**ФЕДЕРАЛЬНОЕ АГЕНТСТВО**

**ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ**

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ГОСТ Р**
***Проект версия 1***

# АНТИТЕРРОРИСТИЧЕСКАЯ ЗАЩИЩЕННОСТЬ

## Общие требования к техническим средствам и системам антитеррористической защиты.

Anti-terrorism security of buildings and structures. Events and decisions to ensure the anti-terrorism security of buildings and structures. General requirements

**Настоящий проект станадрта не подлежит применению до его утверждения**

**Москва**
**Стандартинформ**
**2019**

## Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «СОДИС ЛАБ» (ООО «СОДИС ЛАБ») при участии Главного управления вневедомственной охраны и ФКУ «НИЦ «ОХРАНА» Федеральной службы войск национальной гвардии Российской Федерации.

2 ВНЕСЕН Техническим комитетом 340 ”Антитеррористическая деятельность”.

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от

4 ВВЕДЕН ВПЕРВЫЕ.

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

## Введение

Настоящий стандарт является нормативно-техническим документов в области стандартизации, направленным на реализацию установленных законодательством Российской Федерации нормативных правовых требований к антитеррористической защищенности объектов капитального строительства на всех этапах их жизнедеятельности (строительства, реконструкции, капитального ремонта и эксплуатации, в том числе в целях модернизации систем безопасности).

В настоящем стандарте реализованы нормы федерального законодательства в области противодействия терроризму.

Настоящий стандарт является первым, входящим в пакет нормативной документации с общим наименованием «Антитеррористическая защищенность зданий и сооружений».

Изложенные в настоящем стандарте подходы к обеспечению антитеррористической защищенности зданий и сооружений могут быть использованы при разработке проектной документации, методических рекомендаций ведомств и организаций, технических заданий на разработку проектной документации, мониторинга состояния антитеррористической защищенности объектов и других мероприятий в сфере противодействия терроризму.

## Содержание

1 Область применения . . . . . 1
2 Нормативные ссылки . . . . . 1
3 Общие требования к средствам и сооружениям инженерно-технической укрепленности . . . . . 2
4 Общие требования к техническим средствам охраны . . . . . 5
4.1 Общие требования к системе контроля и управления доступом . . . . . 5
4.2 Требования к системе охранной и тревожной сигнализации . . . . . 6
4.3 Требования к системам телевизионного наблюдения . . . . . 7
4.4 Требования к системе охранного освещения . . . . . 10
4.5 Требования к системе экстренной связи . . . . . 10
5 Требования к системе выявления диверсионно-террористических средств . . . . . 11
5.1 Требования к системе контроля воздушно-газовой среды в системах вентиляции и кондиционирования . . . . . 13
Библиография . . . . . 14

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Стандартизация в Российской Федерации**

**АНТИТЕРРОРИСТИЧЕСКАЯ ЗАЩИЩЕННОСТЬ**

**Общие требования к техническим средствам и системам антитеррористической защиты.**

Anti-terrorism security of buildings and structures. Events and decisions to ensure the anti-terrorism security of buildings and structures. General requirements

**Дата введение — 2019–хх–хх**

## 1 Область применения

Настоящий стандарт распространяется на объекты капитального строительства жилого, общественного, социально-культурного, коммунально-бытового и производственного назначения. Настоящий стандарт не распространяется на линейные объекты.

Настоящий стандарт:

— устанавливает общий подход к вопросам обеспечения антитеррористической защищенности зданий и сооружений, основанный на снижении риска с применением связанных с антитеррористической защищенностью технических систем и средств, а также внешних средств уменьшения риска;

— определяет состав, роль и место технических систем и средств, связанных с обеспечением антитеррористической защищенности зданий и сооружений, в достижении минимально необходимого уровня антитеррористической защищенности объекта;

С учетом особенностей объектов различного функционального назначения федеральные органы исполнительной власти соответствующей отрасли могут устанавливать дополнительные требования в установленном законодательством Российской Федерации порядке.

## 2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты и/или классификаторы:

ГОСТ Р 1.5-2012 Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения

ГОСТ Р Антитеррористическая защищенность зданий и сооружений.Термины и определения

ГОСТ Р ИСО/МЭК 19794-5-2013 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ГОСТ Р ИСО/МЭК 19795-1-2007 Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура

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

ГОСТ Р 50775-95 (МЭК 60839-1-1:88) Системы тревожной сигнализации.Часть 1. Общие требования. Раздел 1. Общие положения

2.1 ГОСТ Р 50776 (МЭК 60839-1-4:1989) Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

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

ГОСТ Р 51110-97 Средства защитные банковские. Общие технические требования

ГОСТ Р 51136-2008 Стекла защитные многослойные. Общие технические условия

ГОСТ Р 51222-98 Средства защитные банковские. Жалюзи. Общие технические

ГОСТ Р 51224-98 Средства защитные банковские. Двери и люки. Общие технические условия

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

ГОСТ Р 51242-98 Конструкции защитные механические и электромеханические для дверных и оконных проемов. Технические требования и методы испытаний на устойчивость к разрушающим воздействиям

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51287-99 Техника телефонная абонентская. Требования безопасности и методы испытаний

ГОСТ Р 51558-2014 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний

ГОСТ Р 51635-2000 Мониторы радиационные ядерных материалов. Общие технические условия

