КОМПЛЕКС ГРАДОСТРОИТЕЛЬНОЙ ПОЛИТИКИ И СТРОИТЕЛЬСТВА ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МОСКОВСКОГО СТРОИТЕЛЬСТВА
ГУП «НИИМосстрой»

ТЕХНИЧЕСКИЕ РЕКОМЕНДАЦИИ

по проектированию систем антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий

ТР 205-09

Москва 2009

ДЕПАРТАМЕНТ ГРАДОСТРОИТЕЛЬНОЙ ПОЛИТИКИ,
РАЗВИТИЯ И РЕКОНСТРУКЦИИ ГОРОДА МОСКВЫ

ГУП «НИИМосстрой»

ТЕХНИЧЕСКИЕ РЕКОМЕНДАЦИИ

по проектированию систем антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий

ТР 205-09

Утверждены директором ГУП «НИИМосстрой»
март 2009 г.

Москва 2009

Настоящие технические рекомендации разработаны в соответствии с планом научно-исследовательских и опытно-конструкторских работ на 2007г., утвержденным Департаментом градостроительной политики, развития и реконструкции г. Москвы.

Настоящие Рекомендации предназначены для специалистов, выполняющих работы по проектированию систем комплексного обеспечения безопасности и антитеррористической защищенности высотных и уникальных зданий.

Рекомендации содержат основные требования к разработке общих технических требований по антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий.

Рекомендации направлены на унификацию основных требований, предъявляемых к разработке технических требований по антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий.

Рекомендации разработаны: ГУП «НИИМосстрой» (В.Ф. Коровяков, д-р техн. наук – руководитель работ, В.А. Устюгов, канд. техн. наук, В.Г. Петров, М.В. Фирсов, канд. техн. наук, А.М. Шахраманьян, канд. техн. наук, А.К. Маилянц, И.Е. Штунцайгер, М.В. Сидорко, В.М. Сорока, научный сотрудник,

Е.В. Ларионова), Университет КСБ и ИО (Г.Г. Соломанидин, д-р техн. наук, О.М. Любимова, канд. техн. наук, Е.Е. Соколов, канд. техн. наук, И.В. Нестругина).

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ ... 4
2 НОРМАТИВНЫЕ ССЫЛКИ ... 4
3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ... 4
4 ОБЩИЕ ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ СИСТЕМЫ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ... 7
5 ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СИСТЕМЫ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ... 8
6 ТРЕБОВАНИЯ К ПРОЕКТНЫМ РЕШЕНИЯМ ... 10
6.1 Требования к генеральному плану ... 10
6.2 Требования к архитектурным, объемно-планировочным решениям и функциональным элементам ... 10
6.3 Требования к составу служебных помещений ... 10
6.4 Требования к защите конструктивных элементов ... 11
7 ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВХОДА/ВЫХОДА В ВЫДЕЛЕННЫЕ ЗОНЫ ДОСТУПА ... 12
8 ТРЕБОВАНИЯ К СТРУКТУРНЫМ КОМПОНЕНТАМ И ЭЛЕМЕНТАМ ТЕХНИЧЕСКИХ СРЕДСТВ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ... 13
9 ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМАМ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ... 14
9.1 Общие положения ... 14
9.2 Система охранной сигнализации ... 14
9.3 Средства тревожно-вызывной сигнализации ... 15
9.4 Система контроля и управления доступом ... 15
9.4.1 Требования к пропускам ... 17
9.5 Средства локализации взрывных устройств ... 17
9.6 Досмотровые средства ... 17
9.7 Система телевизионного наблюдения (охранного телевидения) ... 17
9.7.1 Требования к размещению телекамер ... 18
9.7.2 Требования к постам наблюдения ... 19
9.8 Система управления эвакуацией людей при возникновении чрезвычайных ситуаций (СУЭВ) ... 19
9.9 Система мониторинга несущих конструкций ... 20
9.10 Система мониторинга инженерных систем (СМИС) ... 22
9.11 Системы контроля воздушно-газовой среды в системах вентиляции и кондиционирования ... 23
9.12 Требования к обеспечивающим системам ... 23
9.12.1 Требования к оперативной связи ... 23
9.12.2 Требования к системе телекоммуникаций ... 24
9.12.3 Подсистема электропитания ... 25
9.12.4 Подсистема защиты информации ... 24
9.12.5 Подсистема охранного освещения ... 25
9.12.6 Подсистема эвакуационного освещения ... 26
10 ОБОРУДОВАНИЕ ЦЕНТРАЛЬНОГО ПУНКТА УПРАВЛЕНИЯ СИСТЕМОЙ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ... 26
Приложение А ... 28

Департамент градостроительной политики, развития и реконструкции города Москвы	ТЕХНИЧЕСКИЕ РЕКОМЕНДАЦИИ по проектированию систем антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий	ТР 205-09 Вводятся впервые

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие рекомендации содержат основные положения, регламентирующие порядок проектирования систем комплексного обеспечения безопасности и антитеррористической защищенности высотных и уникальных зданий в городе Москве.

