-5—95) Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Требования и методы испытаний

ГОСТ Р 51317.4.11—99 (МЭК 61000-4-11—94) Совместимость технических средств электромагнитная. Устойчивость к динамическим изменениям напряжения электропитания. Требования и методы испытания

ГОСТ Р 51318.4.1—99 (СИСПР 14-1—93) Совместимость технических средств электромагнитная. Радиопомехи индустриальные от бытовых приборов, электрических инструментов и аналогичных устройств. Нормы и методы испытаний

ГОСТ Р МЭК 60065—2002 Аудио-, видео- и аналогичная электронная аппаратура. Требования безопасности

3 Определения, обозначения и сокращения

В настоящем стандарте применяют следующие термины с соответствующими определениями.

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

несанкционированный доступ: Доступ людей или объектов, не имеющих права доступа.

санкционированный доступ: Доступ людей или объектов, имеющих права доступа.

контроль и управление доступом (КУД): Комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

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

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

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

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

идентификатор доступа, идентификатор (носитель идентификационного признака): Уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код, — предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и т.д.).

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

запоминаемый код: Код, вводимый вручную с помощью клавиатуры, кодовых переключателей или других подобных устройств.

устройства преграждающие управляемые (УПУ): Устройства, обеспечивающие физическое препятствие доступу людей, транспорта и других объектов и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т.п. конструкции).

устройства исполнительные: Устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние УПУ (электромеханические и электромагнитные замки, защелки, механизмы привода шлюзов, ворот, турникетов и т.д.).

устройства ввода идентификационных признаков (УВИП): Электронные устройства, предназначенные для ввода запоминаемого кода, ввода биометрической информации, считывания кодовой информации с идентификаторов. В состав УВИП входят считыватели и идентификаторы.

считыватель: Устройство в составе УВИП, предназначенное для считывания (ввода) идентификационных признаков.

устройства управления (УУ): Устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с УВИП, управление УПУ, отображение и регистрацию информации.

точка доступа: Место, где непосредственно осуществляется контроль доступа (например дверь, турникет, кабина прохода, оборудованные считывателем, исполнительным механизмом, электромеханическим замком и другими необходимыми средствами).

зона доступа: Совокупность точек доступа, связанных общим местоположением или другими характеристиками (например точки доступа, расположенные на одном этаже).

временно́й интервал доступа (окно времени): Интервал времени, в течение которого разрешается перемещение в данной точке доступа.

уровень доступа: Совокупность временны́х интервалов доступа (окон времени) и точек доступа, которые назначаются определенному лицу или группе лиц, имеющим доступ в заданные точки доступа в заданные временны́е интервалы.

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

пропускная способность: Способность средства или системы КУД пропускать определенное количество людей, транспортных средств и т.п. в единицу времени.

несанкционированные действия (НСД): Действия, целью которых является несанкционированное проникновение через УПУ.

взлом: Действия, направленные на несанкционированное разрушение конструкции.

вскрытие: Действия, направленные на несанкционированное проникновение через УПУ без его разрушения.

манипулирование: Действия, производимые с устройствами контроля доступа без их разрушения, целью которых является получение действующего кода или приведение в открытое состояние заграждающего устройства. Устройства контроля доступа могут при этом продолжать правильно функционировать во время манипулирования и после него; следы такого действия не будут заметны. Манипулирование включает в себя также действия над программным обеспечением.

наблюдение: Действия, производимые с устройствами контроля и управления доступом без прямого доступа к ним, целью которых является получение действующего кода.

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

принуждение: Насильственные действия над лицом, имеющим право доступа, с целью несанкционированного проникновения через УПУ. Устройства контроля и управления доступом при этом могут функционировать нормально.

саботаж (состояние саботажа — по ГОСТ Р 50776): Преднамеренно созданное состояние системы, при котором происходит повреждение части системы.

устойчивость к взлому: Способность конструкции противостоять разрушающему воздействию без использования инструментов, а также с помощью ручных и других типов инструментов.

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

устойчивость к взрыву: Способность конструкции противостоять разрушающему действию взрывчатых веществ.

4 Классификация

4.1 Классификация средств КУД

4.1.1 Средства КУД классифицируют по:

- функциональному назначению устройств;
- устойчивости к НСД.

4.1.2 Средства КУД по функциональному назначению устройств подразделяют на:

- устройства преграждающие управляемые (УПУ) в составе преграждающих конструкций и исполнительных устройств;
- устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов;
- устройства управления (УУ) в составе аппаратных и программных средств.

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

По виду перекрытия проема прохода УПУ могут быть:

- с частичным перекрытием (турникеты, шлагбаумы);
- с полным перекрытием (сплошные двери, ворота);
- с блокированием объекта в проеме (шлюзы, кабины проходные).

По способу управления УПУ могут быть:

- с ручным управлением;
- с полуавтоматическим управлением;
- с автоматическим управлением.

4.1.4 УВИП классифицируют по следующим признакам:

- по виду используемых идентификационных признаков;
- по способу считывания идентификационных признаков.