ГОСТ Р 52435-2005 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний

ГОСТ Р 52502-2012 Жалюзи-роллеты металлические. Технические условия

ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения

ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования

ГОСТ Р 53705-2009 Системы безопасности комплексные. Металлообнаружители стационарные для помещений. Общие технические требования. Методы испытаний

ГОСТ Р 54830-2011 ”Системы охранные телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов”

СП 44.13330.2011 Административные и бытовые здания. «СНиП 2.09.04-87* »

СП 52.13330.2011 «СНиП 23-05-95* Естественное и искусственное освещение»

СП 54.13330.2011 «СНиП 31-01-2003 Здания жилые многоквартирные»

СП 56.13330.2011 «СНиП 31-03-2001 Производственные здания»

СП 59.13330.2012 «СНиП 35-01-2001. Доступность зданий и сооружений для маломобильных групп населения»

СП 118.13330.2012 «СНиП 31-06-2009 Общественные здания и сооружения»

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов (сводов правил и/или классификаторов) в информационной системе общего пользования - на официальном сайте федерального органа исполнительной власти в сфере стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю ”Национальные стандарты”, который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячно издаваемого информационного указателя ”Национальные стандарты” за текущий год. Если заменен ссылочный стандарт (документ), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (документа) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (документ), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (документа) с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт (документ), на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт (документ) отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

## 3 Общие требования к средствам и сооружениям инженерно-технической укрепленности

3.1 Инженерно-техническая укрепленность объекта предназначена для:

— защиты людей и самого объекта путем создания физической преграды, препятствующей несанкционированным действиям нарушителя;

— создания препятствий на пути движения нарушителя с целью затруднения (задержки) продвижения нарушителя к объектам защиты на время, достаточное для прибытия сил реагирования;

— обеспечения доступа в охраняемые зоны, здания, сооружения и помещения только через установленные рубежи доступа;

— обозначения границ охраняемых зон;

— предотвращения таранного прорыва транспортных средств в охраняемую зону;

— создания благоприятных условий силам охраны для решения служебных задач.

3.2 К инженерным средствам и сооружениям инженерно-технической укрепленности относятся:

— ограждения периметра и отдельных участков территории;

— инженерные заграждения;

— инженерные средства и сооружения периметра;

— противотаранные устройства и устройства снижения скорости движения автотранспорта;

— контрольно-пропускные пункты;

— помещения для размещения подразделений охраны;

— средства защиты оконных проемов зданий и сооружений;

— средства защиты дверных проемов зданий, сооружений и помещений;

— замки и запирающие устройства;

— стены, перекрытия и перегородки зданий, сооружений и помещений.

Выбор средств для конкретного объекта определяется в задании на проектирование объекта и техническом задании на проектирование САТЗ с учетом требований нормативных документов.

3.3 Большинство средств строятся на основе физических барьеров, которые по функциональному признаку подразделяют на постоянные, переносные и управляемые физические барьеры.

Физические барьеры должны удовлетворять следующим требованиям:

— обладать прочностью и долговечностью;

— затруднять нарушителю несанкционированный проход через рубеж доступа;

— ограничивать использование нарушителем подручных средств;

— обеспечивать достаточную пропускную способность при санкционированном или аварийном проходе;

— не оказывать влияния на работу технических средств охраны;

— обеспечивать эффективную работу службы охраны.

Постоянные физические барьеры предназначены для обозначения границ объекта и охраняемых зон и создания препятствий продвижению нарушителя к цели преступной акции.

К постоянным физическим барьерам относятся строительные конструкции объекта охраны и специально разработанные конструкции:

— стены, перекрытия;

— ограждения, инженерные заграждения, решетки, усиленные двери, неавтоматические противотаранные устройства, стационарные устройства снижения скорости движения автотранспорта и другие физические препятствия. К переносным средствам физической защиты инженерным относятся:

— противотаранные упоры;

— мобильные средства для принудительной остановки транспорта;

— малые архитектурные формы;

— переносные (мобильные) ограждения.

Управляемые средства физической защиты инженерные и/или устройства преграждающие управляемые предназначены для обеспечения санкционированного доступа на объект и в охраняемые зоны объекта через установленные рубежи доступа, а также создания условий для задержания нарушителя на рубежах доступа при попытке несанкционированного прохода/проезда. К ним относятся:

— ворота распашные, раздвижные, в том числе с электроприводом; турникеты, шлагбаумы;

— автоматизированные и автоматические противотаранные устройства; калитки, двери в помещения, в том числе с дистанционно управляемыми запирающими устройствами.

Места установки, типы и плотность инженерных заграждений определяются заданием на проектирование.

3.4 По функциональному назначению ограждения подразделяются на:

— основные;

— дополнительные;

— локальных зон.

К основным ограждениям предъявляются следующие общие требования:

— достаточная высота и заглубленность в грунт, максимально затрудняющие его преодоление и удовлетворяющие режимным условиям объекта;

— простота конструкции, высокая прочность и долговечность;

— отсутствие узлов и конструкций, облегчающих его преодоление;

— экономичность строительства и эксплуатации.

