ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55250— 2012

Воздушный транспорт

АЭРОПОРТЫ. ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ ДОСТУПА И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ

Общие технические требования

Издание официальное

Москва
Стандартинформ
2013

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием Государственный научно-исследовательский институт гражданской авиации (ФГУП ГосНИИ ГА)

2 ВНЕСЕН Техническим комитетом ТК 034 «Воздушный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2012 г. № 1342-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2013

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Общие технические требования к системам контроля доступа и инженерно-техническим средствам охраны 4
5 Требования назначения 4
6 Требования по обеспечению охраны воздушных судов и объектов аэропорта 9
7 Требования к системе охранно-тревожной сигнализации 10
8 Требования к системе охранного телевидения 11
Библиография 12

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Воздушный транспорт

АЭРОПОРТЫ. ТЕХНИЧЕСКИЕ СРЕДСТВА КОНТРОЛЯ ДОСТУПА И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ

Общие технические требования

Air transport. Technical means of access control and engineering and technical means of protection. General technical requirements

Дата введения — 2013—07—01

1 Область применения

Настоящий стандарт распространяется на инженерно-технические средства охраны и технические средства контроля и управления доступом, предназначенные для исключения несанкционированного доступа людей и транспорта в (из) контролируемую зону аэропорта и объекты его инфраструктуры, а также контроля и санкционирования доступа.

Стандарт устанавливает общие технические требования к инженерно-техническим средствам охраны и техническим средствам контроля и управления доступом. Настоящий стандарт распространяется на вновь разрабатываемые и модернизируемые средства и системы контроля и управления доступом.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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 Системы тревожной сигнализации

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

ГОСТ 12.2.006—87 Безопасность аппаратуры электронной сетевой и сходных с ней устройств, предназначенных для бытового и аналогичного общего применения. Общие требования и методы испытаний

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

ГОСТ 27.002—2009 Надежность в технике. Термины и определения

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

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

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

ГОСТ 27570.0—87 Безопасность бытовых и аналогичных электрических приборов. Общие требования и методы испытаний

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, определения и сокращения

3.1 В настоящем стандарте применены следующие термины с соответствующими определениями:

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

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

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

3.1.4 **временной интервал доступа («окно времени»):** Интервал времени, в течение которого разрешается перемещение в данной точке доступа.

3.1.5 **вскрытие:** Действия, направленные на несанкционированное проникновение через устройство преграждающее управляемое без его разрушения.

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

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

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

3.1.9 **зона общего доступа:** Участки территории и внутренние помещения объекта, доступ в которые разрешен любым физическим лицам без предъявления каких-либо разрешительных документов.

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

Примечание — Термин-синоним — носитель идентификационного признака.

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

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

3.1.13 **контрольно-пропускной пункт:** Специально оборудованное место на объекте для осуществления контроля в установленном порядке за проходом людей и проездом транспортных средств в зону ограниченного доступа.

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

3.1.15 **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 с программным обеспечением.

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

3.1.17 **несанкционированные действия:** Действия, целью которых является несанкционированное проникновение через устройства преграждающие управляемые.

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

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

3.1.20 **принуждение:** Насильственные действия над лицом, имеющим право доступа, в целях несанкционированного проникновения через устройства преграждающие управляемые. Устройства контроля и управления доступом при этом могут функционировать нормально.

3.1.21 **пропускная способность:** Способность средства или системы контроля управления доступом пропускать определенное количество людей, транспортных средств и т. п. в единицу времени.

3.1.22 **пропускной режим:** Порядок допуска физических лиц и транспортных средств в зону ограниченного доступа в целях обеспечения антитеррористической защищенности объекта.

3.1.23 **пулестойкость:** Способность преграды противостоять сквозному пробиванию пулями и обеспечивать при этом безопасность человека (людей) от вторичных поражающих элементов.

3.1.24 **саботаж:** Преднамеренно созданное состояние системы, при котором происходит повреждение части системы.

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

3.1.26 **система контроля и управления доступом; система КУД:** Совокупность средств контроля и управления, обладающих технической, информационной, программной и эксплуатационной совместимостью.

