Некоммерческое партнерство «Объединение организаций в сфере проектирования

«Академический Проектный Центр (АПЦ)»

СТАНДАРТ ОРГАНИЗАЦИИ НП «АПЦ»

СТО – 94160974 – П-119-03-05.2014

УТВЕРЖДЕН
Общим собранием членов
Некоммерческого партнерства
«Объединение организаций в сфере проектирования
«Академический Проектный Центр (АПЦ)»
Протокол №14 от «23» мая 2014г.

Генеральный директор

_____ Ильичев В.А.

Обеспечение антитеррористической защищенности зданий и сооружений

МЕРОПРИЯТИЯ И РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ЗДАНИЙ И СООРУЖЕНИЙ

Общие требования

Москва 2014

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», правила разработки и оформления – ГОСТ Р 1.5-2004 «Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила построения, изложения, оформления и обозначения».

Сведения о стандарте организации

1. РАЗРАБОТАН Отделом комплексного обеспечения безопасности и антитеррористической защищенности Общества с ограниченной ответственностью «Научно-производственное объединение «Современные диагностические системы» (ООО «НПО СОДИС») при участии Общероссийской негосударственной некоммерческой организации «Национальное объединение саморегулируемых организаций, основанных на членстве лиц, осуществляющих подготовку проектной документации» и Некоммерческого партнерства «Объединение организаций в сфере проектирования «Академический Проектный Центр (АПЦ)» (НП «АПЦ»).

2. ВНЕСЕН ООО «НПО СОДИС».

3. УТВЕРЖДЕН Решением Общего собрания членов НП «АПЦ» (Протокол №14 от «23» мая 2014г.) И ВВЕДЕН В ДЕЙСТВИЕ с 03 июня 2014г.

4. В настоящем стандарте реализованы нормы следующих нормативных правовых актов в части противодействия терроризму:

- Федеральный закон от 6.03.2006 г. №35-ФЗ «О противодействии терроризму»;
- Федеральный Закон от 28.12.2010 г. № 390-ФЗ «О безопасности»;
- Указ Президента Российской Федерации от 12.05.2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»;
- Распоряжение Правительства Российской Федерации от 17.11.2008 г. № 1663-р «Об утверждении основных направлений деятельности Правительства Российской Федерации на период до 2012 года и перечня проектов по их реализации».

5. ВВЕДЕН ВПЕРВЫЕ.

Информация об изменениях к настоящему стандарту организации публикуется в информационном указателе «Технические регламенты и стандарты НП «АПЦ»». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в информационном указателе «Технические регламенты и стандарты НП «АПЦ»». Соответствующая информация, уведомление и тексты размещаются в информационной системе общего пользования — на официальном сайте НП «АПЦ» в сети Интернет прарс.ru

Содержание

Введение

Стандарт организации разработан в исполнение постановления Правительства Российской Федерации от 15.02.2011 г. № 73 «О некоторых мерах по совершенствованию подготовки проектной документации в части противодействия террористическим актам» и направлен на реализацию нормативных правовых документов Российской Федерации и требований Технического регламента «О безопасности зданий и сооружений» в области противодействия терроризму.

Настоящий стандарт является первым, входящим в пакет нормативной документации с общим наименованием «Обеспечение антитеррористической защищенности зданий и сооружений».

Общая структура комплекса документации, рекомендуемая к разработке, приведена в приложении Г.

Данный документ:

– определяет состав, роль и место систем, связанных с обеспечением антитеррористической защищенности зданий и сооружений, в достижении безопасности объекта;

– устанавливает общий подход к вопросам обеспечения антитеррористической защищенности зданий и сооружений, основанный на снижении риска с применением связанных с антитеррористической защищенностью систем и внешних средств уменьшения риска.

Стандарт разработан ООО «НПО «СОДИС» (Генеральный директор – *А.М. Шахраманьян*, руководитель разработки – Заместитель генерального директора *В.Г. Петров*) при участии Общероссийской негосударственной некоммерческой организации «Национальное объединение саморегулируемых организаций, основанных на членстве лиц, осуществляющих подготовку проектной документации» и Некоммерческого партнерства «Объединение организаций в сфере проектирования «Академический Проектный Центр (АПЦ)» (НП «АПЦ»).

СТАНДАРТ ОРГАНИЗАЦИИ НП «АПЦ»

МЕРОПРИЯТИЯ И РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ЗДАНИЙ И СООРУЖЕНИЙ ОБЩИЕ ТРЕБОВАНИЯ

Measures and the solutions for the guarantee of an anti-terrorist protection of buildings and construction. General requirements

Дата введения 03-06-2014

1 Область применения

1.1 Стандарт организации «Мероприятия и решения по обеспечению антитеррористической защищенности зданий и сооружений. Общие требования» (далее – стандарт) устанавливает общие требования к обеспечению антитеррористической защищенности зданий и сооружений.

1.2 Стандарт распространяется на жилые, общественные и производственные здания и сооружения.

1.3 Стандарт не распространяется на линейные объекты.

2 Нормативные ссылки

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

ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. Стандарты организаций. Общие положения

ГОСТ Р 1.5-2004 Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила построения, изложения, оформления и обозначения

ГОСТ Р 6.30-2003 Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов

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

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 условия

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 51558-2008 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 53778-2010 Здания и сооружения. Правила обследования и мониторинга технического состояния. Общие требования

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

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 и классификаторов в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому 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 документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения, обозначения и сокращения

3.1 В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **антитеррористическая защищенность объекта:** Состояние здания, строения, сооружения или иного объекта, при котором обеспечивается безопасность его функционирования посредством применения инженерно-технических и режимных мер, направленных на предотвращение совершения террористического акта.

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

3.1.3 **зона ограниченного доступа:** Участки территории и внутренние помещения объекта, доступ в которые разрешен только физическим лицам определенных категорий в соответствии с установленным пропускным режимом.

3.1.4 **инженерно-техническая укрепленность объекта:** Совокупность мероприятий, направленных на усиление конструктивных элементов зданий, помещений и охраняемых территорий, обеспечивающих необходимое противодействие несанкционированному проникновению в охраняемую зону, взлому и другим преступным посягательствам.
[1]

3.1.5 **критически важный элемент здания и сооружения:** Строительные конструкции, помещения с размещением технологического, инженерного оборудования и других систем, выход из строя которых или несанкционированное воздействие на которые может привести к возникновению чрезвычайной ситуации или нарушению нормального функционированию объекта.

3.1.6 **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.

3.1.7 **мероприятия по обеспечению антитеррористической защищенности объекта:** Комплекс организационно-технических мер направленных на обеспечение требований к планировочной организации земельного участка, отводимого под объект, к архитектурным и конструктивным решениям, к зонированию объекта, к техническим средствам и системам, а также поддержание их соответствия требованиям проектной документации в процессе эксплуатации объекта.

3.1.8 **объект (объект защищаемый):** Предприятие, организация, учреждение, заведение, жилое домовладение или жилой комплекс, комплекс зданий и/или сооружений (или их неотъемлемая составная часть, включая занимаемую территорию и прилегающую акваторию в отведенных границах), состояние которых контролируется или подлежит контролю с конкретной целью (для защиты от угроз и/или для профилактики угроз) и на основе соблюдения действующего законодательства.

3.1.9 **объект особо важный:** Объект, значимость которого определяется органами государственной власти Российской Федерации или местного самоуправления с целью определения мер по защите интересов государства, юридических и физических лиц от преступных посягательств и предотвращения ущерба, который может быть нанесен природе и обществу, а также от возникновения

чрезвычайной ситуации.

3.1.10 **объект критически важный:** Объект, нарушение или прекращение функционирования которого приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению, разрушению или существенному снижению безопасности жизнедеятельности населения, проживающего на этой территории, на длительный период времени.
[ГОСТ Р 52551-2006, пункт 2.4.1]

3.1.11 **объект повышенной опасности:** Объект, на котором используют, производят, перерабатывают, хранят или транспортируют радиоактивные, взрыво- и пожароопасные, опасные химические и биологические вещества, создающие реальную угрозу жизни и здоровью людей, а также окружающей среде.
[ГОСТ Р 52551-2006, пункт 2.4.3]

3.1.12 **программно-техническое обеспечение**: Совокупность технических и программных средств, позволяющая на основе информации от систем инженерно-технического обеспечения и технического состояния несущих конструкций, результатов математического и компьютерного моделирования осуществлять обнаружение негативных факторов, угрожающих антитеррористической защищенности зданий и сооружений, прогноз их возможного развития и формировать рекомендации по их локализации и устранению.