Основные ограждения могут быть сплошными и просматриваемыми. При выборе типа и высоты ограждения должны учитываться функциональное назначение объекта, его архитектурные решения, историческое и культурное значение, а также риски совершения террористических актов в отношении объекта.

Основное ограждение объекта может быть:

— железобетонным толщиной не менее 100 мм;

— каменным, кирпичным толщиной не менее 250 мм;

— сплошным металлическим с толщиной листа не менее 2 мм, усиленным ребрами жесткости;

— из профлиста;

— из сетчатых секций с диаметром прутков не менее 5 мм и ячейками размером не более 50х100 мм;

— из металлических прутьев диаметром не менее 12 мм, в том числе архитектурно оформленным.

В местах въезда/выезда на территорию объекта автомобильного транспорта в ограждении устанавливаются ворота. По периметру ограждения территории охраняемого объекта могут быть установлены основные и запасные ворота.

При необходимости (оговаривается в техническом задании на проектирование) подъезды автомобильного транспорта к периметру территории объекта помимо ворот могут оборудоваться устройствами снижения скорости движения транспортных средств либо противотаранными устройствами.

В дренажных канавах, проходящих под основным ограждением, устанавливаются сварные металлические решетки, изготовленные из прутков арматурной стали диаметром не менее 16 мм и ячейками не более 150 х 150 мм.

Дополнительное ограждение устанавливается для затруднения преодоления нарушителем основного ограждения при необходимости в случаях установления таких требований нормативными документами или заказчиком в задании на проектирование.

Ограждения локальных зон устанавливаются внутри территории объекта для ограждения отдельных зданий и сооружений или временных территорий и могут быть как постоянного типа, так и временного.

Локальные ограждения постоянного типа как правило могут применяться для ограждения отдельно стоящих технологических зданий ( резервные подстанции, ТП и т.п), имеющие важное значения для функционирования объекта. Высота ограждений должна быть не менее 2 м и иметь запирающиеся калитки.

Локальные ограждения временного типа как правило применяются для ограждения временных участков территории объекта, для организации временных парковок, организации прохода людей и т.п

3.5 В зависимости от функционального назначения на объекте могут быть организованы КПП для:

— прохода персонала объекта и посетителей (КПП);

— проезда автомобильного транспорта (ТКПП).

Количество КПП на охраняемом объекте определяется в зависимости от протяженности периметра объекта, его конфигурации, интенсивности движения людей и транспорта через КПП.

Устройство помещения КПП для сотрудников охраны должно иметь достаточный обзор и обеспечивать надежную защиту охранника. Требования к обеспечению безопасности охранников распространяются на все виды КПП.

Строительные конструкции зданий и сооружений КПП (стены, перекрытия, оконные и дверные проемы), выходящие на внешнюю сторону ограждения должны иметь класс защиты, соответствующий категории объекта, и быть устойчивы к противоправным действиям, включая террористические акты.

Управление воротами и шлагбаумами может осуществляться дистанционно охранником КПП. Ворота и шлагбаумы должны иметь электромеханический и ручной привод.

При ТКПП на линии ограждения организуются досмотровые зоны транспорта, количество которых определяется интенсивностью движения автомобильного транспорта через КПП и, при необходимости, необходимой пропускной способностью, контрольно-пропускными пунктами для досмотра пассажиров и лиц, сопровождающих грузы, а также противотаранными устройствами (при необходимости. Досмотровая зона транспорта оборудуется последовательно расположенными шлагбаумами (воротами) на расстоянии, обеспечивающим размещение между ними и возможность организации досмотра не менее одного транспортного средства.

Для контроля подъезжающего транспорта и прибывающих граждан сплошные ворота и входная дверь на территорию объекта оборудуются смотровыми окошками или «глазками», переговорными устройствами, видеокамерами.

КПП для прохода персонала и посетителей должны обеспечивать необходимую пропускную способность прохода людей и проезда транспорта.

Места размещения КПП для прохода людей на периметре объекта должны быть согласованы с маршрутами движения общественного и специализированного транспорта.

Двери объекта и его помещений должны быть исправными, хорошо подогнанными под дверные коробки.

Дверные конструкции должны обеспечивать надежную защиту помещения объекта от разрушающих воздействий.

3.6 Оконные конструкции (окно, форточка, фрамуга) в помещении охраняемого объекта должны быть остеклены, иметь надежные и исправные запирающие устройства и обеспечивать надежную защиту помещения объекта.

Оконные стекла должны быть жестко закреплены в пазах.

Оконные проемы специальных помещений объекта, требующих повышенных мер защиты, независимо от этажности, в обязательном порядке оборудуются защитными конструкциями или защитным остеклением.

3.7 Вентиляционные короба, дымоходы и другие технологические каналы и отверстия, диаметром более 200 мм, имеющие выход на крышу или в смежное помещение и своим сечением входящие в помещение, где размещены материальные ценности, должны быть оборудованы на входе металлическими решетками, изготовленными из стальных прутьев сечением не менее 78 кв.мм, свариваемых в пересечениях, с ячейкой 150 х 150 мм.

Решетка в вентиляционном коробе, дымоходе со стороны охраняемого помещения должна отставать от внутренней поверхности стены (перекрытия) не более чем на 100 мм.