1.2 Выполнение положений настоящих рекомендаций направлено на реализацию единой политики в области комплексного обеспечения безопасности и антитеррористической защищенности высотных и уникальных зданий, обеспечение безопасности эксплуатирующихся высотных и уникальных зданий за счет качественного выполнения проектных и монтажных работ, использования сертифицированного оборудования.

1.3 Данные Рекомендации не отменяют и не заменяют обязательность выполнения нормативно-технических документов по обеспечению безопасности и надежности зданий и сооружений.

1.4 Общие технические требования разрабатывают специализированные организации по договорам с Заказчиком (Застройщиком). Объем работ определяется настоящими рекомендациями и нормативными документами организацией, осуществляющей разработку и согласованной с Заказчиком (Застройщиком) и проектной организацией. Финансирование этих работ должно быть предусмотрено в смете на строительство здания, а после введения его в эксплуатацию – в смете расходов на эксплуатацию и содержание здания. Разработка этих требований может проводиться как одной организацией, так и совместно несколькими.

1.5 Положения данных «Рекомендаций» могут быть изменены или отменены после выхода Технических регламентов в соответствии с Законом РФ № 184-ФЗ от 27 декабря 2002г. «О техническом регулировании».

2 НОРМАТИВНЫЕ ССЫЛКИ

Перечень нормативных и рекомендательных документов приведен в приложении А.

3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Настоящие технические рекомендации устанавливают термины и определения основных понятий в области антитеррористической защищенности и комплексной безопасности высотных и уникальных объектов г. Москвы.

Безопасность - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений. (Федеральный Закон «О техническом регулировании» от27.12 2002 № 184-ФЗ (в ред. ФЗ от 09.05.2005 N 45-ФЗ, от 01.05.2007 № 65-ФЗ)).

Безопасность уникальных и высотных объектов города Москвы - состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений, находящихся в уникальных, высотных объектах или в непосредственной близости от них, в результате реализации угроз. (Распоряжение Правительства Москвы от 27.06.2007 № 1305-РП «Об утверждении Концепции комплексного обеспечения безопасности уникальных и высотных объектов города Москвы»).

Внешний нарушитель - нарушитель из числа лиц, не имеющих права доступа в охраняемые зоны.

Внешняя угроза - угроза, исходящая от внешнего нарушителя.

Внутренний нарушитель - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны.

Время живучести системы - время сохранения работоспособности системы в заданных условиях воздействий при возникновении чрезвычайной ситуации.

Высота здания - расстояние от поверхности проезда для пожарных машин до нижней границы открывающегося проема (окна) в наружной стене верхнего (жилого, офисного) этажа (не считая верхнего технического этажа. (МГСН 4.19- 2005 Многофункциональные высотные здания и комплексы, СНиП 21-01-97 Пожарная безопасность зданий и сооружений, СНиП 31-01-2003 Здания жилые многоквартирные).

Высотное здание - здание высотой более 75 м. (МГСН 4.19-2005 Многофункциональные высотные здания и комплексы).

Высотный объект – высотное здание или уникальный высотный объект

Доступ - проход (проезд) в охраняемые зоны высотного объекта.

Живучесть технической системы при возникновении чрезвычайной ситуации - свойство системы сохранять свою работоспособность в течение гарантированного времени в заданных условиях воздействий, в том числе при возникновении чрезвычайной ситуации, которое должно быть обеспечено применением специальных мер, технических мероприятий и проектных решений.

Защищенность высотного объекта - совокупность организационно-технических мероприятий, направленных на обеспечение охраны объекта, зоны объекта (ГОСТ Р 50776-95).

Идентификатор доступа, идентификатор (носитель идентификационного признака) - уникальный признак субъекта или объекта доступа. В качестве идентификатора может использоваться запоминаемый код, биометрический признак или вещественный код. Идентификатор, использующий вещественный код - предмет, в который (на который) с помощью специальной технологии занесен идентификационный признак в виде кодовой информации (карты, электронные ключи, брелоки и т.д.) (ГОСТ Р 51241-98).