3.1.13 **обеспечение антитеррористической защищенности**: Реализация совокупности проектных решений, организационно-технических и специальных мероприятий, направленных на обеспечение безопасности здания (сооружения) с целью предотвращения совершения террористического акта и (или) минимизацию его последствий.

3.1.14 **система техническая антитеррористической защищенности:** Система, включающая в себя технические средства, обеспечивающие защищенность объекта и субъекта от террористических угроз.

3.1.15 **система контроля и управления доступом**: Совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью.
[ГОСТ Р 51241-2008, пункт 3.28]

3.1.16 **система мониторинга инженерно-технического обеспечения**: Совокупность технических и программных средств, позволяющая осуществлять сбор и обработку информации о различных параметрах работы системы инженерно-технического обеспечения здания (сооружения) с целью контроля возникновения в ней дестабилизирующих факторов и передачи сообщений о возникновении или прогнозе аварийных ситуаций в единую систему оперативно-диспетчерского управления города.
[ГОСТ Р 53778-2010, пункт 3.26]

3.1.17 **система мониторинга технического состояния несущих конструкций**: Совокупность технических и программных средств, позволяющая осуществлять сбор и обработку информации о различных параметрах строительных конструкций (геодезические, динамические, деформационные и др.) с целью оценки технического состояния зданий и сооружений.
[ГОСТ Р 53778-2010, пункт 3.25]

3.1.18 **система обеспечения антитеррористической защищенности:** Организационно-техническая система, включающая в себя совокупность технических систем антитеррористической защищенности, технических средств или их комплексов, программное обеспечение, персонал, а также документированные процедуры штатных действий персонала, эксплуатационную документацию, материалы, инструменты, приборы, необходимые для использования в антитеррористической защищенности объекта.

3.1.19 **система охранная телевизионная**: Телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения его защищенности.

3.1.20 **система охранной сигнализации**: Совокупность совместно действующих технических средств обнаружения проникновения (попытки проникновения) на охраняемый объект, сбора, обработки, передачи и представления в заданном виде информации о проникновении (попытке проникновения) и другой служебной информации.

3.1.21 **система тревожной сигнализации**: Совокупность совместно действующих технических средств, позволяющих автоматически или в ручную выдавать сигналы тревоги на пункт охраны (в дежурную часть органов внутренних дел) при нападении на объект в период его работы.

3.1.22 **сооружения и средства физической защиты инженерные:** Сооружения и средства (ограждения, преграды, барьеры, строительные конструкции, малые архитектурные формы), препятствующие своими физическими свойствами несанкционированному проникновению/проезду на объект и/или в охраняемую зону (на часть территории, объекта).

3.1.23 **точка доступа:** Место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные необходимыми средствами).
[ГОСТ Р 51241-2008, пункт 3.31]

3.1.24 **угроза террористическая**: Совокупность условий и факторов, создающих опасность реализации террористического акта.

3.1.25 **устройства преграждающие управляемые (УПУ):** Устройства, обеспечивающие физическое препятствие доступу и оборудованные исполнительными устройствами для управления их состоянием (турникеты, шлюзы, проходные кабины, двери и ворота, оборудованные исполнительными устройствами СКУД, а также другие подобные устройства).
[ГОСТ Р 51241-2008, пункт 3.35]

3.2 В настоящем стандарте применены следующие обозначения и сокращения:

ГАПВВ – газоанализатор паров взрывчатых веществ;

КПП – контрольно-пропускной пункт;

ЛВУ – локализатор взрывных устройств;

МОб – стационарный металлообнаружитель;

МИ – ручной металлоискатель;

ПРТУ – переносная рентгеновская установка;

ПТО АТЗ – программно-техническое обеспечение системы антитеррористической защищенности зданий и сооружений;

ПУ (ЦПУ, ЛПУ) – пункт управления (центральный ПУ, локальный ПУ);

РМ – радиационный монитор;

РП – передатчик помех (генератор помех, синтезатор помех);
РТУ – рентгенотелевизионная установка;
САТЗ – система обеспечения антитеррористической защищенности;
СВДТС – система выявления диверсионно-террористических средств;
СИБ – система информационной безопасности;
СКВГС – система контроля воздушно-газовой среды в системах вентиляции и кондиционирования;
СКУД – система контроля и управления доступом;
СМИС – система мониторинга инженерно-технического обеспечения;
СМНК - система мониторинга технического состояния несущих конструкций;
СОО – система охранного освещения;
СОС – система оперативной связи;
СОТ – система охранного телевидения;
СОТС – система охранной и тревожной сигнализации;
СрВД – средства визуального досмотра;
СЭС – система экстренной связи;
УПУ – устройство преграждающее управляемое.

4 Общие положения

4.1 Антитеррористическая защищенность объектов обеспечивается посредством:
– установления проектных значений параметров объектов и их качественных характеристик, соответствующих требованиям защищенности;
– реализации указанных значений и характеристик в процессе строительства;
– поддержания состояния таких параметров и характеристик на требуемом уровне в процессе эксплуатации.
4.2 Антитеррористическая защищенность объекта достигается:
– планировочной организацией земельного участка, отводимого под объект, осуществляемой с учетом требований защищенности;
– архитектурными и конструктивными решениями, принятыми с учетом требований защищенности;
– зонированием территории и помещений объекта с учетом функционального назначения, требований защищенности;
– созданием на объекте САТЗ.

5 Классификация объектов в целях обеспечения их антитеррористической защищенности

Классификация объектов предназначена для установления минимально необходимых требований обеспечения антитеррористической защищенности.
Объекты в зависимости от уровня ответственности [2], их назначения, а также от возраста, физического состояния и количества людей, находящихся в объекте, классифицируются согласно таблице 5.1.
Кроме того согласно [1] осуществляется категорирование охраняемого объекта: комплексная оценка объекта, учитывающая его экономическую или иную (например, культурную) значимость, в зависимости от характера и концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой охраны.

Таблица 5.1 – Классификация объектов в целях обеспечения их антитеррористической защищенности

Уровень	Класс		Подкласс	
Повышенный	А.1	Особо опасные и технически сложные объекты [3]	А.1.1	объекты использования атомной энергии (в том числе ядерные установки, пункты хранения ядерных материалов и радиоактивных веществ, пункты хранения радиоактивных отходов)
			А.1.2	гидротехнические сооружения первого и второго классов, устанавливаемые в соответствии с законодательством о безопасности гидротехнических сооружений
			А.1.3	сооружения связи, являющиеся особо опасными, технически сложными в соответствии с законодательством Российской Федерации в области связи
			А.1.4	линии электропередачи и иные объекты электросетевого хозяйства напряжением 330 киловольт и более
			А.1.5	объекты космической инфраструктуры
			А.1.6	объекты авиационной инфраструктуры
			А.1.7	объекты инфраструктуры железнодорожного транспорта общего пользования
			А.1.8	метрополитены
			А.1.9	морские порты, за исключением морских специализированных портов, предназначенных для обслуживания спортивных и прогулочных судов
			А.1.10	тепловые электростанции мощностью 150 мегаватт и выше
			А.1.11	опасные производственные объекты, на которых: – получаются, используются, перерабатываются, образуются, хранятся, транспортируются, уничтожаются опасные вещества в количествах, превышающих предельные. Такие вещества и предельные количества опасных веществ соответственно указаны в приложениях 1 и 2 к [4]. Не относятся к особо опасным и технически сложным объектам газораспределительные системы, на которых используется, хранится, транспортируется природный газ под давлением до 1,2 мегапаскаля включительно или сжиженный углеводородный газ под давлением до 1,6 мегапаскаля включительно; – получаются расплавы черных и цветных металлов и сплавы на основе этих расплавов; – ведутся горные работы, работы по обогащению полезных ископаемых, а также работы в подземных условиях
		Объекты производственного назначения, имеющие признаки уникальных [3]	А.1.12	Объекты в проектной документации которых предусмотрены: – высота более чем 100 метров; – пролеты более чем 100 метров; – наличие консоли более чем 20 метров; – заглубление подземной части (полностью или частично) ниже планировочной отметки земли более чем на 15 метров, не являющиеся особо опасными и технически сложными