Допускается для защиты вентиляционного короба и дымохода использовать фальшрешетку с ячейкой не более 100 х 100 мм из металлической трубки с диаметром отверстия не менее 6 мм для протягивания провода шлейфа сигнализации.

3.8 Водопропуски сточных или проточных вод, подземные коллекторы (кабельные, канализационные) при диаметре трубы или коллектора 300 500 мм, выходящие с территории объекта, должны быть оборудованы металлическими решетками.

## 4 Общие требования к техническим средствам охраны

### 4.1 Общие требования к системе контроля и управления доступом

4.1.1 Система должна обеспечивать:

— санкционированный доступ людей и транспортных средств на территорию объекта и в зоны ограниченного доступа в соответствии с правами доступа по идентификационным признакам;

— предотвращение несанкционированного доступа на объект и в зоны ограниченного доступа людей и транспортных средств;

— выдачу информации на пульт централизованного наблюдения о попытках несанкционированного прохода (проезда) людей (транспортных средств) на охраняемый объект или в зону ограниченного доступа;

— разграничение доступа в соответствии с зонированием объекта;

— контроль перемещения людей и транспортных средств внутри объекта;

— контроль перемещения по объекту, а также выноса с объекта оборудования, прошедшего специальную проверку и оснащенного чипами с электронной меткой;

— взаимодействие с другими системами на аппаратном и программном уровнях;

— разблокировку на выход дверей и заграждений при ЧС.

4.1.2 Система должна выполнять следующие основные функции:

— установление действительности представленных оснований для прохода в зону ограниченного доступа.

— управление устройствами заграждения и оповещения, исполнительными устройствами инженерных систем защиты;

— регистрацию, выдачу и аннулирование электронных меток;

— установку уровня доступа для пользователей;

— регистрацию входов, выходов и попыток несанкционированного проникновения;

— дистанционное перепрограммирование кодовых замков;

— хранение и документирование информации;

— идентификацию личности (транспортного средства) при проходе (въезде) на объект.

4.1.3 Система контроля и управления доступом должна включать:

— подсистему контроля и управления доступом посетителей;

— подсистему контроля и управления доступом обслуживающего персонала;

— подсистему контроля и управления доступом пользователей объектом;

— подсистему контроля и управления доступом в зонах безопасности

— подсистему контроля и управления доступом транспортных средств (транспортные КПП);.

4.1.4 Подсистема контроля и управления доступом транспортных средств (транспортный КПП) должна обеспечить:

— идентификацию транспортных средств по государственным номерным знакам и/или дистанционно считываемым электронным идентификационным номерам;

— предотвращение таранного прорыва транспортных средств в зону безопасности;

— беспрепятственный пропуск транспортных средств имеющих право проезда без досмотра;

— беспрепятственный пропуск специальных транспортных средств, участвующих в локализации (ликвидации) чрезвычайной ситуации.

Основным элементом подсистемы контроля и управления доступом транспортных средств в зону безопасности является транспортный КПП.

4.1.5 Подсистема контроля и управления доступом посетителей должна обеспечивать:

— идентификацию прибывающих лиц;

— установление действительности представленных оснований для прохода в зону безопасности.

4.1.6 Подсистема контроля и управления доступом обслуживающего персонала должна обеспечивать:

— идентификацию прибывающих лиц;

— установление действительности представленных оснований для прохода в зону безопасности.

4.1.7 Средствами системы контроля и управления доступом должны быть оборудованы все входы/выходы (въезды/выезды) на объект, в зоны ограниченного доступа. Входы/выходы в помещения с массовым пребыванием людей в объекте оборудуются средствами СКУД в соответствии с заданием заказчика.

4.1.8 Входные двери подъездов в жилую зону МКД, в зоны свободного доступа других объекта должны быть оборудованы домофонами (должны быть установлены вызывные и/или кодонаборные панели).

4.1.9 Нормативные документы рекомендуемые для применения при разработке проектных решений по построению СКУД:

ГОСТ Р 51241-2008, ГОСТ Р 52551-2016, [9].

### 4.2 Требования к системе охранной и тревожной сигнализации

4.2.1 Система охранно-тревожной сигнализации включает:

— подсистему охранной сигнализации;

— подсистему тревожной сигнализации.

4.2.2 Подсистема охранной сигнализации должна обеспечивать:

— оповещение о несанкционированных попытках доступа на объект, в зоны ограниченного доступа (в выделенные помещения и т.д.);

— оповещение о проникновении в охраняемые зоны;

— централизованную или децентрализованную постановку помещений под охрану;

— на аппаратном уровне должна сопрягаться с системой контроля и управления доступом и системой охранного телевидения.

4.2.3 Оконечными устройствами подсистемы охранной сигнализации должны быть оборудованы:

— все кабинеты руководителей;

— служебные помещения с размещением вычислительной и оргтехники;

— помещения серверных, автоматизированных телефонных станций, кроссовых и других помещений средств связи и коммуникации;

— помещения с размещением систем инженерно-технического обеспечения объекта;

— все внешние двери и ворота объекта;

— двери технических этажей;

— колодцы, люки, лазы, шахты коммуникаций сечением 250х250 мм и более.

4.2.4 Постановку/снятие с охраны необходимо предусматривать как централизовано, так и децентрализовано (с кодонаборных устройств, размещаемых непосредственно в охраняемых помещениях).