Комплекс инженерно-технических средств охраны - совокупность совместно действующих инженерно-технических средств охраны, установленных на охраняемом высотном объекте и объединенных системой инженерных сетей и коммуникаций.

Комплексное обеспечение безопасности - реализованное в проектных решениях согласованное взаимодействие инженерно-технических систем (средств) и персонала, задействованных в предотвращении несанкционированных действий, обеспечении безопасности людей при чрезвычайных ситуациях.

Контрольно-пропускной пункт - специально оборудованное место, через которое осуществляется доступ в соответствии с пропускным режимом.

Критически-важные точки объекта - строительные конструкции, элементы, узлы, коммуникации инженерных и других систем, несанкционированное воздействие на которые может привести к развитию чрезвычайных ситуаций.

Математическая (компьютерная) модель объекта – представление зданий и сооружений в виде конечно-элементной схемы для проведения численных расчетов для решения комплекса задач, возникающих при проектировании, строительстве и реконструкции зданий и сооружений, в том числе для определения рациональной структуры автоматизированной системы мониторинга и объективного анализа результатов.

Модель нарушителя - формализованные сведения о численности, оснащенности, подготовленности, осведомленности и тактике действий нарушителей (ля), их мотивации и преследуемых ими целях, используемые при выработке требований к системам комплексного обеспечения безопасности и оценке эффективности комплексного обеспечения безопасности многофункциональных высотных зданий и комплексов.

Нарушитель - лицо, совершившее или пытающееся совершить несанкционированное действие, а также лицо, оказывающее ему содействие в этом.

Несанкционированное воздействие - вмешательство в работу комплекса, направленное на нарушение правильности его функционирования.

Несанкционированное действие - совершение или попытка совершения диверсии, хищения, несанкционированного доступа, проноса (провоза) запрещенных предметов, вывода из строя технических средств защиты.

Несанкционированный доступ - проникновение лиц, не имеющих права доступа, в охраняемые зоны, здания, сооружения, помещения.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых сред-

ствами вычислительной техники или автоматизированными системами.

Обнаружение - установление факта несанкционированного действия.

Периметр - граница охраняемой зоны, оборудованная физическими барьерами и контрольно-пропускными пунктами.

Пропускной режим - установленный порядок пропуска персонала, посетителей, командированных лиц, транспортных средств, предметов, материалов и документов через границу охраняемой зоны, в (из) здания, сооружения, помещения.

Противотаранное устройство - заграждение, предназначенное для принудительной остановки транспортного средства.

Комплексное обеспечение безопасности уникальных и высотных объектов - разработка и реализация комплекса мероприятий в целях снижения рисков проявления угроз в отношении уникальных и высотных объектов на всех этапах их жизненного цикла. («Концепция комплексного обеспечения безопасности уникальных и высотных объектов города Москвы» введена распоряжением Правительства Москвы от 27.06.2007 № 1305-РП).

Система комплексного обеспечения безопасности уникальных и высотных объектов - совокупность структур в сфере государственной власти Российской Федерации и органов государственной власти города Москвы, организаций и граждан города, а также специально создаваемых органов управления, сил и средств, деятельность которых направлена на комплексное обеспечение безопасности уникальных и высотных объектов. («Концепция комплексного обеспечения безопасности уникальных и высотных объектов города Москвы» введена распоряжением Правительства Москвы от 27.06.2007 № 1305-РП).

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.

Система мониторинга инженерных систем - совокупность технических и программных средств, позволяющая осуществлять сбор и обработку информации о различных параметрах работы инженерных систем с целью передачи сообщений о возникновении или прогнозе аварийных ситуаций в Единую систему оперативно-диспетчерского управления г. Москвы.

Система охранная телевизионная - телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений (со звуковым сопровождением или без него), служебной информации и извещений о тревоге с охраняемого объекта (ГОСТ Р 51558-2000).

Служба безопасности - структурное подразделение высотного объекта, предназначенное для организации и контроля над выполнением мероприятий по обеспечению защиты высотного объекта, а также для выполнения ряда других специальных функций.

Считыватель - устройство в составе устройств ввода идентификационных признаков, предназначенное для считывания (ввода) идентификационных признаков (ГОСТ Р 51241-98).

Техническое средство обнаружения - устройство, предназначенное для автоматической выдачи сигнала срабатывания в случае несанкционированного действия.