Продолжение таблицы 5.1

Уровень	Класс		Подкласс	
Повышенный	А.2	Объекты непроизводственного назначения, имеющие признаки уникальных [3]	А.2.1	объекты, предназначенные для постоянного проживания и временного пребывания людей, в том числе: здания детских дошкольных образовательных учреждений, специализированных домов престарелых и инвалидов, больницы, спальные корпуса образовательных учреждений интернатного типа и детских учреждений; санатории и дома отдыха
			А.2.2	здания зрелищных и культурно-просветительных учреждений, в том числе: театры, кинотеатры, концертные залы, клубы, цирки, спортивные сооружения с трибунами, библиотеки и другие учреждения с расчетным числом посадочных мест для посетителей в закрытых помещениях и на открытом воздухе; музеи, выставки, танцевальные залы и другие подобные учреждения в закрытых помещениях
			А.2.3	здания организаций по обслуживанию населения, в том числе: здания организаций торговли; здания организаций общественного питания; вокзалы; поликлиники и амбулатории
			А.2.4	здания научных и образовательных учреждений, научных и проектных организаций, органов управления учреждений, в том числе: здания образовательных учреждений; здания органов управления учреждений, проектно-конструкторских организаций, информационных и редакционно-издательских организаций, научных организаций, банков, контор, офисов
			А.2.5	многоквартирные жилые дома (нежилые помещения, в которых предполагается единовременное нахождение более 50 человек, входы в жилую зону), гостиницы, общежития, кемпинги, мотели и пансионаты
Нормальный	В.1	Объекты производственного назначения [5]	В.1.1	критически важные объекты, не подпадающие под повышенный уровень ответственности
			В.1.2	особо важные объекты, не подпадающие под повышенный уровень ответственности
			В.1.3	объекты повышенной опасности, не подпадающие под повышенный уровень ответственности
			В.1.4	иные объекты, не подпадающие под повышенный уровень ответственности
	В.2	Объекты непроизводственного назначения, в которых согласно заданию на проектирование предполагается единовременное нахождение в любом из помещений более 50 человек [5]	В.2.1	объекты, предназначенные для постоянного проживания и временного пребывания людей, в том числе: здания детских дошкольных образовательных учреждений, специализированных домов престарелых и инвалидов, больницы, спальные корпуса образовательных учреждений интернатного типа и детских учреждений; санатории и дома отдыха
			В.2.2	здания зрелищных и культурно-просветительных учреждений, в том числе: театры, кинотеатры, концертные залы, клубы, цирки, спортивные сооружения с трибунами, библиотеки и другие учреждения с расчетным числом посадочных мест для посетителей в закрытых помещениях и на открытом воздухе; музеи, выставки, танцевальные залы и другие подобные учреждения в закрытых помещениях
			В.2.3	здания организаций по обслуживанию населения, в том числе: здания организаций торговли; здания организаций общественного питания; вокзалы; поликлиники и амбулатории

Окончание таблицы 5.1

Уровень	Класс		Подкласс	
Нормальный	В.2	Объекты непроизводственного назначения, в которых согласно заданию на проектирование предполагается единовременное нахождение в любом из помещений более 50 человек [5]	В.2.4	здания научных и образовательных учреждений, научных и проектных организаций, органов управления учреждений, в том числе: здания образовательных учреждений; здания органов управления учреждений, проектно-конструкторских организаций, информационных и редакционно-издательских организаций, научных организаций, банков, контор, офисов
			В.2.5	многоквартирные жилые дома (нежилые помещения, в которых предполагается единовременное нахождение более 50 человек, входы в жилую зону), гостиницы, общежития, кемпинги, мотели и пансионаты
	В.3	объекты непроизводственного назначения, в которых согласно заданию на проектирование предполагается единовременное нахождение в любом из помещений менее 50 человек [5]	В.3.1	объекты, предназначенные для постоянного проживания и временного пребывания людей, в том числе: здания детских дошкольных образовательных учреждений, специализированных домов престарелых и инвалидов, больницы, спальные корпуса образовательных учреждений интернатного типа и детских учреждений; спальные корпуса санаториев и домов отдыха
			В.3.2	здания зрелищных и культурно-просветительных учреждений, в том числе: театры, кинотеатры, концертные залы, клубы, цирки, спортивные сооружения с трибунами, библиотеки и другие учреждения с расчетным числом посадочных мест для посетителей в закрытых помещениях и на открытом воздухе; музеи, выставки, танцевальные залы и другие подобные учреждения в закрытых помещениях
			В.3.3	здания организаций по обслуживанию населения, в том числе: здания организаций торговли; здания организаций общественного питания; вокзалы; поликлиники и амбулатории
			В.3.4	здания научных и образовательных учреждений, научных и проектных организаций, органов управления учреждений, в том числе: здания образовательных учреждений; здания органов управления учреждений, проектно-конструкторских организаций, информационных и редакционно-издательских организаций, научных организаций, банков, контор, офисов
			В.3.5	многоквартирные жилые дома (входы в жилую зону), гостиницы, общежития, кемпинги, мотели и пансионаты
Пониженный	С.1	объекты производственного назначения	С.1.1	объекты временного (сезонного) назначения
			С.1.2	объекты вспомогательного использования, связанные с осуществлением строительства или реконструкции основного объекта
	С.2	объекты непроизводственного назначения	С.2.1	объекты временного (сезонного) назначения
			С.2.2	объекты вспомогательного использования, связанные с осуществлением строительства или реконструкции здания или сооружения
			С.2.3	объекты, расположенные на земельных участках, предоставленных для индивидуального жилищного строительства

6 Требования к подготовке проектной документации объектов в части обеспечения их антитеррористической защищенности

6.1 При проектировании объектов класса А, В.1, В.2 в составе проектной документации должен быть разработан подраздел «Мероприятия и решения по обеспечению противодействия террористическим актам» раздела «Сведения об инженерном оборудовании, о сетях инженерно-технического обеспечения, перечень инженерно-технических мероприятий, содержание технологических решений», подраздела «Технологические решения» [6].

6.2 Подраздел «Мероприятия и решения по обеспечению противодействия террористическим актам», разрабатываемый для объектов производственного назначения класса А.1, В.1 должен содержать:

– описание мероприятий и обоснование проектных решений (на основе полученных сведений об инженерном оборудовании, сетях инженерно-технического обеспечения, инженерно-технических мероприятиях, технологических решениях для проектируемого Объекта (сведений о расположении, количестве и основных характеристиках оборудования, а также принципиальные схемы инженерных и слаботочных систем)), направленных на предотвращение несанкционированного доступа на объект физических лиц, транспортных средств и грузов, осуществление контроля над ними в процессе эксплуатации;

– описание технических средств и проектные решения, направленные на обнаружение террористических средств.

6.3 Подраздел ««Мероприятия и решения по обеспечению противодействия террористическим актам»», разрабатываемый для объектов непроизводственного назначения класса А.2, В.2 должен содержать:

– описание мероприятий и проектных решений (на основе полученных сведений об инженерном оборудовании, сетях инженерно-технического обеспечения, инженерно-технических мероприятиях, технологических решениях для проектируемого Объекта (сведений о расположении, количестве и основных характеристиках оборудования, а также принципиальные схемы инженерных и слаботочных систем)), направленных на предотвращение террористических актов на объекте в процессе эксплуатации;

– описание технических средств и проектные решения, направленные на обнаружение террористических средств.

6.4 При проектировании объектов раздел «Проект организации строительства» должен содержать описание проектных решений и мероприятий по охране объектов в период строительства, в том числе и описание технических средств и проектные решения, направленные на обнаружение террористических средств [6].

6.5 В случае необходимости отступления от требований или недостаточности требований к антитеррористической защищенности, установленных нормативными документами при подготовке проектной документации на строительство объекта в соответствии с [2] должны разрабатываться специальные технические условия в порядке, установленном уполномоченным федеральным органом исполнительной власти.

6.6 Для объектов класса А перед разработкой проектной документации рекомендуется проведение анализа уязвимости объекта угрозам террористического характера (далее - анализ уязвимости).

6.7 Анализ уязвимости проводится индивидуально для конкретного объекта, с учетом особенностей самого объекта, его функционального назначения и подкласса, а также особенностей субъекта Российской Федерации (административно-

территориальной единицы), на территории которого он располагается. Для вновь проектируемых объектов первоначальный анализ уязвимости проводится на основе концептуальных проектных решений.