4.2.5 Подсистема тревожной сигнализации предназначена для автоматической или ручной передачи сигналов тревоги (тревожных сообщений) на пульт охраны объекта и в подразделения войск национальной гвардии Российской Федерации (подразделения вневедомственной охраны войск национальной гвардии Российской Федерации) или в систему обеспечения вызова экстренных оперативных служб по единому номеру «112» 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 внешние двери и ворота объекта (оборудуются с внутренней стороны);

— помещения камер хранения;

— помещения, предназначенные для работы с ценностями;

— помещения дежурных служб объекта.

4.2.6 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 опасных факторов окружающей среды;

— восстанавливать работоспособное состояние после воздействия опасных факторов окружающей среды;

— быть устойчивым 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 бесконтрольного снятия/постановки под охрану.

4.2.7 Система охранно-тревожной сигнализации не должны выдавать ложных тревог при переключениях источников электропитания.

4.2.8 Нормативные документы рекомендуемые для применения при разработке проектной документации по построению СОТС:

ГОСТ Р 50009, ГОСТ Р 50775 (МЭК 60839-1-4), ГОСТ Р 50776 (МЭК 60839-1-4), ГОСТ Р 52435, ГОСТ Р 52551.

### 4.3 Требования к системам телевизионного наблюдения

4.3.1 Системы телевизионного наблюдения в целом предназначены для информационного обеспечения выполнения задач как по охране объекта, так и по выявлению и пресечению противоправных действий.

В этих целях в зависимости от функционального назначения объекта и установленных требований применяемые технические системы и средства СТН должны обеспечивать следующие функции (в сочетании или в отдельности):

— круглосуточного контроля границ территории объекта и охраняемых зон доступа (функции охраны - выполняет система охранного телевидения (СОТ) );

— непрерывного визуального контроля за критически важными элементами, служебными и техническими помещениями, охраняемыми зонами, а также прилегающей территорией объекта и подъездными путями с целью раннего обнаружения противоправных действий (функции видеомониторинга - выполняет система видеонаблюдения (СВН));

— идентификации физических лиц/транспортных средств (функции идентификации (распознования)и обнаружения тревожных ситуаций - выполняет система интеллектуального видеонаблюдения (СИВН));

— обеспечения необходимой видеоинформацией соответствующей службы (передачи видеоизображения на видеомонитор оператора видеонаблюдения в ЦПУ) для оценки поступивших тревожной сигналов от СОТС, СКУД, средств идентификации, а также возникновения тревожных сценариев в зонах наблюдения, для принятия управленческих решений и координации сил обеспечения безопасности.

— видеофиксации лиц и транспортных средств, пересекающих установленные границы охраняемой территории или зон;

— выделения из общей видеокартины и фиксирования лиц нарушителей с целью предоставления свидетельств для последующих следственных мероприятий и судебных разбирательств;

— повторного просмотра оператором не менее 100 событий, в том числе и при ограничении полномочий доступа к архиву;

— архивирования информации от телевизионных камер с разграничением полномочий доступа к ней.

4.3.2 Видеокамеры СТН необходимо устанавливать максимально близко к горизонтальной визирной линии по отношению к фиксируемому объекту.

В зависимости от решаемых задач СТН может сопрягаться с системой пожарной безопасности, системой контроля и управления доступом, системой охранно-тревожной сигнализации.

4.3.3 Системы охранного телевидения должны обеспечивает автоматизированный контроль за охраняемыми зонами объекта, а в случае получения извещения о тревоге позволять определить характер нарушения, место нарушения, количество нарушителей, направление движения нарушителя (нарушителей) и оптимальные меры противодействия.

В целях создания СОТ и выполнения охранных функций должно быть обеспечено взаимодействие технических средств СТН с СОТС.

Выдаваемые на экраны мониторов видеоизображения, в зависимости от режима работы, должны сопровождаться информацией о времени, дате и месте поступления сигнала от системы охранной сигнализации.

В целях выявления попыток реализации террористических угроз путем выводы из строя оборудования инженерно-технического обеспечения в помещениях с технологическим оборудованием необходимо предусматривать возможность контрольного видеонаблюдения во время проведения в них каких-либо работ обслуживающим персоналом. Для решения этой задачи должно быть обеспечено взаимодействие технических средств СТН с СКУД.

4.3.4 Система видеонаблюдения обеспечивает наблюдение за обстановкой на охраняемой территории и/или зоне объекта (видеомониторинг), за критически важными элементами объекта, в помещениях с массовым пребыванием людей в режиме реального времени.

Получаемая от СВН видеоинформация анализируется операторами. В этих целях организуется отдельный пост видеонаблюдения с дежурным оператором видеонаблюдения; В соответствии с разработанными регламентами передачи информации видеоинформация может передаваться и иным центрам управления.

Допускается вывод изображения от видеокамер на видеомонитор оператора СВН размером не более 100х150 мм мм со следующей детализацией цели видеонаблюдения в зависимости от решаемой видекамерой задачи:

— обнаружения - не менее 10% высоты изображения (или более 40 мм на пиксель);

— наблюдения - не менее 25% высоты изображения (или более 16 мм на пиксель ;

— распознавания - не менее 50% высоты изображения (или более 8 мм на пиксель;

— идентификации - не менее 100% высоты изображения (или более 4 мм на пиксель;

— детального осмотра - не менее 400% высоты изображения (или более 1 мм на пиксель;

СВН входных дверей подъездов МКД должны подключаться к локальным центрам мониторинга Системы обеспечения безопасности субъекта Российской Федерации (административно-территориальной единицы).