По виду используемых идентификационных признаков УВИП могут быть:

- механические — идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);

- магнитные — идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т. д.);

- оптические — идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении (карты со штриховым кодом, голографические метки и т. д.);

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

- акустические — идентификационные признаки представляют собой кодированный акустический сигнал;

- биометрические — идентификационные признаки представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);

- комбинированные — для идентификации используются одновременно несколько идентификационных признаков.

По способу считывания идентификационных признаков УВИП могут быть:

- с ручным вводом — ввод производится с помощью нажатия клавиш, поворотом переключателей или других подобных элементов;

- контактные — ввод происходит при непосредственном, в том числе и при электрическом, контакте между считывателем и идентификатором;

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

- комбинированные.

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

4.1.6 Средства КУД к информации представляют собой программные, технические и программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации [1]. К этим средствам относятся также специальные защитные знаки (СЗЗ) [2]. СЗЗ представляют собой продукты, созданные на основе физико-химических технологий и предназначенные для контроля доступа к объектам защиты, а также для защиты документов, идентифицирующих личность, от подделки.

4.2 Классификация систем КУД

4.2.1 Системы КУД классифицируют по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;
- уровню защищенности системы от несанкционированного доступа к информации.

4.2.2 По способу управления системы КУД могут быть:

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

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

- универсальные — включающие функции как автономных, так и сетевых систем, работающие в сетевом режиме под управлением центрального устройства управления и переходящие в автономный режим при возникновении отказов в сетевом оборудовании, в центральном устройстве или обрыве связи.

4.2.3 По количеству контролируемых точек доступа системы КУД могут быть:

- малой емкости (менее 16 точек);
- средней емкости (не менее 16 и не более 64 точек);
- большой емкости (64 точки и более).

4.2.4 По функциональным характеристикам системы КУД могут быть трех классов:

1 — системы с ограниченными функциями;

2 — системы с расширенными функциями;

3 — многофункциональные системы.

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

4.2.5 По виду объектов контроля системы КУД могут быть:

- для контроля доступа физических объектов;
- для контроля доступа к информации.

4.3 Классификация средств и систем КУД по устойчивости к НСД

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

- нормальной;
- повышенной;
- высокой.

4.3.2 УПУ и УВИП классифицируют по устойчивости к разрушающим воздействиям.

Устойчивость УПУ устанавливают по:

- устойчивости к взлому;
- пулестойкости;
- устойчивости к взрыву.

Устойчивость УВИП устанавливают по устойчивости считывателя к взлому.

Для УПУ повышенной и высокой устойчивости устанавливают дополнительно 5 классов по показателям устойчивости (1-й класс — низший).

4.3.3 По устойчивости к неразрушающим воздействиям средства и системы КУД в зависимости от их функционального назначения классифицируют по следующим показателям:

- устойчивости к вскрытию — для УПУ и исполнительных устройств (замков и запорных механизмов);
- устойчивости к манипулированию;
- устойчивости к наблюдению — для УВИП с запоминаемым кодом (клавиатуры, кодовые переключатели и т.п.);
- устойчивости к копированию (для идентификаторов);
- устойчивости защиты средств вычислительной техники УУ от несанкционированного доступа к информации.

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

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

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

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

4.4 Условные обозначения средств и систем КУД

4.4.1 Условные обозначения средств и систем КУД указывают в стандартах и (или) нормативных документах на средства и системы КУД конкретного типа.

Размещение символа условного обозначения должно быть частью технической информации и не должно быть совмещено с обозначением торговой марки.

4.4.2 Условное обозначение систем КУД в документации и при заказе должно содержать:

а) название «Система»;

б) название класса системы по количеству контролируемых точек доступа и по способу управления;

в) обозначение КУД;

г) три символа (первый и второй с точкой), обозначающие:

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

д) обозначение настоящего стандарта;

е) условное обозначение по нормативной документации изготовителя или поставщика.

Пример условного обозначения системы сетевой малой емкости второго класса по функциональным возможностям, первой категории по устойчивости к электромагнитным помехам и класса 3А по защищенности системы от несанкционированного доступа к информации:

Система малой емкости сетевая КУД-2.1.3А ГОСТ Р ХХХХХ АБВГ.ХХХХХ ТУ

5 Общие технические требования

5.1 Общие положения

5.1.1 Средства и системы КУД должны изготовляться в соответствии с требованиями настоящего стандарта, ГОСТ Р 50775, а также стандартов и других нормативных документов на средства и системы КУД конкретного типа.

5.1.2 Средства и системы КУД должны обеспечивать возможность как круглосуточной, так и сменной работы, с учетом проведения регламентного технического обслуживания.

5.1.3 Средства КУД, предназначенные для построения систем, должны обладать конструктивной, информационной, надежностной и эксплуатационной совместимостью.

Параметры и требования, определяющие совместимость средств, должны быть установлены в зависимости от назначения и условий применения в нормативных документах на средства и системы КУД конкретного типа.

5.1.4 Требования к средствам контроля доступа вида — специальные защитные знаки (СЗЗ) устанавливают по документу [2].