Техническое средство охраны (техническое средство) - конструктивно законченное, выполняющее самостоятельные функции (аппаратно-программное) устройство, входящее в состав систем охранной, тревожной и/или пожарной сигнализации, контроля и управления доступом, охранного телевидения, сбора и обработки информации, других систем, предназначенных для обеспечения безопасности и антитеррористической защищенности высотного объекта, отдельных зон доступа объекта.

Тревожно-вызывная сигнализация - система экстренного вызова подразделений службы безопасности.

Уникальный объект - объекты, попадающие под категорию уникальных в соответствии со пунктом 2 статьи 48 Градостроительного кодекса РФ. (в ред. Федеральных законов от 22.07.2005 № 117-ФЗ, от 31.12.2005 № 199-ФЗ, от 31.12.2005 № 210-ФЗ, от 03.06.2006 № 73-ФЗ, от 27.07.2006 № 143-ФЗ, от 04.12.2006 № 201-ФЗ, от 18.12.2006 № 232-ФЗ, от 29.12.2006 №258-ФЗ).

Устройства ввода идентификационных признаков - электронные устройства, предназначенные для ввода запоминаемого кода, ввода биометрической информации, считывания кодовой информации с идентификаторов. В

состав данных устройств входят считыватели и идентификаторы (ГОСТ Р 51241-98).

Устройства исполнительные - устройства или механизмы, обеспечивающие приведение в открытое или закрытое состояние устройства преграждающие управляемые (электромеханические, электромагнитные замки, защелки, механизмы привода шлюзов, ворот, турникетов и т.д.) (ГОСТ Р 51241-98).

Устройства преграждающие управляемые - устройства, обеспечивающие физическое препятствие доступу людей, транспорта и других объектов, и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т.п. конструкции) (ГОСТ Р 51241-98).

Устройства управления - устройства и программные средства, устанавливающие режим доступа и обеспечивающие прием и обработку информации с устройства ввода идентификационных признаков, управление устройствами преграждающими управляемыми, отображение и регистрацию информации (ГОСТ Р 51241-98).

Физический барьер - инженерные сооружения, малые архитектурные формы и другие решения, создающие задержку проникновению нарушителя, использующего различные средства и приспособления, в охраняемые зоны или к уязвимым местам или препятствующие прорыву транспортных средств.

Электромагнитная совместимость инженерно-технических средств - способность инженерно-технических средств сохранять требуемое качество функционирования при воздействии на них электромагнитных помех с регламентированными значениями параметров и не создавать при этом электромагнитных помех другим техническим средствам (ГОСТ 29073-91).

4 ОБЩИЕ ТРЕБОВАНИЯ К ПРОЕКТИРОВАНИЮ СИСТЕМЫ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ

4.1 При проектировании необходимо рассматривать систему комплексного обеспечения безопасности и антитеррористической защищенности здания как организованное взаимодействие всех составных частей системы безопасности, включая инженерно-технические системы и персонал, выполняемых им организационных и технических действий и мероприятий, с единым центром управления, направленное на обеспечение безопасности людей, предотвращение несанкционированных действий, чрезвычайных ситуаций и минимизацию их последствий. Баланс между функциями безопасности, реализуемыми инженерно – техническими системами здания и принимаемыми организационными мерами, необходимо определить и обосновать при проектировании.

4.2 В составе проектной документации в соответствии с распоряжением Правительства Москвы от 29.12.2005 N 2683-РП «Об организации работы по обеспечению антитеррористической защищенности и комплексной безопасности высотных зданий и сооружений города Москвы» выполнить специальный раздел «Обеспечение комплексной безопасности и антитеррористической защищенности», на который необходимо получить заключения научно-технического совета Москомархитектуры и головной организации ГУП «НИИМосстрой», одобренных Межведомственной комиссией по обеспечению безопасности и антитеррористической защищенности высотных сооружений города Москвы.

4.3 Специальный раздел проекта должен выполняться по техническому заданию, согласованному Межведомственной комиссией по обеспечению антитеррористической защищенности и комплексной безопасности высотных сооружений города Москвы, специализированной организацией, имеющей соответствующие лицензии, а также специалистов, имеющих необходимую квалификацию по вопросам обеспечения комплексной безопасности и антитеррористической защищенности высотных зданий и сооружений и опыт в разработке требований к проектированию систем комплексного обеспечения безопасности и антитеррористической защищенности.