4.3.5 Системы интеллектуального видеонаблюдения - это комплекс аппаратных и программных средств, предназначенных для автоматического обнаружения тревожных событий (сценариев), определяемых набором заранее заданных критериев, и реакция на обнаружение по установленному правилу в режиме реального времени.

В зависимости от установленных требований и решаемых задач на объекте СИВН должна обеспечивать:

— идентификацию или распознавание физических лиц;

— распознавание номерных знаков;

— выявление тревожных ситуаций по заранее определенным сценариям;

— сопровождение объекта;

— обнаружение объекта;

4.3.6 Системы телевизионного наблюдения должны обеспечивать автоматическую запись видеоинформации в архив и хранение данных в течение одного месяца для последующего просмотра и анализа.

Видеозапись в зависимости от требований безопасности охраняемого объекта и решаемой задачи может производиться:

— непрерывно;

— периодически по заданному расписанию;

— по срабатыванию средств обнаружения проникновения;

— по срабатыванию видеодетектора системы охранной телевизионной.

4.3.7 В целом СТН должны соответствовать требованиям ГОСТ Р 51558-2014 ”Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний”.

4.3.8 Основные технические характеристики применяемых средств и систем СТН в целях АТЗ объектов должны отвечать следующим требованиям:

— изображения, получаемые при помощи СТН, должны отображать максимально возможное число признаков, идентифицирующих объекты.

— разрешение регистрируемого видеоизображения - не менее 1,2 мегапикселя

— частота кадров средств регистрации видеоизображений- не менее 25 кадров в секунду для средств СОТ и СВН и не менее 16 кадров в секунду для средств СИВН;

— расстояние между центрами глаз на изображении лица, зарегистрированном на рабочей дистанции съемки должно составлять не менее 60 пикселей (для области в центре кадра и на расстоянии до одной третьей ширины, высоты и диагоналей кадра от центра включительно);

— глубина резко отображаемого пространства - не менее 1 метра (для области в центре кадра и на расстоянии до одной третьей ширины, высоты и диагоналей кадра от центра включительно);

— максимальное отношение ”сигнал - шум” (с выключенной функцией автоматического усиления сигнала) - не менее 45 дБ;

— технические характеристики системам и средствам обнаружения тревожных ситуаций в зависимости от сценария должны обеспечивать:

а) чувствительность - не менее 99-95 %;

б) специфичность - не менее 95-99 %;

в) время реакции на появление (движения, оставление, исчезновение) объекта (человека, транспортного средства, животного) в запрещенной зоне изменение в сцене (затемнение изображения, расфокусировка, засветка) настраивается в диапазоне от 1 до 300 секунд с шагом 1 секунда;

— степень сжатия - не более 30 процентов по стандарту H 264 или MJPEG. Степень сжатия определяется по ГОСТ Р 54830-2011 ”Системы охранные телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов”;

— использование чересстрочной развертки не допускается;

— оптическая разрешающая способность по горизонтали - не менее 800 линий на горизонтальный размер кадра, по вертикали - не менее 650 линий на вертикальный размер кадра;

— взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

— обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

— настройка скорости видеозаписи средствами видеозаписи СТН должна обеспечивать при отсутствии движения в кадре в диапазоне от 3 до 30 кадров в секунду с шагом 1 секунда и при автоматическом обнаружении движения не менее 12 кадров в секунду;

— цикличность видеозаписи - не менее 24 часов при использовании максимального для изделия количества видеокамер и следующих характеристик видеопотока:

а) разрешение (число пикселей в каждом кадре) - не менее 1,2 мегапикселя;

б) горизонтальное разрешение кадра - не менее 1200 пикселей;

в) вертикальное разрешение кадра - не менее 1000 пикселей;

4.3.9 Нормативные документы, рекомендуемые для применения при разработке проектных решений по построению СТН:

ГОСТ Р 51558-2014, ГОСТ Р 54830-2011, ГОСТ Р ИСО/МЭК 19794-5-2013,ГОСТ Р ИСО/МЭК 19795-1-2007,[1], [10].

### 4.4 Требования к системе охранного освещения

4.4.1 Система охранного освещения должна обеспечивать необходимые условия видимости на ограждении периметра территории объекта и охраняемых зонах.

В состав охранного освещения должны входить:

— осветительные приборы;

— кабельные и проводные сети;

— аппаратура управления.

Система охранного освещения должна обеспечивать:

— освещенность горизонтальную на уровне земли или вертикальную на плоскости ограждения, стены не менее 0,5 лк в темное время суток;

— равномерно освещенную сплошную полосу вдоль ограждения периметра шириной 3-4 м;

— освещенность в плоскости лица или зоны регистрации тревожных ситуаций в целях идентификации лица и/или обнаружения тревожных ситуаций СИВН - не менее 100 лк;

— возможность автоматического включения дополнительных источников света на отдельном участке (зоне) охраняемой территории (периметра) при срабатывании охранной сигнализации;

— ручное управление работой освещения из помещения службы безопасности объекта;

— непрерывность работы на лестничных клетках, в тамбурах, в помещениях и на постах охраны.