5.2 Требования назначения

5.2.1 Требования к функциональным характеристикам систем КУД

5.2.1.1 Автономные системы КУД должны обеспечивать:

- открывание УПУ при считывании зарегистрированного в памяти системы идентификационного признака;
- запрет открывания УПУ при считывании незарегистрированного в памяти системы идентификационного признака;
- запись идентификационных признаков в память системы;
- защиту от несанкционированного доступа при записи кодов идентификационных признаков в памяти системы;
- сохранение идентификационных признаков в памяти системы при отказе и отключении электропитания;
- ручное, полуавтоматическое или автоматическое открывание УПУ для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- автоматическое формирование сигнала сброса на УПУ при отсутствии факта прохода;
- выдачу сигнала тревоги при использовании системы аварийного открывания УПУ для несанкционированного проникновения.

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

Таблица 1 — Функциональные характеристики автономных систем

Функциональные характеристики автономной системы	Класс системы		
	1	2	3
1 Установка уровней доступа	—	+/—	+
2 Установка временны́х интервалов доступа	—	+/—	+
3 Возможность установления времени открывания УПУ	—	+/—	+
4 Защита от повторного использования идентификатора для прохода в одном направлении	—	+/—	+
5 Ввод специального идентификационного признака для открывания под принуждением	—	+/—	+

Окончание таблицы 1

Функциональные характеристики автономной системы	Класс системы		
	1	2	3
6 Подключение УВИП различных типов	—	+/—	+/—
7 Доступ по «правилу двух (и более) лиц»	—	+/—	+/—
8 Световая индикация о состоянии доступа	+/—	+	+
9 Контроль состояния УПУ	+/—	+	+
10 Световое и (или) звуковое оповещение о попытках НСД	+/—	+/—	+
11 Регистрация и хранение информации о событиях в энергонезависимой памяти	—	+	+
12 Количество событий, хранимых в энергонезависимой памяти, не менее	—	16	64
13 Ведение даты и времени возникновения событий	—	+/—	+
14 Возможность подключения принтера для вывода информации	—	+/—	+
15 Возможность передачи информации на устройства сбора информации или ЭВМ	—	+/—	+
16 Возможность объединения в сеть и обмена информацией с устройствами сбора информации и управления (ЭВМ)	—	+/—	+
17 Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	—	+/—	+
18 Возможность интегрирования с системой видеоконтроля на релейном уровне	—	+/—	+
19 Возможность подключения дополнительных средств специального контроля, средств досмотра	—	—	+/—

Примечание — Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «—» — отсутствие функции, а знак «+/—» — наличие или отсутствие функции.

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

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

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

Таблица 2 — Функциональные характеристики систем с централизованным управлением и универсальных

Функциональные характеристики систем с централизованным управлением (сетевых) и универсальных	Класс системы		
	1	2	3
1 Количество уровней доступа	2	8	16
2 Количество временны́х интервалов доступа	2	8	16
3 Защита от повторного использования идентификатора для прохода в одном направлении	+/—	+	+
4 Ввод специального идентификационного признака для открывания под принуждением	+/—	+	+
5 Подключение УВИП различных типов	+/—	+	+
6 Доступ по «правилу двух (и более) лиц»	+/—	+/—	+
7 Количество событий, сохраняемых в энергонезависимой памяти контроллеров, не менее	50	250	1000
8 Возможность интегрирования с системой охранной и (или) пожарной сигнализации на релейном уровне	+	+/—	+/—
9 Возможность интегрирования с системой видеоконтроля на релейном уровне	+	+/—	+/—
10 Возможность интегрирования с системой охранной, пожарной сигнализации и системами видеоконтроля на системном уровне	+/—	+/—	+
11 Возможность управления работой дополнительных устройств в точках доступа (освещение, вентиляция, лифты, технологическое оборудование и т.п.)	—	+/—	+/—
12 Возможность подключения переговорных устройств и (или) средств связи в точках доступа	—	+/—	+/—
13 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	+/—	+/—	+
14 Интерактивное управление средствами по изображению плана объекта на экране ЭВМ	—	—	+/—
15 Ведение баз данных на сотрудников (пользователей)	+/—	+	+
16 Поддержание фотографических данных пользователей в базе данных	—	+/—	+
17 Контроль за перемещением и поиск сотрудников	+/—	+/—	+
18 Контроль времени нахождения на объекте посетителей	+/—	+/—	+

Примечание — Условный знак «+» означает наличие функции и обязательность ее проверки при установлении класса, знак «—» — отсутствие функции, а знак «+/—» — наличие или отсутствие функции.

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

5.2.1.6 Значения характеристик и требования, приведенные в 5.2.1.1—5.2.1.5, должны быть установлены в стандартах и (или) технических условиях на системы КУД конкретного типа.

Системы КУД должны также иметь следующие характеристики, значения которых должны быть установлены в стандартах и (или) технических условиях на системы конкретного типа:

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

5.2.1.7 По требованиям заказчика допускается устанавливать дополнительные характеристики и показатели в технических условиях на системы конкретного типа.