4.4 В соответствии с принятыми расчетными (проектными) угрозами и моделью нарушителя при проектировании необходимо определить перечень расчетных кризисных ситуаций, которые могут возникнуть вследствие реализации расчетных угроз.

4.5 При проектировании инженерно-технических систем и средств безопасности высотного и уникального здания (далее – объекта) необходимо привлечь специалистов служб, которые будут обеспечивать безопасность в процессе его эксплуатации, с тем, чтобы применение инженерно-технических систем и средств безопасности служило средством реализации организационных мер при решении задач:

- предупреждения чрезвычайных ситуаций;
- обнаружения фактов реализации угроз;
- эвакуации и спасения людей;
- ликвидации чрезвычайных ситуаций.

4.6 Для обеспечения комплексной безопасности и антитеррористической защищенности проектируемого объекта на период его сдачи в эксплуатацию должны быть разработаны оперативные планы действий при возникновении расчетных кризисных ситуаций, в процессе приемочных испытаний должны проводиться учения по их отработке и уточнению алгоритмов взаимодействия систем безопасности и служб.

5 ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СИСТЕМЫ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ

5.1 При проектировании системы комплексного обеспечения безопасности и антитеррористической защищенности при решении приведенных ранее задач необходимо руководствоваться следующими принципами:

- зонального построения;
- равнопрочности;
- обеспечения надежности и живучести;
- адаптивности;
- регулярности контроля функционирования;
- адекватности.

5.2 В рамках реализации *зонального* принципа:

- на объекте должны быть выделены контролируемые зоны общего и ограниченного доступа в соответствии с требованиями МГСН 4.19-2005 и с учетом результатов анализа уязвимости проектных решений (градостроительные, архитектурные, объемно-планировочные, конструктивные, технологические проектные решения);
- для каждой выделенной зоны ограниченного доступа должны быть разработаны алгоритмы входа/выхода с реализацией процедур, установленных пропускным режимом.

5.3 В рамках реализации принципа *равнопрочности*:

- при проектировании должен быть обеспечен примерно одинаковый (сопоставимый) уровень эффективности комплексного обеспечения безопасности и антитеррористической защищенности при реализации каждой из расчетных угроз для всех типов нарушителей, способов совершения несанкционированных действий и маршрутов движения нарушителей;
- уровень эффективности комплексного обеспечения безопасности и антитеррористической защищенности должен определяться в процессе проектирования с учетом критерия «эффективность-стоимость», включая затраты на эксплуатацию систем комплексного обеспечения безопасности и антитеррористической защищенности;
- равнопрочность должна обеспечиваться по всему периметру каждой выделенной зоны (для заданного помещения или группы помещений, территории), включая контролируемые проходы и/или КПП.

5.4 В рамках реализации принципа *обеспечения надежности и живучести*:

- должны быть предусмотрены взаимоувязанные и взаимно дополняющие друг друга технические решения и организационные меры, обеспечивающие выполнение задач системы комплексного обеспечения безопасности в штатных, проектных (расчетных) и чрезвычайных ситуациях, а также в процессе ликвидации последствий чрезвычайных ситуаций;
- должно быть предусмотрено резервирование функций управления системой комплексного обеспечения безопасности и антитеррористической защищенности высотного объекта;
- для обеспечения безопасности каждой отдельной зоны доступа, а также входящих в ее состав помещений, в составе комплекса технических средств

должны быть выделены отдельные группы инженерно-технических средств с организацией локальных пультов управления (ЛПУ), которые должны иметь все необходимые элементы управления, индикации и связи для обеспечения безопасности отдельных зон доступа (или функциональных элементов высотного объекта) и должны работать в автономном режиме;

- организация эксплуатации инженерно-технических средств должна предусматривать реализацию системы планово-предупредительного технического обслуживания и ремонта;

- должно быть обеспечено резервирование функций и элементов систем комплексного обеспечения безопасности (в том числе при проведении регламентных и ремонтных работ), при этом допускается резервирование отдельных функций за счет компенсационных мероприятий (с использованием персонала, технических и организационных мероприятий);

- для связи и передачи данных должны быть предусмотрены основные и резервные каналы передачи информации. Следует применять кольцевые структуры для обмена информацией, как наиболее эффективные;

- системы комплексного обеспечения безопасности должны быть спроектированы с использованием унифицированных модулей, обеспечивающих структурную, конструктивную, программную, информационную, электромагнитную совместимость;

- время, затрачиваемое на устранение неисправностей и отказов, возникающих в системе комплексного обеспечения безопасности, не должно превышать заданную при проектировании системы величину, а функции системы безопасности в этот период должны выполняться за счет резервирующих и компенсационных организационно-технических мероприятий.