3.1.27 **средства контроля и управления доступом; средства КУД:** Механические, электромеханические, электрические, электронные устройства, конструкции и программное обеспечение, обеспечивающие реализацию контроля и управления доступом.

3.1.28 **считыватель:** Устройство в составе устройства ввода идентификационных признаков, предназначенное для считывания (ввода) идентификационных признаков.

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

3.1.30 **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.

3.1.31 **устойчивость к взлому:** Способность конструкции противостоять разрушающему воздействию без использования инструмента, а также с помощью ручного и других типов инструмента.

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

3.1.33 **устройства ввода идентификационных признаков:** Электронные устройства, предназначенные для ввода запоминаемого кода, ввода биометрической информации, считывания кодовой информации с идентификаторов.

Примечание — В состав УВИП входят считыватели и идентификаторы.

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

3.1.35 **устройства преграждающие управляемые:** 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 другие конструкции).

3.1.36 **устройства управления:** Устройства и программное обеспечение, устанавливающие режим доступа и обеспечивающие прием и обработку информации с УВИП, управление УПУ, отображение и регистрацию информации.

3.2 В настоящем стандарте применены следующие сокращения:
КУД — контроль и управление доступом;
КПП — контрольно-пропускной пункт;
НСД — несанкционированные действия;
САБ — служба авиационной безопасности;
система КУД — система контроля и управления доступом;
средства КУД — средства контроля и управления доступом;
УВИП — устройства ввода идентификационных признаков;
УПУ — устройства преграждающие управляемые;
УУ — устройства управления.

4 Общие технические требования к системам контроля доступа и инженерно-техническим средствам охраны

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

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

4.3 Средства КУД, предназначенные для построения систем, должны обладать конструктивной, информационной, надежной 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 Требования назначения

5.1 Требования к функциональным характеристикам систем КУД

5.1.1 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 пожарной безопасности;
- автоматическое формирование сигнала сброса на УПУ при отсутствии факта прохода;
- выдачу сигнала тревоги при использовании системы аварийного открывания УПУ для несанкционированного проникновения.

5.1.2 Системы КУД с централизованным управлением и универсальные должны 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, установкам режимов и к информации;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением их 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.

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

5.1.4 Значения характеристик и требования, приведенные в 5.1.1—5.1.3, должны быть установлены в стандартах и (или) технических условиях на системы КУД конкретного типа.

Системы КУД должны 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;

- число и вид временных интервалов доступа («окон времени»), уровней доступа;

- число 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 (требование обязательно для СКУД с биометрической идентификацией, для остальных допускается не указывать);

- показатели по уровням устойчивости к НСД.

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

5.2 Требования к функциональным характеристикам УПУ

5.2.1 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 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 и (или) технических условиях на УПУ конкретного типа должны быть установлены показатели пропускной способности.

5.2.3 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) технических условиях 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.

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

5.2.5 Для УПУ должна быть предусмотрена возможность механического аварийного открывания в случае отключения электропитания, при пожаре или других стихийных бедствиях. Аварийная система открывания должна быть защищена от возможности использования ее для несанкционированного проникновения.

5.2.6 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.

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

5.3 Требования к функциональным характеристикам УВИП

5.3.1 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.

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

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

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

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

5.3.6 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.

5.3.7 В стандартах и технических условиях на конкретные виды идентификаторов должен быть определен минимум кодовых комбинаций. Пользователь автономных систем должен иметь возможность сменить или переустановить открывающий код не менее 100 раз. Смена кода должна происходить только после ввода действующего кода.

5.4 Требования к функциональным характеристикам УУ

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

5.4.2 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 технических условиях на УУ конкретного типа с учетом требований ГОСТ 26139.

5.4.3 Программное обеспечение УУ должно обеспечивать:

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

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

- отключение электропитания аппаратных средств;
- программный сброс аппаратных средств;

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

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

5.5 Требования к электромагнитной совместимости

5.5.1 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.

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

5.6 Требования по устойчивости средств и систем КУД в НСД

5.6.1 Требования по устойчивости к НСД устанавливают в настоящем подразделе и технических условиях на средства и системы КУД конкретного типа.

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

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

5.6.3 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.

5.6.4 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.