5.2.2 Требования к функциональным характеристикам УПУ

5.2.2.1 УПУ должны обеспечивать:

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

5.2.2.2 УПУ в дежурном режиме могут быть в нормально открытом или нормально закрытом состоянии.

УПУ с частичным перекрытием проема прохода могут быть, при необходимости, обеспечены средствами сигнализации, срабатывающими при попытке обхода заграждающего устройства.

Для УПУ, используемых на проходных или в других местах с большими потоками людей, в стандартах или технических условиях на УПУ конкретного типа должны быть установлены показатели пропускной способности.

5.2.2.3 УПУ в закрытом состоянии должны обеспечивать физическое препятствие перемещению людей, транспорта и других объектов в (из) помещение, здание, зону или на территорию и открывание запирающего механизма при подаче управляющего сигнала от устройства управления.

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

Нормально закрытые УПУ могут быть оборудованы средствами звуковой сигнализации, которая включается после их открывания и при отсутствии прохода в течение установленного времени, или могут иметь средства для возврата в закрытое состояние.

5.2.2.4 УПУ при необходимости могут иметь защиту от прохода через них одновременно двух или более человек.

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

5.2.2.6 Умышленное повреждение внешних электрических соединительных цепей и элементов блокировки не должно приводить к открыванию УПУ.

Должны быть предусмотрены меры по защите внешних электрических соединительных цепей от возможности подачи по ним напряжений, приводящих к нарушению работы или к открыванию УПУ.

5.2.2.7 УПУ могут иметь дополнительно средства специального контроля, встроенные или совместно функционирующие. Требования к УПУ, в состав которых входят средства специального контроля, устанавливаются в нормативных документах на устройства конкретного типа.

5.2.3 Требования к функциональным характеристикам УВИП

5.2.3.1 Считыватели УВИП должны обеспечивать:

- возможность считывания идентификационного признака с идентификаторов;
- введение биометрической информации (для считывателей биометрической информации);
- преобразование введенной информации в электрический сигнал;

- передачу информации на УУ.

5.2.3.2 УВИП должны быть защищены от манипулирования путем перебора и подбора идентификационных признаков. Виды защиты должны быть указаны в стандартах и (или) нормативных документах на УВИП конкретного типа.

5.2.3.3 Идентификаторы УВИП должны обеспечивать хранение идентификационного признака в течение срока службы и при эксплуатации.

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

5.2.3.5 Производитель идентификаторов должен гарантировать, что код данного идентификатора не повторится, или указать условия повторяемости кода и меры по предотвращению использования идентификаторов с одинаковыми кодами.

5.2.3.6 Считыватели УВИП при взломе и вскрытии, а также в случае обрыва или короткого замыкания подходящих к ним цепей не должны вызывать открывание УПУ. При этом автономные системы могут выдавать звуковой сигнал тревоги, а системы с централизованным управлением сигнал тревоги могут передавать на пункт управления и, при необходимости, выдавать звуковой сигнал.

5.2.3.7 В стандартах и нормативных документах на конкретные виды идентификаторов должен быть определен минимум кодовых комбинаций. Значение кодовых комбинаций приведено в таблице 3.

Таблица 3 — Значение кодовых комбинаций

Уровень устойчивости к НСД	Количество кодовых комбинаций
Нормальный	$10^2 — 10^5$
Повышенный	$10^5 — 10^7$
Высокий	Не менее 10^7

Пользователь автономных систем должен иметь возможность сменить или переустановить открывающий код не менее 100 раз. Смена кода должна происходить только после ввода действующего кода.

5.2.4 Требования к функциональным характеристикам УУ

5.2.4.1 Аппаратные средства УУ должны обеспечивать прием информации от УВИП, обработку информации и выработку сигналов управления на исполнительные устройства УПУ.

5.2.4.2 Аппаратные средства УУ в системах с централизованным управлением и универсальных должны обеспечивать:

- обмен информацией по линии связи между контроллерами и средствами управления;
- сохранность данных в памяти при обрыве линий связи со средствами централизованного управления, отключении питания и при переходе на резервное питание;
- контроль линий связи между контроллерами, средствами централизованного управления.

Протоколы обмена информацией должны обеспечивать необходимую помехоустойчивость, скорость обмена информацией, а также, при необходимости, защиту информации.

Виды и параметры протоколов и интерфейсов должны быть установлены в стандартах и других нормативных документах на УУ конкретного типа с учетом требований ГОСТ 26139.

5.2.4.3 Программное обеспечение УУ должно обеспечивать:

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

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

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

После указанных воздействий и перезапуске программы должна сохраняться работоспособность системы и сохранность установленных данных. Указанные воздействия не должны приводить к открыванию УПУ и изменению действующих кодов доступа.

5.2.4.5 Общие показатели качества программного обеспечения следует устанавливать по ГОСТ 28195.