4.4.2 В темное время суток, если освещенность охраняемой зоны ниже чувствительности видеокамер, объект (охраняемая зона объекта) должен оборудоваться охранным освещением видимого диапазона.

4.4.3 Зоны охранного освещения должны совпадать с зоной обзора видеокамеры. При использовании СОТ цветного изображения применение инфракрасного освещения недопустимо.

4.4.4 Осветительные приборы охранного освещения могут быть любого типа: подвесные, консольные, прожектора и другие типы.

Лампы охранного освещения должны быть защищены от механических повреждений.

4.4.5 В обоснованных случаях функции охранного освещения может выполнять архитектурное, уличное и другое освещение.

4.4.6 Нормативные документы рекомендуемые для применения:

ГОСТ Р 51558, СП 52.13330, [1], [10].

### 4.5 Требования к системе экстренной связи

Система экстренной связи представляет собой систему, обеспечивающую незамедлительную видео и аудио связь граждан из пунктов связи с оперативными службами административно-территориальной единицы.

Она предназначена для предотвращения и своевременного пресечения противоправных посягательств в том числе вследствие возникновения потенциальных угроз террористического характера жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

С этой целью на зданиях и сооружениях, территории в необходимых, обоснованных случаях организуются пункты экстренной связи жителей с территориальными отделами федеральных органов исполнительной власти (пунктами безопасности), оснащенные переговорными устройствами и системами видеонаблюдения в антивандальном исполнении.

Система должна обеспечивать круглосуточное выполнение следующих функций:

— поддерживать двустороннюю (полнодуплексную) аудио связь пользователя из пункта связи с диспетчером СЭС в пункте наблюдения/экстренной связи;

— поддерживать видеонаблюдение (диспетчером СЭС) пользователя системы во время его связи;
— передачу аудио и видеоинформации;
— архивирование аудио и видеоинформации;

СЭС интегрируется с СОТ объекта, с использованием общих компонентов системы электропитания, домового регистратора, видеокамер, коммутационного, кроссового и вспомогательного оборудования, а также линии связи.

При развертывании пункта связи СЭС на внутридомовой территории или ином месте, согласованном с федеральными органами исполнительной власти, видеокамера(ы), переговорное устройство подключаются к системе электроснабжения/связи ближайшего здания.

Переговорное устройство СЭС должно:

— быть климатически устойчиво (работать в диапазоне температур минус 40°…плюс 40°С);
— быть устойчиво к вандализму;
— обеспечивать двустороннюю (полнодуплексную) связь с диспетчером;
— обеспечивать удаленную диагностику;
— обеспечивать удаленный сброс состояния.

От переговорного устройства кабель связи прокладывается до домового регистратора или к аудио входу видеокамеры (в случае его наличия), наблюдающей за пунктом связи.

Размещение пункта связи СЭС определяется конкретными условиями и выполняется на домах и придворовых территориях.

Размещение пункта связи СЭС должно проектироваться на входе в подъезд жилого здания.

Переговорное устройство должно быть размещено на подъездной двери проектируемого жилого здания. При наличии домофона рядом с ним.

Видеонаблюдение осуществляется видеокамерой СОТ, контролирующей вход в подъезд.

Место размещения пункта связи СЭС на придворовой территории должно быть согласовано с органами внутренних дел района застройки.

Пункт связи СЭС должен подключаться к СОТ проектируемого здания.

В состав пункта связи в этом варианте размещения должны входить: переговорное устройство на вызывной панели — кнопка вызова диспетчера СЭС, микрофон, динамик; скрытая видеокамера (пинхол), монтируемая на вызывной панели; видеокамера обзора на поворотном устройстве и прожектор подсветки, размещаемый на том же поворотном устройстве

## 5 Требования к системе выявления диверсионно-террористических средств

5.1 Система выявления диверсионно-террористических средств ( далее СВДТС - это совокупность систем и средств досмотра и локализации, позволяющих в зависимости от функционального назначения объекта и задания на проектирование выявлять попытки проноса на объект (в охраняемую зону) запрещеннх для проноса предметов и веществ, которые могут быть использованы для совершения террористических актов (взрывчатые, химические, отравляющие, наркотические, биологических и радиоактивных вещества, оружие, боеприпасы, патроны к оружию, взрывные устройства), а также локализовать террористические средства или минимизировать возможные последствия в случае, когда предотвратить террористический акт не удалось.

5.2 СВДТС должна обеспечивать:

— контроль и индивидуальный досмотр персонала и посетителей объекта, а также въезжающего в контролируемую зону транспорта на предмет возможного наличия у них средств совершения террористических актов;

— обнаружение средств совершения террористических актов, скрытно проносимых на человеке и в его ручной клади, почтовой корреспонденции, поставляемых на объект транспортным средством грузов;

— снижение последствий воздействия поражающих факторов взрывного устройства или предотвращение срабатывания взрывного устройства с радиовзрывателем.