6.8 Анализ уязвимости должен содержать:

– перечень возможных угроз террористического характера конкретному объекту с учетом статистических данных о террористической активности в данном субъекте Российской Федерации (административно-территориальной единице);

– описание модели угроз и модели нарушителя;

– результаты математического моделирования вероятных сценариев возникновения и развития кризисных ситуаций и оценка возможных последствий;

– перечень критически важных элементов и меры по их защите;

– выводы о достаточности или недостаточности требований для обеспечения антитеррористической защищенности объекта, установленных нормативными документами, либо необходимости отступления от требований.

6.9 Материалы анализа уязвимости объекта согласно [7] являются сведениям, к которым устанавливается ограниченный доступ.

6.10 Результаты анализа уязвимости конкретного объекта могут быть согласованы с органом, полномочия которого устанавливаются органами исполнительной власти субъекта Российской Федерации.

6.11 Для объектов класса В.1.1, В.1.2, В.1.3 и В.2 анализ уязвимости объекта может быть как индивидуальным, так и типовым – для индивидуальных проектов для повторного применения.

6.12 Анализ уязвимости объекта угрозам террористического характера для объектов класса В.3, С.1, С.2 не требуется.

7 Требования к планировочной организации земельного участка, отводимого под объект в части обеспечения его антитеррористической защищенности

7.1 На территории объекта должны быть предусмотрены места (площадки, проходы и т.п.), обеспечивающие беспрепятственное и безопасное рассредоточение эвакуирующихся людей.

7.2 Земельные участки, отводимые под объект, должны планироваться с учетом доступности зданий и сооружений для маломобильных групп населения.

7.3 На въездах/выездах на подземную автостоянку объекта должны быть предусмотрены пункты контроля транспорта для исключения провоза террористических средств, проезда транспортных средств, не имеющих права проезда, и несанкционированного прохода.

7.4 Все парковочные площадки рекомендуется располагать на границе внешнего периметра территории объекта с целью минимизации возможных последствий реализации террористического акта.

8 Общие требования к архитектурным, конструктивным решениям объекта в части обеспечения антитеррористической защищенности

8.1 Территория объекта должна быть оборудована инженерными средствами физической защиты для исключения несанкционированного подъезда (прорыва) транспортных средств к объекту (его уязвимым местам).

8.2 Въезды на территорию объекта должны быть оснащены средствами сниже-

ния скорости и/или УПУ. На отдельных участках территории должны быть установлены средства снижения скорости и/или УПУ. Места установки и типы средств определяются проектом.

8.3 В обоснованных случаях, в зависимости от классификации объекта, его назначения, территория может быть оборудована ограждением высотой не менее 2,5 м и КПП.

Ограждение рекомендуется выполнять в виде прямолинейных участков, с минимальным количеством изгибов и поворотов, ограничивающих наблюдение. К ограждению не должны примыкать какие-либо пристройки, кроме зданий, являющихся продолжением периметра.

Ограждение должно исключать случайный проход людей (животных), въезд транспорта и затруднять проникновение нарушителей на охраняемую территорию, минуя КПП, не должно иметь лазов, проломов и других повреждений, а также не запираемых дверей, ворот и калиток.

В местах въезда на огражденную территорию объекта должны устанавливаться ворота. Конструкция ворот должна обеспечивать их жесткую фиксацию в закрытом положении.

8.4 Объекты, помещения, пути движения, входы и т.д. должны быть спроектированы с учетом доступности зданий и сооружений для маломобильных групп населения.

8.5 Вестибюли входов должны быть спроектированы с учетом возможного размещения пропускных устройств и досмотрового оборудования, точек доступа.

8.6 При нормальном режиме эксплуатации (при отсутствии команды на эвакуацию) должен быть исключен несанкционированный доступ со стороны эвакуационных выходов (со стороны улицы) на эвакуационные лестницы надземной и подземной частей объекта.

8.7 Выбор мест размещения эвакуационных выходов из надземных частей объекта и его подземного объема должен быть спроектирован с учетом возможности беспрепятственного и безопасного рассредоточения эвакуирующихся людей.

8.8 Критически важные элементы объекта, коммуникации, воздухозаборы, узлы и оборудование, помещения и ниши, в которых располагаются элементы инженерно-технических систем безопасности и жизнеобеспечения, систем технических антитеррористической защищенности, в отношении которых акт незаконного вмешательства приведет к полному или частичному прекращению его функционирования и/или возникновению чрезвычайных ситуаций, должны быть оснащены инженерными средствами физической защиты и средствами контроля САТЗ во избежание несанкционированных воздействий на них.

8.9 Подземные и наземные коммуникации объекта, имеющие входы или выходы, через которые можно проникнуть на объект, должны быть оборудованы постоянными или съемными решетками, крышками, дверями с запорами.

8.10 Потенциально доступные для проникновения нарушителя окна, выходы вентиляционных коробов, воздухозаборы и др. могут быть оснащены инженерными средствами физической защиты.

8.11 При проведении расчета несущей конструктивной системы и ограждающих конструкций объектов класса А.1, А.2 и В.2 рекомендуется учитывать воздействия проектных нагрузок, вызываемых ударной взрывной волной, на критически важные элементы, определенные в результате проведения анализа уязвимости объекта угрозам террористического характера.

8.12 Конструкции окон, витражей и их крепление к несущим конструкциям

должны обеспечивать безопасность людей, находящихся в объекте, от поражения фрагментами перечисленных элементов.

8.13 На объектах класса А производственного и непроизводственного назначения должны быть предусмотрены служебные помещения:

– ЦПУ объекта (площадь уточняется при проектировании, конкретное размещение ЦПУ определяют при проектировании с учетом принятых проектных решений по организации взаимодействия с инженерными системами и системами противопожарной защиты и т.д.);

– диспетчерского пункта управления инженерными системами (возможность объединения с ЦПУ уточняется при проектировании);

– ЛПУ объекта (необходимость выделения служебных помещений для организации ЛПУ определяется при проектировании);

– постов охраны (состав и площадь помещений определяется при проектировании);

– личного состава службы безопасности (необходимость выделения служебных помещений определяется при проектировании);

– для автоматизированной СМНК в случае ее создания (места размещения измерительных пунктов определяются при проектировании, площадь определяется в зависимости от используемого оборудования);

– для СМИС (возможность объединения с ЦПУ уточняется при проектировании).

Необходимость организации и размещения других служебных помещений, используемых для решения задач антитеррористической защищенности, определяется в задании на проектирование.

8.14 Для объектов класса В.1 за исключением В.1.4 должны быть предусмотрены помещения:

– ПУ (необходимость выделения отдельных служебных помещений для организации ПУ и возможность объединения с постом охраны определяется заданием на проектирование);

– постов охраны (состав и площадь помещений определяется при проектировании).

8.15 Для объектов классов В.1.4, В.2, В.3 могут быть предусмотрены помещения постов охраны (консьержей) (состав и площадь помещений определяется заданием на проектирование).

8.16 Пункты управления и диспетчерские пункты управления должны быть защищены от несанкционированного проникновения.

8.17 Общие требования к инженерным сооружениям и средствам физической защиты представлены в приложении Б, минимально необходимые требования к инженерно-техническому оснащению объектов в зависимости от классификации представлены в табл.А.1.

9 Требования к зонированию объектов в части обеспечения их антитеррористической защищенности

9.1 Объект с учетом архитектурных решений и функционального назначения помещений здания (сооружения) и территории должен быть разделен на зоны общего и ограниченного доступа.

9.2 При проектировании должен быть определен перечень контролируемых зон общего и ограниченного доступа с учетом режима работы, функционального назначения каждого из блоков, помещений или групп помещений объекта.

9.3 На входе/выходе (въезде/выезде) в зоны ограниченного доступа должен быть организован пропускной режим.

9.4 В состав зон ограниченного доступа могут быть включены:

- помещения инженерно-технического назначения;
- загрузочная зона (зона загрузки помещений общественного назначения);
- места стоянки (отстоя) транспортных средств;
- кровля объекта;
- помещения служб обеспечения безопасности и управления объектом;
- жилая зона;
- гостиничная зона;
- офисная зона;
- зона эвакуационных путей;
- иные зоны, доступ в которые разрешен только физическим лицам (транспорту) определенных категорий в соответствии с установленным пропускным режимом.