5.6.5 Автономные системы КУД должны быть защищены от манипулирования в целях изменения или подбора кода. Вид защиты должен быть указан в технических условиях на системы конкретного типа.

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

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

5.7 Требования надежности

5.7.1 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.

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

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

5.8 Требования по устойчивости к внешним воздействующим факторам

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

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

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

5.9 Требования к электропитанию

5.9.1 Основное электропитание средств и систем КУД должно осуществляться от сети переменного тока номинальным напряжением 220 В ± 10 %, частотой (50 ± 1) Гц.

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

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

5.9.2 Средства и системы КУД должны иметь резервное электропитание при падении 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.

5.9.3 Резервный источник питания должен обеспечивать выполнение основных функций системы КУД при падении напряжения 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.

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

5.9.5 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.

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

5.10 Требования безопасности

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

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

6 Требования по обеспечению охраны воздушных судов и объектов аэропорта

6.1 Под постоянной охраной в контролируемой зоне аэропорта должны находиться: воздушные суда; территории отдельно стоящих объектов и транспортные средства с горючим и смазочными материалами, специальными жидкостями и газами; почтово-грузовые терминалы; цеха бортового питания; коммерческие склады; склады хранения опасных грузов; КПП.

6.2 Территория аэропорта и расположенных за пределами аэропорта объектов управления воздушным движением и навигации должны патрулироваться нарядами службы авиационной безопасности (САБ).

6.3 Места стоянок воздушных судов, территории отдельно стоящих объектов с горючим и смазочными материалами, специальными жидкостями и газами, почтово-грузовые терминалы, цеха бортового питания, коммерческие склады, склады хранения опасных грузов и КПП оборудуются охранным освещением.

6.4 Территория аэропорта и особо важных объектов гражданской авиации должна иметь железобетонное, кирпичное, металлическое сплошное, металлическое сетчатое (сварная сетка), металлическое решетчатое, многорядное колюче-проволочное, спиральное колюче-ленточное ограждение высотой 2,13—2,44 м [1] по всему периметру с предупредительными аншлагами, запрещающими проникновение в контролируемую зону. Расстояние между предупредительными аншлагами не более 100 м.

Поверх периметрового ограждения устанавливаются металлические конструкции различного профиля (козырьки из угловых консолей с несколькими рядами колючей проволоки, армированной колючей ленты и др.).

С внутренней и внешней сторон периметрового ограждения полоса шириной 3 м должна быть очищена от мусора, кустарника и деревьев. На ней не допускается строительство объектов, складирование оборудования и материалов, стоянка транспортных средств и т. п. На участках, где невозможно соблюдение требований по очистке периметра с внешней стороны, обязательно применение охранной сигнализации.

6.5 На участках ограждения вдоль периметра объектов аэропорта дополнительно могут быть установлены:

а) постовые вышки или смотровые площадки для наблюдения за состоянием ограждения и прилегающей местностью;

б) контрольно-следовая полоса для определения места проникновения нарушителя пропускного режима;

в) блок-посты служебных собак;

г) системы охранной сигнализации, иные технические средства охраны, сертифицированные для применения в гражданской авиации;

д) электронные устройства обнаружения и подачи сигнала тревоги при преодолении или попытке преодоления ограждения нарушителем.

6.6 С внутренней стороны вдоль ограждения аэропорта прокладывается дорога с искусственным покрытием.

6.7 Подразделения охраны САБ аэропортов и (или) подразделения, осуществляющие охрану аэропортов и объектов их инфраструктуры, размещаются в караульном помещении (караульных помещениях). Хранение оружия и боеприпасов обеспечивается в соответствии с требованиями, установленными нормативными правовыми актами Российской Федерации, в специально оборудованной комнате.

6.8 На привокзальных площадях создаются зоны безопасности шириной не менее 50 м от зданий аэровокзальных комплексов и других объектов аэропортов.

Кратковременная остановка автотранспортных средств в зонах безопасности допускается только для посадки (высадки) пассажиров. Стоянка автотранспортных средств в зонах безопасности разрешается не более 3 ч при наличии электронной системы фиксации государственных регистрационных номеров автотранспорта и не ближе 10 м от зданий аэровокзальных комплексов и других объектов аэропортов.