5.3 Входные группы на объект в зависимости от класса здания (сооружения), его функционального назначения, установленных требований к антитеррористической защищенности, анализа уязвимости объекта (в случае его проведения) и решаемых задач могут быть оснащены минимально необходимым набором из следующих технических систем и средств обнаружения :

— металлодетектор ручного ;
— металлообнаружитель стационарный;

— стационарный радиационный монитор;
— рентгенотелевизионной установки конвейерного типа (интроскоп);
— газоанализатора паров ВВ (детектор ВВ);
— средстав выявления диверсионно-террористических средств на человеке и /или в ручной клади, почтовой корреспонденции, основанных на альтернативных принципах;
— детектор отравляющих, химических и биологических веществ.
— средства локализации взрыва.

5.4 На объекта массового пребывания людей, где требуется обеспечить заполнение объекта в определенный промежуток времени средства СВДТС должны обеспечивать требуемую пропускную способность входных досмотровых групп (входных групп контроля).

Пропускная способность входных групп подразделяется на:

— малую – 200-300 чел./ч;
— среднюю – 400-600 чел./ч;
— высокую – более 600 чел./ч.

При малом и среднем потоках посетителей, для проверки входящей почтовой корреспонденции могут использоваться технические средства обнаружения биологических агентов, в том числе установленные на входных группах.

При высоком потоке посетителей входящая почтовая корреспонденция должна поступать на отдельный пост, где проводится соответствующая ее проверка.

5.5 Система выявления диверсионно-террористических средств на въездных группах должна размещаться на стационарном пункте досмотра транспортных средств (его необходимость устанавливается заданием на проектирование).

Система выявления диверсионно-террористических средств на въездных группах может состоять в зависимости от категории объекта, кроме выше указанных средств на входных группах, из минимально необходимого ряда технических средств обнаружения, в том числе:

— стационарного радиационного монитора;
— досмотрового радиометрического комплекса;
— переносного рентгенотелевизионного прибора;
— газоанализатора паров ВВ (детектор ВВ);
— детектор отравляющих, химических и биологических веществ
— стационарных автоматизированных видеосистем сканирования днища транспортных средств;
— портативных средств визуального досмотра транспортных средств.

5.6 Состав оборудования и необходимость его использования должен уточняться при проектировании на основании анализа уязвимости конкретного объекта (в случае его проведения).

5.7 Стационарный пункт досмотра транспортных средств должен обеспечить надежность выявления террористических средств и одновременно высокую пропускную способность.

5.8 При выборе технических систем и средства досмотра необходимо руководствоваться следующими основными требованиями к их функциональным свойствам. Они должны обеспечивать:

а) не менее 49 случаев правильного обнаружения радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

б) не менее 49 случаев правильного идентифицирования радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

в) не более 3 случаев ложного обнаружения радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

г) не более 3 случаев ложной идентификации радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств из 50 испытаний;

д) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

е) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

5.9 Для обеспечения безопасности людей в случаях обнаружения подозрительных бесхозных предметов на объектах проектными решениями целесообразно предусматривать оснащение объекта ) средствами локализации взрыва с целью их применения подразделениями службы безопасности объекта или групп быстрого реагирования (при их наличии.

К данным средствам, в частности, относятся:

— стационарный (носимый) передатчик помех (блокиратор радиоуправляемых взрывных устройств);

— средство локализации взрыва.

Стационарный (носимый) передатчик помех должен обеспечивать излучение широкополосного помехового сигнала, как во всем диапазоне рабочих частот, так и в любом сочетании частотных литер передатчиков. В зависимости от мощности радиус действия РП должен составлять не менее 10 м.

Средство локализации взрыва должно обеспечить подавление фугасного, осколочного и термического действия взрывного устройства при взрыве.

### 5.1 Требования к системе контроля воздушно-газовой среды в системах вентиляции и кондиционирования

Системы контроля воздушно-газовой среды должна обеспечивать обнаружение отравляющих и других опасных веществ, горючих и токсичных газов, биологических агентов, перечень которых должен уточняться в техническом задании, на основании требований, установленных нормативными документами федеральных органов исполнительной власти.

В случае выявления веществ, подлежащих обнаружению, должны определяться их концентрация и выдаваться соответствующие сообщения дежурным операторам в ЦПУ и диспетчерского пункта управления инженерными системами.

В случае превышения концентрации отравляющих и других опасных веществ, горючих и токсичных газов выше установленной, должны выдаваться автоматические сигналы остановки тех систем приточной вентиляции и кондиционирования воздуха, в которых обнаружено превышения концентрации для предотвращения дальнейшего распространения загрязненной воздушно-газовой среды.

## Библиография

[1] РД 78.36.003-2002. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств

[2] Федеральный закон от 30.12.2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»

[3] Градостроительный Кодекс Российской Федерации от 29.12.2004 г. № 190-ФЗ

[4] Федеральный закон от 21.07.1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»

[5]

[6] Постановление Правительства Российской Федерации от 16.02.2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию»

[7] Закон Российской Федерации от 21.07.1993 г. № 5485-1 «О государственной тайне»

[8]

[9] РД 78.36.006-2005. Выбор и применение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрепленности для оборудования объектов

[10] Р 78.36.005-2011. Выбор и применение систем контроля и управления доступом. Рекомендации

[11] Р 78.36.002-2010. Выбор и применение систем охранных телевизионных. Рекомендации