5.3 Требования к электромагнитной совместимости

5.3.1 Средства и системы КУД в зависимости от устойчивости к воздействию электромагнитных помех должны иметь следующие степени жесткости по ГОСТ Р 50009:

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

Требования по устойчивости к искусственно создаваемым электромагнитным помехам предъявляют к устройствам, имеющим степень жесткости не ниже второй, и должны быть установлены в технических условиях на средства и системы КУД конкретного типа.

5.3.2 Уровень допустимых радиопомех при работе средств и систем КУД должен соответствовать ГОСТ 23511 и ГОСТ Р 50009.

5.4 Требования по устойчивости средств и систем КУД в НСД

5.4.1 Требования по устойчивости к НСД устанавливают в настоящем пункте и нормативных документах на средства и системы КУД конкретного типа.

5.4.2 Требования по устойчивости к НСД разрушающего действия распространяются на УПУ и считыватели УВИП. Требования включают:

- устойчивость к взлому;
- пулестойкость;
- устойчивость к взрыву.

5.4.3 Устойчивость к разрушающим воздействиям устанавливают для средств с повышенным и высоким уровнями устойчивости.

Нормальная устойчивость обеспечивается механической прочностью конструкции без оценки по показателям устойчивости.

Повышенную устойчивость определяют по показателям устойчивости к взлому одиночными ударами и (или) набором инструментов.

Высокую устойчивость определяют по показателям устойчивости к взлому, пулестойкости и (или) взрыву.

Требования по пулестойкости применяют только к УПУ с полным (сплошным) перекрытием проема прохода.

Показатели устойчивости по классам приведены в таблице 4.

Таблица 4 — Классы УПУ по показателям устойчивости

Показатель устойчивости	Класс УПУ				
	1	2	3	4	5
1 Защищенность от взлома одиночными ударами	+	+	+	+	+
2 Защищенность от взлома набором инструментов	—	—	—	+	+
3 Пулестойкость	—	—	±	±	±
4 Устойчивость к взрыву	—	—	—	±	±

Примечание — Условный знак «+» означает наличие требования и обязательность его проверки, знак «—» — отсутствие требования, а знак «±» — возможность исполнения УПУ как устойчивыми, так и неустойчивыми к данному виду воздействия.

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

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

Показатели устойчивости по данным требованиям и методы их испытаний должны быть указаны в стандартах и (или) технических условиях на средства КУД конкретного типа.

5.4.5 Автономные СКУД должны быть защищены от манипулирования с целью изменения или подбора кода. Вид защиты должен быть указан в технических условиях на системы конкретного типа.

5.4.6 Системы КУД повышенной и высокой устойчивости к НСД должны иметь защиту от принуждения и саботажных действий. Конкретный метод защиты и показатели защиты должны быть приведены в технических условиях на системы КУД конкретного типа.

5.4.7 Программное обеспечение УУ должно быть защищено от несанкционированного доступа. Требования по защите программного обеспечения УУ от несанкционированного доступа устанавливают по ГОСТ Р 50739.

5.4.8 Программное обеспечение УУ должно быть также защищено от:

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

Рекомендуемые уровни доступа по типу пользователей:

первый («администратор») — доступ ко всем функциям;

второй («дежурный оператор») — доступ только к функциям текущего контроля;

третий («системный оператор») — доступ к функциям конфигурации программного обеспечения без доступа к функциям, обеспечивающим управление УПУ.

Количество знаков в пароле должно быть не менее шести.

При вводе пароля в систему вводимые знаки не должны отображаться на средствах отображения информации.

После ввода в систему пароли должны быть защищены от просмотра средствами операционных систем ЭВМ.

5.4.9 Требования по защите систем КУД с централизованным управлением и универсальных от несанкционированного доступа к информации должны соответствовать для систем нормальной устойчивости к НСД требованиям 5.4.8 данного стандарта; для систем повышенной и высокой устойчивости требования устанавливают по классам в соответствии с документом [3], и они должны соответствовать приложению А.

При этом класс защиты системы от несанкционированного доступа к информации должен соответствовать:

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

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

При этом класс защиты средств КУД от несанкционированного доступа к информации должен соответствовать:

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

5.4.11 Системы и средства КУД высокой устойчивости подлежат обязательной сертификации по требованиям защиты от несанкционированного доступа к информации.

5.5 Требования надежности

5.5.1 В стандартах и (или) технических условиях на средства и системы КУД конкретного типа должны быть установлены следующие показатели надежности в соответствии с ГОСТ 27.002 и ГОСТ 27.003:

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

При установлении показателей надежности должны быть указаны критерии отказа.

Показатели надежности средств КУД устанавливают исходя из необходимости обеспечения надежности системы в целом.

По требованию заказчика в технических условиях на конкретные средства и системы КУД могут быть установлены дополнительно другие требования по надежности.

5.5.2 Средняя наработка на отказ систем КУД с одной точкой доступа (без учета УПУ) — не менее 10000 ч.

5.5.3 Средний срок службы систем КУД — не менее 8 лет с учетом проведения восстановительных работ.