9.5 Минимально необходимые требования к оснащению функциональных элементов различных зон доступа средствами антитеррористической защищенности в зависимости от классификации объектов представлены в таблице А.2.

10 Требования к техническим системам антитеррористической защищенности объектов

10.1 К техническим системам антитеррористической защищенности объектов могут относиться следующие:

- контроля и управления доступом;
- охранной и тревожной сигнализации;
- охранного телевидения;
- охранного освещения;
- выявления диверсионно-террористических средств;
- контроля воздушно-газовой среды в системах вентиляции и кондиционирования;
- мониторинга инженерно-технического обеспечения;
- мониторинга технического состояния несущих конструкций;
- программно-технического обеспечения САТЗ;
- информационной безопасности;
- экстренной связи;
- оперативной связи;
- электропитания;
- иные системы.

10.2 Технические системы антитеррористической защищенности должны обеспечивать необходимую функциональную и аппаратную надежность, пожарную безопасность, помехоустойчивость.

В системах должны использоваться аппаратные средства, которые сертифицированы по безопасности, а также имеют сертификат, подтверждающий основные технические характеристики.

10.3 Перечень систем и средств, составляющих САТЗ, может быть изменен, уменьшен, дополнен при необходимости другими средствами и системами для повышения антитеррористической защищенности охраняемого объекта.

10.4 Для обеспечения эффективной работы системы и средства могут быть объединены в интегрированный комплекс систем технических антитеррористической защищенности.

В случае отсутствия целесообразности объединения отдельных систем в комплекс допускается самостоятельное развертывание указанных систем, однако в этом случае интеграция, с целью повышения эффективности охраны объекта, должна быть компенсирована организационными мерами.

10.5 Для обеспечения антитеррористической защищенности объекта могут быть применены системы технические антитеррористической защищенности совместно с другими системами (средствами) обеспечения безопасности (пожарной, автоматизации и диспетчеризации технологического оборудования и т.п.) В этом случае функции совместно действующих систем должны дополнять друг друга, не оказывая взаимного мешающего влияния на работоспособность составных частей. В совместно действующих системах должны обеспечиваться: алгоритмическая совместимость и раздельная регистрация поступающих от них служебных и тревожных сигналов. Условия совместного применения систем должны быть оговорены в техническом задании на проектирование и в эксплуатационной документации.

10.6 Технические средства управления и контроля функционирования совместно действующих систем определяются их целевым назначением. Предпочтительны автоматические средства управления и контроля, но как дублирующие допускаются и ручные. Целесообразность дублирования определяется требованиями обеспечения эксплуатационной надежности систем. Средства управления и контроля должны иметь защиту от возможных ошибочных действий персонала. Предпочтение следует отдавать системам и комплексам, аппаратные средства и программное обеспечение которых взаимосвязаны, и отлажены заводом-изготовителем.

10.7 Требования к основным техническим системам антитеррористической защищенности изложены в приложении В и нормативных документах [1, 8, 9, 10].

11 Требования к обеспечению антитеррористической защищенности объектов в процессе эксплуатации

Антитеррористическая защищенность объекта в процессе эксплуатации должна быть обеспечена посредством технического обслуживания, периодических осмотров и контрольных проверок и (или) мониторинга состояния компонентов САТЗ объекта, а также посредством текущих ремонтов оборудования.

Параметры и другие характеристики САТЗ объекта в процессе эксплуатации должны соответствовать требованиям проектной документации и документации нормативно-технического сопровождения обеспечения антитеррористической защищенности объектов в течение всего срока эксплуатации. Указанное соответствие должно поддерживаться согласно статьи 40 [2].

Приложение А
(рекомендуемое)

Инженерно-техническое оснащение различных зон доступа

Таблица А.1 – Требования к инженерно-техническому оснащению объектов в зависимости от классификации

Класс	Подкласс	Зоны	ПУ	Ограждение/малые арх.формы	Посты охраны/точки доступа	СОТС	СКУД/домофон	СОТ/СОО	СВДТС	СМИС	СМНК	СКВГС	СИБ	СОС	СЭС
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
А.1	А.1.1		Требования устанавливаются ведомственными нормативными документами и дополнительными условиями федеральных органов исполнительной власти												
	А.1.2														
	А.1.3														
	А.1.4														
	А.1.5														
	А.1.6														
	А.1.7														
	А.1.8														
	А.1.9														
	А.1.10														
	А.1.11														
	А.1.12	Ограниченного доступа	+	+/*	*/+	+	+/-	+/+	+	+	+	*	-	+	-
А.2	А.2.1	Общего доступа	+	*/+	*/+	-	-	+/+	*	+	+	*	-	+	*
		Ограниченного доступа		*/+	*/+	+	*/*	+/+				*	*		*
	А.2.2	Общего доступа	+	*/+	*/+	-	-	+/+	*	+	+	*	-	+	*
		Ограниченного доступа		*/+	*/+	+	*/*	+/+				*	*		*
	А.2.3	Общего доступа	+	*/+	*/+	-	-	+/+	*	+	+	*	-	+	*
		Ограниченного доступа		*/+	*/+	+	*/*	+/+				*	*		*
	А.2.4	Общего доступа	+	*/+	*/+	-	-	+/+	*	+	+	*	-	+	*
		Ограниченного доступа		*/+	*/+	+	*/*	+/+				*	*		*
	А.2.5	Общего доступа	+	*/+	*/+	-	-	+/+	*	+	+	*	-	+	*
		Ограниченного доступа, в том числе:		*/+	*/+	*	*/*	+/+	*			*	-		*
		Помещения с единовременным нахождением более 50 чел.		*/+	+/*	*	*/-	+/+	+			*	*		*
		вход в жилую зону		*/+	-/*	-	-/+	+/+	-			*	-		+

Окончание таблицы А.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
В.1	В.1.1	Общего доступа	+	+/	*/-	-	-	+/+	+	*	-	*	-	+	*
		Ограниченного доступа		+/	+/+	+	+/-	+/+	+			*	*	+	*
	В.1.2	Общего доступа	+	*/+	*/-	-	-	+/+	+	*	-	*	-	+	*
		Ограниченного доступа		*/+	+/+	+	+/-	+/+	+			*	*	+	*
	В.1.3	Общего доступа	+	*/+	*/-	-	-	+/+	+	*	-	*	-	+	*
		Ограниченного доступа		*/+	+/+	+	+/-	+/+	+			*	*	+	*
	В.1.4	Общего доступа	*	*/+	*/*	*	*/*	*/*	+	*	-	-	-	*	*
		Ограниченного доступа		*/+	*/*	*	*/*	*/*	+			*	*	*	*
В.2	В.2.1	Общего доступа	*	+/*	+/+	+	-	+/+	+	*	-	*	-	*	*
		Ограниченного доступа		+/*	+/+	+	+/*	+/+	+			*	*	*	*
	В.2.2	Общего доступа	*	*/+	*/+	+	-	+/+	+	*	*	*	*	*	*
		Ограниченного доступа		*/+	*/+	+	+/*	+/+	+			*	*	*	*
	В.2.3	Общего доступа	*	*/+	*/+	+	-	+/+	+	*	-	*	-	*	*
		Ограниченного доступа		*/+	*/+	+	+/*	+/+	+			*	*	*	*
	В.2.4	Общего доступа	*	*/+	*/+	+	-	+/+	+	*	-	*	-	*	*
		Ограниченного доступа		*/+	*/+	+	+/*	+/+	+			*	*	*	*
	В.2.5	Общего доступа	*	*/+	*/+	+	-	+/+	+	*	-	*	-	*	*
		Ограниченного доступа, в том числе:		*/+	*/+	+	*/+	+/+	*			*	-	*	*
		Помещения с единовременным нахождением более 50 чел.		*/+	+/*	+	+/*	+/+	+			*	*	*	*
		вход в жилую зону		*/+	-/*	*	-/+	+/*	-			*	-	*	+
В.3	В.3.1	Общего доступа	*	+/*	*/-	-	-	*/*	*	-	-	-	-	*	*
		Ограниченного доступа		+/*	*/*	*	*/*	*/*	*			-	*	*	-
	В.3.2	Общего доступа	*	-/+	-/-	-	-	*/*	*	-	-	-	-	*	*
		Ограниченного доступа		-/+	-/*	*	*/*	*/*	*			-	*	*	-
	В.3.3	Общего доступа	*	-/+	-/-	-	-	*/*	*	-	-	-	-	*	*
		Ограниченного доступа		-/+	-/*	*	*/*	*/*	*			-	*	*	-
	В.3.4	Общего доступа	*	-/+	-/-	-	-	*/*	*	-	-	-	-	*	*
		Ограниченного доступа		-/+	-/*	*	*/*	*/*	*			-	*	*	-
	В.3.5	Общего доступа	*	-/*	-/-	-	-	*/*	*	-	-	-	-	*	+
		Ограниченного доступа		-/*	-/*	*	*/*	*/*	-			-	*	*	-
		вход в жилую зону		-/*	-/*	*	-/*	+/*	-			-	-	*	+
С	Требования, при необходимости, устанавливаются ведомственными нормативными документами														

Примечание:

«+» - обязательное применение;

«*» - рекомендуемое применение;

«-» - необязательное применение.

