

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 идентификационные. 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 аналоговая 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 предотвращение 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 (электромагнитические, 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 запираания:

- 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](https://www.gost.ru/standards/gost_r/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	КД
- прибор приемно-контрольный доступа	ППКД
Средства управления - программные:	
программное обеспечение	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

УИ - по способу запираания	С полным перекрытием (полноростовые турникеты, специализированные ворота)	2
	Со сплошным перекрытием проема (сплошные двери, ворота)	3
	С блокированием объекта в проеме (шлюзы, кабины проходные)	4
	Электромеханические замки	1
	Электромагнитные замки	2
	Электромагнитные защелки	3
	Механизмы привода ворот	4
	С ручным вводом	1
ИД - по способу считывания идентификационных признаков	Контактные	2
	Бесконтактные	3
	Биометрические	4
	Комбинированные	5
	Механические	1
КД, ППКД - по способу управления	Магнитные	2
	Оптические	3
	Электронные контактные	4
	Электронные радиочастотные	5
	Акустические	6
	Комбинированные	7
	Автономный	1
	Централизованный	2
	Универсальный	3