5.6 Требования по устойчивости к внешним воздействующим факторам

5.6.1 Требования по устойчивости в части воздействия климатических факторов устанавливают в стандартах и нормативных документах на средства и системы КУД конкретного типа в соответствии с климатическим исполнением и категорией изделий по ГОСТ 15150.

5.6.2 Оболочки средств КУД при необходимости защиты от внешних воздействий должны иметь степени защиты по ГОСТ 14254.

5.6.3 Требования по устойчивости в части воздействия механических факторов должны быть установлены в стандартах и (или) нормативных документах на средства и системы КУД конкретного типа в соответствии с требуемой группой условий эксплуатации по ГОСТ 17516 и степенью жесткости изделий по ГОСТ 16962.

5.7 Требования к электропитанию

5.7.1 Основное электропитание средств и систем КУД должно осуществляться от сети переменного тока с номинальным напряжением 220 В, частотой 50 Гц.

Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения сети от минус 15 % до плюс 10 % номинального значения и частоты (50 ± 1) Гц.

Электропитание отдельных средств контроля и управления доступом допускается осуществлять от источников с иными параметрами выходных напряжений, требования к которым устанавливают в нормативных документах на средства КУД конкретного типа.

5.7.2 Средства и системы КУД должны иметь резервное электропитание при пропадании напряжения основного источника питания. В качестве резервного источника питания допускается использовать резервную сеть переменного тока или источник питания постоянного тока.

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

Переход на резервное питание должен происходить автоматически без нарушения установленных режимов работы и функционального состояния средств и систем КУД.

Средства и системы КУД должны быть работоспособны при допустимых отклонениях напряжения резервного источника от минус 15 % до плюс 10 % номинального значения.

5.7.3 Резервный источник питания должен обеспечивать выполнение основных функций системы КУД при пропадании напряжений в сети на время не менее 0,5 ч для систем первого и второго класса по функциональным характеристикам и не менее 1 ч для систем третьего класса.

Допускается не применять резервирование электропитания с помощью аккумуляторных батарей для УПУ, которые требуют для управления значительных мощностей приводных механизмов (приводы ворот, шлюзы и т.п.). При этом такие УПУ должны быть оборудованы аварийными механическими средствами открывания.

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

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

5.7.6 Химические источники питания, встроенные в идентификаторы или обеспечивающие сохранность данных в контроллерах, должны обеспечивать работоспособность средств КУД не менее 3 лет.

5.8 Требования безопасности

5.8.1 Средства и системы КУД должны соответствовать требованиям безопасности ГОСТ 12.2.007.0, ГОСТ 12.2.006 и ГОСТ 27570.0.

5.8.2 Материалы, комплектующие изделия, используемые для изготовления средств и систем КУД, должны иметь токсико-гигиенический паспорт, гигиенический паспорт и гигиенический сертификат.

5.8.3 Монтаж и эксплуатация средств и систем КУД должны соответствовать требованиям безопасности ГОСТ 12.2.003.

5.8.4 Средства и системы КУД должны соответствовать требованиям пожарной безопасности ГОСТ 12.1.004.

5.8.5 Электрическое сопротивление изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должно быть не менее значений, указанных в таблице 5.

Таблица 5 — Требуемые значения сопротивления 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

5.8.6 Электрическая прочность изоляции средств и систем КУД между цепями сетевого питания и корпусом, а также между цепями сетевого питания и входными/выходными цепями должна соответствовать требованиям ГОСТ 12997.

5.8.7 Сопротивление изоляции и электрическая прочность средств и систем КУД, предназначенных для бытового и аналогичного общего применения, должны соответствовать требованиям ГОСТ 12.2.006 и ГОСТ 27570.0.

5.8.8 Для средств КУД, работающих при напряжениях не выше 12 В переменного тока и 36 В постоянного тока, допускается не приводить значение электрической прочности изоляции и ее сопротивления в нормативных документах на конкретные средства.

5.8.9 Конкретные значения сопротивления изоляции и электрическая прочность изоляции должны быть указаны в технических условиях на средства и системы КУД конкретного типа.

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

5.8.11 Средства и системы КУД, предназначенные для эксплуатации в зонах с взрывоопасной средой, должны соответствовать требованиям ГОСТ 12.1.010, других стандартов и нормативных документов, регламентирующих требования к изделиям, предназначенным для работы во взрывоопасных средах.

5.9 Требования к конструкции

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

5.9.2 Конструкции средств КУД должны быть построены по модульному и блочно-агрегатному принципу и обеспечивать:

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

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

- механическую прочность;

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

5.10 Требования к маркировке

5.10.1 Маркировка средств и систем КУД должна быть выполнена по ГОСТ Р 50775 и содержать:
- товарный знак и (или) другие реквизиты предприятия-изготовителя;
- условное обозначение средств и систем КУД;
- серийный номер;
- дату изготовления;
- знак сертификата соответствия (при его наличии).

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

6 Методы испытаний

6.1 Общие положения

6.1.1 Испытания средств и систем КУД проводят по настоящему стандарту, а также по методикам действующих нормативных документов на отдельные виды испытаний и по техническим условиям на средства и системы КУД конкретного типа.