6.9 Все объекты, на которых установлен пропускной режим или планируется его применение, должны оснащаться КПП для пропуска людей и разрешенных видов транспорта.

Количество КПП должно быть минимальным и обеспечивать необходимую пропускную способность людей и транспорта. В зависимости от пропускного режима предусматриваются в обязательном порядке при строительстве КПП помещения для хранения пропусков или автоматических карточек.

КПП для транспортных средств оборудуют типовыми раздвижными или распашными воротами с электроприводом и дистанционным управлением, устройствами для их аварийной остановки и открывания вручную. Ворота оборудуют ограничителями или стопорами для предотвращения произвольного открывания (движения). Оборудуют смотровые площадки или эстакады для осмотра автотранспорта, шлагбаумы, а КПП для железнодорожного транспорта — вышкой и площадкой для осмотра подвижного железнодорожного состава.

6.10 Пульт управления воротами следует располагать в КПП или на его наружной стене [2]. В последнем случае необходимо исключить доступ к пульту посторонних лиц.

7 Требования к системе охранно-тревожной сигнализации

7.1 Система охранно-тревожной сигнализации включает в себя:

- подсистему охранной сигнализации;
- подсистему тревожной сигнализации.

7.1.1 Подсистема охранной сигнализации должна обеспечивать:

- оповещение о несанкционированном доступе на территорию объекта, в выделенные помещения и т. д., оповещение о проникновении в охраняемые зоны;
- централизованную или децентрализованную постановку помещений под охрану;
- сопряжение на аппаратном уровне с системой КУД и системой охранного телевидения.

Оконечными устройствами подсистемы охранной сигнализации должны быть оборудованы:

- все кабинеты руководителей;
- служебные помещения с размещением вычислительной и оргтехники;
- помещения серверных, АТС, кроссовых и других помещений средств связи и коммуникации;
- помещения с размещением инженерных систем и систем жизнеобеспечения объекта;
- все внешние двери и ворота здания объекта;
- двери технических этажей;
- колодцы, люки, лазы, шахты коммуникаций сечением 250 × 250 мм и более;
- отдельные объекты внутри помещений (сейфы, шкафы, ниши) по необходимости.

Постановку и снятие с охраны необходимо предусмотреть как централизованно, так и децентрализованно (с кодонаборных устройств, размещаемых непосредственно в охраняемых помещениях).

7.1.2 Подсистема тревожной сигнализации предназначена для автоматической или ручной передачи сигналов тревоги на пульт охраны и в дежурную часть федеральных органов исполнительной власти при возникновении на объекте чрезвычайной ситуации.

Оконечными устройствами подсистемы тревожной сигнализации должны быть оборудованы:

- рабочие помещения и комнаты отдыха руководителей структурных подразделений объекта и их заместителей;
- постоянные и временные посты охраны;
- все КПП;
- все двери и ворота внешнего периметра здания объекта (оборудуются с внутренней стороны);
- помещения камер хранения;
- помещения, предназначенные для работы с ценностями;
- помещения дежурных служб объекта.

7.2 Система охранно-тревожной сигнализации должна:

- обнаруживать действия нарушителя и выдавать извещение о несанкционированном доступе;

- обеспечивать невозможность несанкционированного отключения устройств тревожной сигнализации;
- обеспечивать скрытность установки и удобство пользования вызывным устройством;
- обеспечивать экстренный вызов группы быстрого реагирования;
- выдавать извещение о неисправности при отказе технических средств охранной сигнализации;
- сохранять исправное состояние при воздействии влияющих факторов окружающей среды;
- восстанавливать работоспособное состояние после воздействия опасных факторов окружающей среды;
- быть устойчивой к любым, установленным в стандартах на системы конкретного вида повреждениям какой-либо своей части и не вызывать других повреждений в системе или не приводить к косвенной опасности вне ее;
- сохранять работоспособное состояние при отключении сетевого источника электропитания или другого основного источника электропитания в течение времени прерывания электропитания;
- обеспечивать ведение архива всех сообщений;
- обеспечивать исключение бесконтрольной постановки и снятия с охраны.

7.3 Системы охранно-тревожной сигнализации не должны выдавать ложных тревог при переключениях источников электропитания.