Таблица А.2 – Требования к оснащению функциональных элементов различных зон доступа средствами антитеррористической защиты в зависимости от классификации объектов

класс	Зоны	СОТС/тревожная сигнализация	СКУД/домофон	СОТ	СВДТС									СОС	СЭС	Камеры хранения	Противотаранные устройства
					МОб	РТУ/ ПРТУ	РМ	МИ	ГАПВВ	ЛВУ	РП	ДРК	СрВД				
1	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
А	Входные группы в зоны общего доступа	-/+	-/-	+	+	*/-	+	*	-	*	*	-	+	+	-	+	-
	Входные группы в зоны ограниченного доступа (за исключением жилой)	-/+	+/*	+	+	*/-	+	*	-	*	*	-	+	+	-	+	-
	Входные группы в жилую зону	-/+	*/+	+	-	-	*	*	-	*	*	-	+	+	+	-	-
	Въездные группы	-/+	+/-	+	-	-	+	*	-	*	*	*	+	+	+	-	+
	Приема почтовой корреспонденции	-/+	-/*	+	-	*	+	*	-	*	*	-	+	+	-	+	-
	Территория	*/-	-/-	*	-	-	-	-	-	-	-	-	-	-	*	-	-
	Оснащение резервных групп	-/*	-/-	-	-	-/*	+	+	*	+	*	-	*	-	-	-	-
В	Входные группы в зоны общего доступа	-/*	-/-	+	*	*/-	+	*	-	*	*	-	*	+	-	+	-
	Входные группы в зоны ограниченного доступа (за исключением жилой)	-/*	+/*	+	*	*/-	+	*	-	*	*	-	+	+	-	+	-
	Входные группы в жилую зону	-	*/*	+	-	-	-	-	-	-	-	-	-	-	*	-	-
	Въездные группы	-/*	*/-	+	-	-	-	*	-	*	*	*	+	+	*	-	+
	Приема почтовой корреспонденции	-/*	-/*	*	-	*	*	*	-	-	-	-	*	+	-	*	-
	Территория	-	-/-	*	-	-	-	-	-	-	-	-	-	-	*	-	-
В	Оснащение резервных групп служб безопасности	-/*	-/-	-	-	-/*	+	+	*	+	*	-	*	-	-	-	-
С		-	-	*	-	-	-	-	-	-	-	-	-	-	*	-	-

Примечание:
«+» - обязательное применение;
«*» - рекомендуемое применение;
«-» - необязательное применение.

Приложение Б

(рекомендуемое)

Общие требования к инженерным сооружениям и средствам физической защиты

Б.1 Инженерные сооружения и средства физической защиты объекта предназначены для:

– защиты людей и самого объекта путем создания физической преграды 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.

К инженерным сооружениям и средствам физической защиты 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 техническом задании на проектирование САТЗ объекта с учетом требований нормативных документов.

Б.2 Большинство средств строятся на основе физических барьеров, которые по функциональному признаку подразделяют на постоянные 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.

Б.3 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, устройства снижения скорости движения автотранспорта и другие физические препятствия.

К переносным средствам физической защиты инженерным относятся:

– противотаранные упоры;

– мобильные средства для принудительной остановки транспорта;

– тормозные башмаки и зажимы-укосины.

Б.4 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.

Б.5 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 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 сетчатого ограждения;

– из металлических прутьев диаметром не менее 12 мм.

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.

При необходимости (оговаривается в техническом задании на проектирование) возможные подъезды автомобильного транспорта к полотну основного ограждения (помимо ворот) оборудуются устройствами снижения скорости движения транспортных средств либо противотаранными устройствами.

Дополнительное ограждение устанавливается для затруднения преодоления нарушителем основного ограждения.

Ворота устанавливают на автомобильных въездах на территорию объекта. По периметру территории охраняемого объекта могут быть установлены основные и запасные ворота.

Б.6 В зависимости от функционального назначения на объекте могут быть организованы КПП для:

- прохода персонала объекта и посетителей;
- проезда автомобильного транспорта.

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.

Транспортные КПП оборудуются досмотровыми площадками, количество которых определяется интенсивностью движения автомобильного транспорта через КПП, контрольно-пропускными кабинами или турникетами для пропуска водителей и лиц, сопровождающих грузы, а также противотаранными устройствами.

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.

Б.7 Двери объекта и его помещений должны быть исправными, хорошо подогнанными под дверные коробки.

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

Оконные конструкции (окно, форточка, фрамуга) в помещении охраняемого объекта должны быть остеклены, иметь надежные и исправные запирающие устройства. Оконные стекла должны быть жестко закреплены в пазах.

Оконные конструкции должны обеспечивать надежную защиту помещения объекта.

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

Б.8 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.

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.

Приложение В

(рекомендуемое)

Требования к основным системам техническим антитеррористической защищенности

В.1 Требования к системе контроля и управления доступом

В.1.1 Система должна обеспечивать решение следующих задач:

– контролируемый доступ людей и транспортных средств на территорию объекта и в зоны ограниченного доступа;

– контроль перемещения людей и транспортных средств внутри объекта;

– разграничение доступа в соответствии с зонированием объекта;

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

– оперативную инвентаризацию оборудования, установленного в выделенных помещениях и оснащенного чипами с электронной меткой;

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

– взаимодействие с другими системами на аппаратном и программном уровнях;

– разблокировку на выход дверей и заграждений при пожаре.

Система должна обеспечивать:

– регистрацию, выдачу и аннулирование электронных меток;

– программирование зон доступа для каждого владельца;

– регистрацию входов, выходов и попыток несанкционированного проникновения;

– дистанционное перепрограммирование кодовых замков;

– хранение и документирование информации;

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

Средствами контроля доступа должны быть оборудованы все входы/выходы (въезды/выезды) в зоны ограниченного доступа объекта.

Система контроля и управления доступом должна включать:

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

– 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.

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 транспорт-

ных средств в зону безопасности является транспортный КПП.

Подсистема контроля и управления доступом посетителей должна обеспечивать:

– идентификацию прибывающих лиц;

– установление действительности представленных оснований для прохода в зону безопасности.

Подсистема контроля и управления доступом обслуживающего персонала должна обеспечивать:

– идентификацию прибывающих лиц;

– установление действительности представленных оснований для прохода в зону безопасности.

Подсистема контроля и управления доступом пользователей объектом должна обеспечивать установление действительности представленных оснований для прохода в зону ограниченного доступа.

В жилой зоне доступа объекта двери подъездов должны быть оборудованы домофонами (должны быть установлены вызывные и/или кодонаборные панели).

В.1.2 Нормативные документы рекомендуемые для применения:

ГОСТ Р 51241, ГОСТ Р 52551, [9].

В.2 Требования к системе охранной и тревожной сигнализации

В.2.1 Система охранно-тревожной сигнализации включает:

– подсистему охранной сигнализации;

– подсистему тревожной сигнализации.

Подсистема охранной сигнализации должна обеспечивать:

– оповещение несанкционированном доступом на территорию объекта, 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.

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 инженерных систем и систем жизнеобеспечения объекта;

– все внешние двери и ворота здания объекта;

– двери технических этажей;

– колодцы, люки, лазы, шахты коммуникаций сечением 250х250 мм и более;

– отдельные объекты внутри помещений (сейфы, шкафы, ниши) по необходимости.

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

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 ситуа-

ции.

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.

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 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 снятие/постановки под охрану.