Объем и последовательность испытаний устанавливают в программе испытаний на средства и системы КУД конкретного типа.

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

Оборудование для контроля электрических параметров, радиотехнических измерений должно соответствовать требованиям ГОСТ 24686.

6.1.3 При проведении испытаний должны соблюдаться требования техники безопасности, а также требования ГОСТ 12.2.006, ГОСТ 27570.0 и используемых нормативных документов.

Безопасность проведения работ, использования приборов, инструментов и оборудования должна соответствовать требованиям ГОСТ 12.1.006, ГОСТ 12.1.019, правил [4], [5], [6].

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

6.1.4 Образцы, предназначенные для проведения испытаний, должны иметь техническую документацию в объеме, необходимом для проведения испытаний, и быть полностью укомплектованы в соответствии с технической документацией.

6.1.5 Все испытания, кроме климатических, проводят в нормальных климатических условиях по ГОСТ 15150.

6.1.6 Условия испытаний средств КУД по ГОСТ 12997, для УУ и систем КУД дополнительно необходимо учитывать требования ГОСТ 21552.

6.2 Испытания средств и систем КУД на соответствие общим техническим требованиям

6.2.1 Испытания средств и систем КУД на соответствие функциональным характеристикам (5.2) проводят по методикам, приведенным в стандартах и технических условиях на средства и системы КУД конкретного типа.

6.2.2 Испытания средств и систем КУД на устойчивость к электромагнитным помехам (5.3.1) проводят по ГОСТ Р 50009, ГОСТ Р 51317.4.4, ГОСТ Р 51317.4.2, ГОСТ Р 51317.4.5, ГОСТ Р 51317.4.3, ГОСТ Р 50627.

6.2.3 Испытания средств и систем КУД на соответствие электромагнитной совместимости и нормам радиопомех (5.3.2) проводят по ГОСТ Р 50009 и ГОСТ Р 51318.14.1.

6.2.4 Испытания УПУ и считывателей УВИП на устойчивость к НСД разрушающего воздействия (5.4.2 и 5.4.3) проводят по ГОСТ 30109, ГОСТ Р 50862, ГОСТ Р 50941, ГОСТ Р 51072, ГОСТ Р 51112.

6.2.5 Испытания средств и систем КУД на устойчивость к НСД неразрушающего воздействия (5.4.4—5.4.6) проводят по стандартам и (или) другим нормативным документам на средства и системы КУД конкретного типа.

6.2.6 Испытания УУ по защите программного обеспечения от несанкционированного доступа (5.4.7 и 5.4.8) проводят по ГОСТ Р 50739.

6.2.7 Испытания средств и систем КУД на устойчивость от несанкционированного доступа к информации (5.4.9, 5.4.10) проводят по действующим методикам испытаний организациями, имеющими лицензию на право проведения работ в области защиты информации.

6.2.8 Испытания средств и систем КУД на соответствие требованиям надежности (5.5) проводят по методикам, разработанным с учетом требований ГОСТ 27.003, ГОСТ 23773.

6.2.9 Испытания средств и систем КУД на устойчивость к внешним воздействующим факторам (5.6) проводят по ГОСТ 12997 и(или) ГОСТ 21552, ГОСТ 23773 с применением соответствующих методов испытаний по ГОСТ 20.57.406, ГОСТ 16962, ГОСТ 16962.1, ГОСТ 16962.2, ГОСТ 17516, ГОСТ 17516.1.

6.2.10 Испытания средств и систем КУД на соответствие требованиям к электропитанию (5.7) проводят по ГОСТ 12.2.006, ГОСТ 12997, ГОСТ 21552 и ГОСТ 27570.0.

6.2.11 Испытания средств и систем КУД на соответствие требованиям безопасности (5.8) проводят по ГОСТ 12.1.004, ГОСТ 12.2.006, ГОСТ 12997, ГОСТ 27570.0 и техническим условиям на средства и системы КУД конкретного типа.

6.2.12 Проверку конструкции (5.9) и маркировки (5.10) проводят по ГОСТ 23773, а также по стандартам и (или) техническим условиям на средства и системы КУД конкретного типа.

ПРИЛОЖЕНИЕ А
(обязательное)

Автоматизированные системы

Классификация автоматизированных систем и требований по защите информации

Классификация автоматизированных систем — по документу [3].

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)	—	—	—	+	+

Окончание таблицы А.1

Подсистемы и требования	Группы и классы				
	3		2	1	
	3Б	3А	2Б	1Г	1В
- 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 требования к данному классу, знак «—» — отсутствие требования к данному классу.

Пояснения к требованиям

Термины и определения — по документу [7].

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

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

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

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.

защита от несанкционированного доступа. Защита от НСД: Предотвращение или существенное затруднение несанкционированного доступа.

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

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

уровень полномочий субъекта доступа: Совокупность прав доступа субъектов доступа.

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

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

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

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

целостность информации: Способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

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

класс защищенности средств ВТ и АС: Определенная совокупность требований по защите средств ВТ и АС от несанкционированного доступа к информации.