7.4 Средства охранно-тревожной сигнализации должны соответствовать требованиям безопасности ГОСТ 12.2.007.0, ГОСТ 12.2.006 и ГОСТ 27570.0.

7.5 Средства охранно-тревожной сигнализации должны соответствовать требованиям пожарной безопасности ГОСТ 12.1.004.

8 Требования к системе охранного телевидения

8.1 Система охранного телевидения (далее — система) предназначена для осуществления непрерывного наблюдения за обстановкой в контролируемых зонах внутри объекта, прилегающей территории, на подъездных путях.

8.2 Система должна выполнять как охранные функции, так и функции обеспечения необходимой видеоинформацией соответствующих служб для оценки тревожной ситуации, возникшей в зонах наблюдения, и принятия управляющих решений, обеспечивающих пресечение противоправных действий.

8.3 Система должна обеспечивать:

- осуществление непрерывного, круглосуточного контроля границ зон доступа и территории объекта с фиксированием лиц и транспортных средств, пересекающих зоны;
- постоянное наблюдение за критически важными элементами, служебными и техническими помещениями, а также за прилегающей территорией объекта и подъездными путями в целях раннего обнаружения противоправных действий и координации сил обеспечения безопасности;
- видеоаналитический анализ полученной информации и активный видеоконтроль (реагирование системы на нестандартное поведение людей в автоматическом режиме);
- выделение из общей видеокартины и фиксирование лиц нарушителей в целях предоставления свидетельств для последующих следственных мероприятий и судебных разбирательств;
- использование сертифицированной электронной цифровой подписи, удостоверяющей подлинность данных видеоархива;
- повторный просмотр оператором не менее 100 событий, в т. ч. и при ограничении полномочий доступа к архиву;
- архивирование информации от телевизионных камер с разграничением полномочий доступа к ней.

8.4 Система должна сопрягаться с системой пожарной безопасности, системой контроля и управления доступом и системой охранно-тревожной сигнализации.

8.5 Система должна включать в себя:

- подсистему охранного телевидения;
- подсистему видеонаблюдения.

8.5.1 Подсистема охранного телевидения предназначена для получения телевизионного изображения, служебной информации и извещений о тревоге с охраняемых помещений и зон объекта.

Выдаваемые на экраны мониторов видеоизображения, в зависимости от режима работы, должны сопровождаться следующей информацией:

- в режиме наблюдения: текущее время, текущая дата, номер и индекс видеокамеры, режим записи;

- в режиме охраны: время и дата поступления сигнала от системы охранно-тревожной сигнализации, условные сообщения и др.

8.5.2 Подсистема видеонаблюдения предназначена для получения видеоинформации об обстановке в местах массового скопления людей на прилегающей территории, помещениях объекта.

Получаемая системой видеоинформация анализируется операторами. В случае обнаружения признаков реализации угроз видеоинформация предоставляется руководителю службы безопасности объекта и (или) передается иным центрам управления в соответствии с разработанными регламентами передачи информации.

В жилой зоне доступа объекта двери подъездов должны находиться под наблюдением видеокамер локальной системы безопасности, подключенной к локальным центрам мониторинга Системы обеспечения безопасности субъекта Российской Федерации (административно-территориальной единицы).

8.6 Средства охранного телевидения должны соответствовать требованиям безопасности ГОСТ 12.2.007.0, ГОСТ 12.2.006 и ГОСТ 27570.0.

Библиография

[1] Федеральные авиационные правила «Требования авиационной безопасности к аэропортам». Введены приказом Минтранса РФ от 28.10.2005 г. № 142, зарегистрированным Минюстом РФ 28.12.2005 г. № 7321

[2] РД 78.36.003—2002 Инженерно-техническая укрепленность. Технические средства охраны

УДК 656.71:351.814.2:006.354 ОКС 03.220.50

Ключевые слова: технические средства контроля и управления доступом, технические средства охраны, объекты аэропорта, воздушные суда, авиационная безопасность, несанкционированные действия

Редактор *П.М. Смирнов*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 06.09.2013. Подписано в печать 23.09.2013. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,35. Тираж 68 экз. Зак. 1061.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru gost.e-ecolog.ru gost.e-ecolog.ru