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

В.2.2 Нормативные документы рекомендуемые для применения:

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

В.3 Требования к системе охранного телевидения

В.3.1 Система охранного телевидения предназначена для осуществления непрерывного наблюдения за обстановкой в контролируемых зонах внутри объекта, прилегающей территории и подъездных путях.

Система должна выполнять как охранные функции, так и обеспечения необходимой видеоинформацией соответствующие службы для оценки тревожной ситуации, возникшей в зонах наблюдения и принятия управляющих решений обеспечивающих

пресечение противоправных действий.

Система должна обеспечивать:

– осуществление непрерывного, круглосуточного контроля границ зон доступа и территории объекта с фиксированием лиц, пересекающих зоны и транспортных средств;

– постоянное наблюдение за критически важными элементами, служебными и техническими помещениями, а также прилегающей территорией объекта и подъездными путями с целью раннего обнаружения противоправных действий и координации сил обеспечения безопасности;

– видеоаналитический анализ полученной информации и активный видеоконтроль (реагирование СОТ на нестандартное поведение людей в автоматическом режиме);

– выделение из общей видеокартины и фиксирование лиц нарушителей с целью 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 том числе и при ограничении полномочий доступа к архиву;

– архивирование информации от телевизионных камер с разграничением полномочий доступа к ней.

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

Система должна включать:

– подсистему охранного телевидения;

– подсистему видеонаблюдения.

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 охранной сигнализации, условные сообщения и др.

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

Получаемая СОТ видеоинформация анализируется операторами. В случае обнаружения признаков реализации угроз видеоинформация представляется 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).

В.3.2 Технические требования к средствам СОТ

В.3.2.1 Изображения, получаемые при помощи СОТ, должны отображать мак-

симально возможное число признаков, идентифицирующих объекты.

В.3.2.2 Для подсистем, решающих задачи фиксации видеоизображения, минимально допустимый размер объекта в кадре должен составлять не менее 240 пикселей по горизонтали. При фиксации лица человека – межзрачковое расстояние должно составлять не менее 120 пикселей.

В.3.2.3 В СОТ с цифровым видеонакопителем должна применяться прогрессивная строчная развертка, аппаратно обеспечиваться получение кадра на выходе системы не ниже 720×576 пикселей.

В.3.2.4 Для цветного изображения цветовая насыщенность 24-битного изображения должна быть таковой, чтобы при его преобразовании к изображению в градациях серого, динамический диапазон интенсивности кодировался, по крайней мере 7-8 бит.

В.3.2.5 Структура дискретизации цифрового сигнала цветного изображения YUV (4:2:2).

В.3.2.6 Для черно-белого изображения динамический диапазон интенсивности изображения должен кодироваться по крайней мере 8 бит (составлять не менее 256 значений).

В.3.2.7 Режим записи должен быть 25 кадров в секунду (по каждому каналу при максимальном качестве видеоданных).

В.3.2.8 Применение алгоритмов цифровой обработки с межкадровым сжатием не допускается.

В.3.2.9 Видеокамеры (телекамеры) СОТ необходимо устанавливать максимально близко к горизонтальной визирной линии по отношению к фиксируемому объекту.

В.3.2.10 Значение разрешения СОТ должно составлять не менее 450 ТВЛ для цветных камер.

В.3.2.11 Значение разрешения СОТ должно составлять не менее 500 ТВЛ для черно-белых камер.

В.3.2.12 Светочувствительность камер не более 0,1 лк.

В.3.2.13 Разрешающая способность объектива – не хуже 40 (пар линий)/мм.

В.3.3 Нормативные документы, рекомендуемые для применения:

ГОСТ Р 51558, [1], [10].

В.4 Требования к системе охранного освещения

В.4.1 Система охранного освещения должна обеспечивать необходимые условия видимости на ограждении территории, периметра объекта.

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 шириной 3-4 м;
- 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 объ-

екта;

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

В темное время суток, если освещенность охраняемой зоны ниже чувствительности видеокамер, объект (зона объекта) должен оборудоваться охранным освещением видимого диапазона. Зоны охранного освещения должны совпадать с зоной обзора видеокамеры. При использовании СОТ цветного изображения применение инфракрасного освещения недопустимо.

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

Лампы охранного освещения должны быть защищены от механических повреждений.

В.4.2 Нормативные документы рекомендуемые для применения:

ГОСТ Р 51558, СП 52.13330, [1], [10].

В.5 Требования к системе выявления диверсионно-террористических средств

В.5.1 Требования к перечню оборудования СВДТС

Система выявления диверсионно-террористических средств – это совокупность средств, обладающих технической, информационной, программной и эксплуатационной совместимостью, позволяющих выявлять и локализовать террористические средства.

Система выявления диверсионно-террористических средств должна обеспечивать:

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

– обнаружение террористических средств, скрытно проносимых на человеке и в его ручной клади, почтовой корреспонденции, перевозимых на транспортном средстве.

Система выявления диверсионно-террористических средств должна быть интегрирована в общую САТЗ объектов.

Система выявления диверсионно-террористических средств на входных группах в зависимости от класса здания (сооружения), анализа уязвимости здания (сооружения) может состоять из минимально необходимого ряда технических средств обнаружения, в том числе:

– ручного металлоискателя;
– металлообнаружителя стационарного;
– стационарного радиационного монитора;
– переносной рентгенотелевизионной установки;
– стационарной рентгеновской установки;
– рентгенотелевизионного интроскопа конвейерного типа;
– средств выявления диверсионно-террористических средств на человеке и /или в ручной клади, почтовой корреспонденции, основанных на альтернативных принципах;
– газоанализатора паров взрывчатых веществ;
– поста управления на базе персонального компьютера.

Состав оборудования и необходимость его использования должен уточняться при проектировании на основании анализа уязвимости конкретного объекта.

Система выявления диверсионно-террористических средств должна 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, установленные на входных группах.

При высоком потоке посетителей входящая почтовая корреспонденция должна поступать на отдельный пост.

Стационарный радиационный монитор (пороговый сигнализатор ионизирующего излучения, гамма-спектрометр-радиометр) является обязательным элементом системы.

Для обеспечения безопасности людей на объектах должны находиться в готовности к применению средства локализации взрыва.

К данным средствам допускается отнести:

- стационарный (носимый) передатчик помех;
- 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.

Кроме того в оснащение групп быстрого реагирования (при их наличии) возможно включить портативный ГАПВВ.

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;
- стационарных автоматизированных видеосистем сканирования днища транспортных средств;
- средств визуального досмотра транспортных средств.

Состав оборудования и необходимость его использования должен уточняться при проектировании на основании анализа уязвимости конкретного объекта.

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

В.5.2 Нормативные документы рекомендуемые для применения:

ГОСТ 51635, ГОСТ Р 53705.

В.6 Требования к системе контроля воздушно-газовой среды в системах вентиляции и кондиционирования

Системы контроля воздушно-газовой среды в системах вентиляции и кондиционирования должна обеспечивать обнаружение отравляющих и других опасных веществ, горючих и токсичных газов, перечень которых должен уточняться в техническом задании, на основании требований, предъявляемых федеральными органами 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.

В.7 Требования к системе мониторинга технического состояния несущих конструкций

Система мониторинга технического состояния несущих конструкций (автоматизированная) должна предусматривать возможность обнаружения несанкционированного изменения несущих конструкций.

Проектирование и создание СМНК осуществляется в соответствии с ГОСТ Р 53778.

В.8 Требования к системе мониторинга инженерно-технического обеспечения

Система мониторинга инженерно-технического обеспечения должна обеспечивать контроль работоспособности инженерных систем и возникновения угроз нарушения нормальной эксплуатации объекта.

Система мониторинга инженерно-технического обеспечения должна обеспечивать контроль способности системы обеспечения АТЗ здания (сооружения) противодействовать угрозам, в том числе террористического характера.

Проектирование и создание СМИС осуществляется в соответствии с ГОСТ Р 53778.

В.9 Требования к программно-техническому обеспечению антитеррористической защищенности зданий и сооружений

Программно-техническое обеспечение САТЗ должно выполнять следующие задачи:

– интеграцию комплекса инженерно-технического обеспечения зданий и сооружений в части обеспечения их антитеррористической защищенности для осуществления информационного обмена между различными субъектами и системами обеспечения безопасности;

– выявление и прогноз развития негативных факторов, угрожающих безопасности здания;

– поддержку принятия решений при обнаружении негативных факторов, угрожающих безопасности здания и формирование рекомендаций по их локализации и устранению;

– информирование операторов службы безопасности о выявлении нештатных ситуаций с указанием необходимых действий оператора службы безопасности, предусмотренных регламентом работы службы безопасности.