сертификация уровня защиты: Процесс установления соответствия средств ВТ или АС набору определенных требований по защите.

А.1 Подсистема управления доступом

А.1.1 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 количестве символов 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.1.2 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.2 Подсистема регистрации и учета

А.2.1 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.2.2 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 с регистрацией защищаемых носителей в картотеке с дублированием учета.

А.2.3 Подсистема должна осуществлять очистку двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации.

При регистрации и учете указываются время и дата, характеристики и результаты проведенной операции.

А.2.4 Подсистема должна осуществлять сигнализацию попыток нарушения защиты.

А.3 Подсистема обеспечения целостности

А.3.1 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.3.2 Физическая охрана средств вычислительной техники должна предусматривать постоянное наличие охраны с помощью технических средств и специального персонала с использованием определенного пропускного режима.

А.3.3 Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС.

А.3.4 Тестирование всех функций СЗИ НСД с помощью специальных программных средств должно проводиться не реже одного раза в год.

А.3.5 Средства восстановления СЗИ НСД должны предусматривать ведение двух копий программных средств СЗИ НСД, их периодическое обновление и контроль работоспособности.

ПРИЛОЖЕНИЕ Б
(обязательное)

Средства вычислительной техники

Показатели защищенности от НСД к информации по классам защищенности

Показатели защищенности от НСД к информации — по документу [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 аутентификация	—	=	+
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.

Пояснения к требованиям по показателям защищенности

Б.1 Дискреционный принцип контроля доступа

Б.1.1 По всем классам защищенности

Комплекс средств защиты (КСЗ) должен контролировать доступ именованных субъектов (пользователей) к именованным 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 каждому субъекту (индивиду или группе равноправных индивидов).

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

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

Б.1.2 Дополнительно по классу защищенности 5 должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Б.1.3 Дополнительно по классу защищенности 4 КСЗ 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» 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.2 Мандатный принцип контроля доступа

Для реализации этого 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 ему 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 доступе 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 санкционировании запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными и мандатными ПРД. Таким образом должен контролироваться не только единичный акт доступа, но и потоки информации.

Б.3 Очистка памяти

Б.3.1 По классу защиты 5

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

Б.3.2 По классу защиты 4

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

Б.4 Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен быть 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.5 Маркировка документов

При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1 и заполняют его реквизиты в соответствии с ведомственным документом Гостехкомиссии России.

Б.6 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 осуществляться только под контролем КСЗ.

Б.7 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.8 Идентификация и аутентификация

Б.8.1 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.8.2 Дополнительно по классу защищенности 4

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

Б.9 Гарантии проектирования

Б.9.1 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.9.2 Дополнительно по классу защищенности 4

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

Б.10 Регистрация

Б.10.1 По классу защищенности 5

КСЗ должен 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 запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

Б.10.2 Дополнительно по классу 4 регистрация должна также регистрировать все попытки доступа, все действия оператора и выделенных пользователей (администраторов защиты и т. п.).

Б.11 Целостность КСЗ

Б.11.1 По классу защищенности 5

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

Б.11.2 По классу защищенности 4

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

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

Б.12 Тестирование

Б.12.1 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.12.2 Дополнительно по классу защищенности 5 должны тестироваться:

- очистка памяти в соответствии с Б.3.1;
- регистрация событий в соответствии с Б.10.1, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- работа механизма, осуществляющего контроль за целостностью КСЗ.

Б.12.3 По классу защищенности 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 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;
- 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.10.2, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

Б.13 Руководство пользователя

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

Б.14 Руководство по КСЗ

Документ адресован администрации защиты.

Б.14.1 По классу защищенности 6 руководство по КСЗ должно содержать:
- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ и процедур проверки правильности старта.

Б.14.2 Дополнительно по классам защищенности 5 и 4 руководство по КСЗ должно содержать описание процедур работы со средствами регистрации.

Б.15 Тестовая документация

Тестовая документация должна представлять описание применяемых тестов (Б.12), испытаний и результатов тестирования.

Б.16 Конструкторская (проектная) документация

Б.16.1 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.16.2 По классу защищенности 5 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.16.3 По классу защищенности 4 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 сопоставление пользователя с устройством;
- описание механизма идентификации и аутентификации;
- описание средств регистрации.

ПРИЛОЖЕНИЕ В
(справочное)

Библиография

[1] Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Гостехкомиссия России. М.: 1992
[2] Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссия России. М.: 1997
[3] Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требований по защите информации. Гостехкомиссия России. М.: 1992
[4] ПУЭ-76 «Правила устройства электроустановок», утверждены Главным техническим управлением по эксплуатации энергосистем и Государственной инспекцией по энергонадзору Министерства энергетики и электрификации СССР
[5] Правила техники безопасности при эксплуатации электроустановок потребителей
[6] Правила безопасности при взрывных работах
[7] Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России. М.: 1992

ОКС 13.320 П77 ОКП 43 7200

Ключевые слова: средства, системы, доступ, идентификация, идентификатор, несанкционированные действия, несанкционированный доступ к информации