– контроль действий оператора службы безопасности и его действий при возникновении нештатных ситуаций

Программно-техническое обеспечение САТЗ включает в себя информационное, математическое и программное обеспечение.

Информационное обеспечение должно включать электронное описание проектных решений и технических характеристик объекта, включая поэтажные планы и разрезы, систем инженерно-технического обеспечения, включая схемы их расположения.

Математическое обеспечение должно включать формализованные правила выявления негативных факторов, результаты математического моделирования оценки их последствий.

Программное обеспечение должно осуществлять вывод информации на автоматизированное рабочее место оператора службы безопасности с возможностью визуализации на трехмерной интерактивной модели объекта.

В.10 Требования к обеспечивающим системам

В.10.1 Требования к оперативной связи

Система оперативной связи должна обеспечивать организацию обмена речевой информацией между персоналом службы безопасности в целях обеспечения скоординированных действий по охране объекта в штатных и чрезвычайных ситуациях.

Система оперативной связи должна обеспечивать:

– надежную и непрерывную работу на всей территории объекта и на ближних подступах к нему, во всех его сооружениях и помещениях и во всех допустимых режимах работы;

– учет и протоколирование всех проводимых переговоров с указанием времени и их продолжительности;

– организацию каналов связи с территориальными органами исполнительной власти.

Система оперативной связи должна включать прямую громкоговорящую, телефонную, сотовую и радиосвязь между постами службы безопасности (нарядами охраны), помещениями пунктов управления, и другими объектами защиты.

Прямая телефонная связь должна обеспечивать:

– телефонную связь оператора центрального пункта управления объекта с ответственным дежурным службы безопасности, с локальными пунктами управления, с пропускными пунктами, с постами охраны, а также со службами (подразделениями) объекта и его администрацией;

– телефонную связь ответственного дежурного службы безопасности с постами охраны;

– прямая телефонная связь оператора центрального пункта управления, ответственного дежурного службы безопасности должна быть автономной и обеспечивать возможность циркулярной связи с абонентами (постами охраны).

Радиосвязь должна обеспечивать устойчивую связь ответственного дежурного

службы безопасности с подвижными нарядами в условиях выполнения ими оперативных задач. В системе радиосвязи следует предусматривать как мобильные, так и стационарные переговорные устройства.

В.10.2 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 проек-

тируемого 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

В.10.3 Система электропитания

Все электроприемники технических средств САТЗ по степени надежности электроснабжения должны быть отнесены к первой категории.

Переход на резервное питание должен производиться автоматически.

Факт перехода комплекса или его элементов на резервное питание должен выводиться на центральный пункт управления с обязательной регистрацией.

Устройства электропитания и кабельное хозяйство основных элементов САТЗ должны быть защищены от несанкционированных действий.

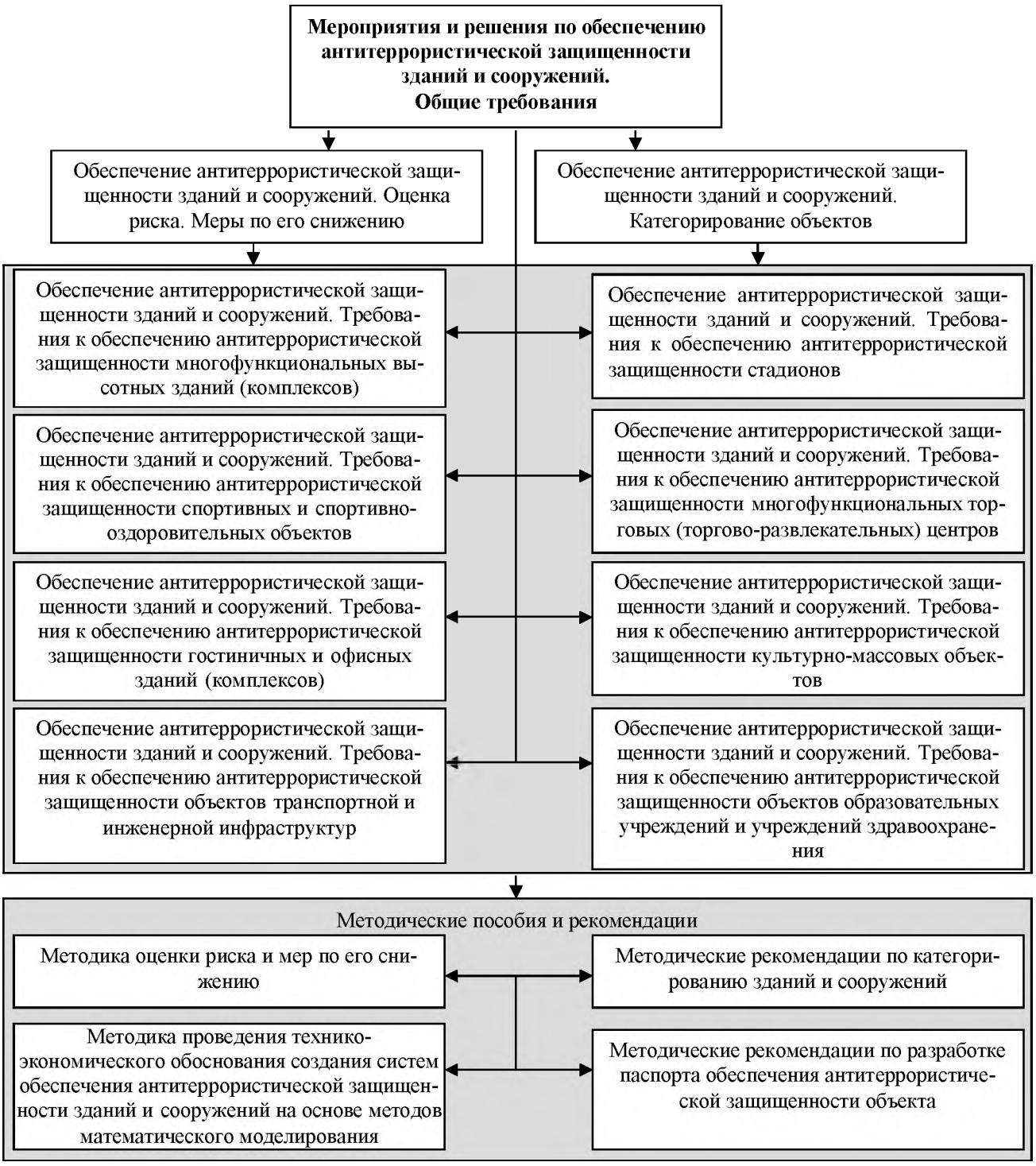
Устройства электропитания (выпрямительные устройства и групповые токораспределительные щиты) должны быть установлены в специально оборудованных помещениях с ограниченным доступом.

Защитное заземление и обнуление технических средств системы обеспечения антитеррористической защищенности должно быть выполнено в соответствии с требованиями и технической документацией на эти средства.

Приложение Г

(справочное)

Структура комплекса нормативной документации «Обеспечение антитеррористической защищенности зданий и сооружений



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] Федеральный закон от 29.12.2004 г. № 190-ФЗ «Градостроительный Кодекс Российской Федерации»;
[4] Федеральный закон от 21.07.1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»;
[5] Постановление Правительства Российской Федерации от 15.02.2011 г. № 73 «О некоторых мерах по совершенствованию подготовки проектной документации в части противодействия террористическим актам»;
[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] РД 78.36.006-2005 Выбор и применение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрепленности для оборудования объектов;
[9] Р 78.36.005-2011 Выбор и применение систем контроля и управления доступом. Рекомендации;
[10] Р 78.36.002-2010 Выбор и применение систем охранных телевизионных. Рекомендации.

ОКС 13.310. 91.120.99 ОКУН 0163130

Ключевые слова: антитеррористическая защищенность, безопасность, здание, обеспечение антитеррористической защищенности, обнаружение, объект капитального строительства, сооружение

Прошито, пронумеровано и скреплено печатью 10 (десять) листов.

Генеральный директор
НП "АПЦ"
Ильичев В.А.