5.5 В рамках реализации принципа *адаптивности*:

- должна быть предусмотрена возможность адаптации систем комплексного обеспечения безопасности при изменении:

- перечня расчетных угроз и моделей нарушителей, а также способов обеспечения безопасности;

- назначения функциональных элементов объекта, а также границ зон доступа;

- системы комплексного обеспечения безопасности должны иметь возможность образовывать, при необходимости, дополнительные рубежи безопасности (охранной сигнализации, управления доступом, видеонаблюдения и т.д.);

- в системах комплексного обеспечения безопасности должны обеспечиваться различные способы постановки под охрану/снятия с охраны зон доступа, помещений, отдельных средств, как в автоматическом, так и в полуавтоматическом режимах.

- системы комплексного обеспечения безопасности проектируемого высотного объекта должны адаптироваться к особенностям его работы, в том числе в чрезвычайных ситуациях с учетом принятых мер общественной, пожарной безопасности.

5.6 В рамках реализации принципа *регулярности контроля функционирования*:

- все технические средства и системы, используемые в системах комплексного обеспечения безопасности, должны иметь в своем составе компоненты и встроенные элементы, позволяющие осуществлять постоянный дистанционный контроль их состояния и работоспособности, а также объективный контроль действий персонала в целях устойчивого функционирования системы комплексного обеспечения безопасности и антитеррористической защищенности проектируемого высотного объекта.

5.7 В рамках реализации принципа *адекватности* (разумной достаточности):

- организационные меры, технические способы реализации комплексного обеспечения безопасности проекти-

руемого высотного объекта должны соответствовать принятым проектным угрозам и моделям нарушителей;

- выбор структуры и состава подсистем комплексного обеспечения безопасности должен производиться на основе результатов проведенного анализа уязвимости проектных решений высотного объекта с учетом критерия «эффективность-стоимость».

6 ТРЕБОВАНИЯ К ПРОЕКТНЫМ РЕШЕНИЯМ

В данном разделе приведены конкретные проектные решенияи, однако в нем можно выделить отдельные аспекты, являющиеся общими для большинства объектов.

6.1 Требования к генеральному плану

На прилегающей к объекту территории необходимо предусматривать места (площадки, проходы и т.п.), обеспечивающие беспрепятственное и безопасное рассредоточение эвакуирующихся из зданий людей с учетом прибывающих подразделений реагирования, которые будут размещаться со своей техникой на этой территории.

Прилегающая к объекту территория должна быть оборудована малыми архитектурными формами для исключения несанкционированного подъезда (прорыва) транспортных средств к высотному объекту (его уязвимым местам).

На въездах/выездах на прилегающую к объекту территорию должны быть предусмотрены контрольно-пропускные пункты для исключения несанкционированного проезда автотранспорта и прохода людей.

Въезды на прилегающую территорию должны оснащаться средствами снижения скорости.

На въездах/выездах на подземную автостоянку должны быть предусмотрены пункты досмотра транспорта, реализующие принцип шлюзования, для исключения провоза запрещенных предметов, проезда автотранспорта, не имеющего права проезда, и несанкционированного прохода.

Въезд в подземную автостоянку и выезд из нее должен осуществляться по специальным пропускам, которые выдаются службой безопасности высотного объекта в установленном порядке, определяемом индивидуально.

В подземной автостоянке не разрешается размещать автомобили с двигателями, работающими на сжатом природном газе и сжиженном нефтяном газе.

Въезд на территорию высотного объекта грузового транспорта, следующего в зоны погрузки/выгрузки, должен осуществляться по специальным пропускам, выдаваемым службой безопасности в установленном порядке.

При проектировании должны быть разделены пешеходные и транспортные потоки.

6.2 Требования к архитектурным, объемно-планировочным решениям и функциональным элементам

Объект должен быть разделен на контролируемые зоны общего и ограниченного доступа с учетом архитектурной концепции надземной части и функционального назначения помещений и территории.

В самостоятельные зоны доступа должны быть выделены пути эвакуации из надземной и подземной частей здания.

При проектировании необходимо определить и уточнить перечень контролируемых зон общего и ограниченного доступа с учетом режима работы, функционального назначения каждого из блоков, помещений или групп помещений объекта (в том числе принадлежащих арендодателю, и арендуемых помещений).

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

Исключить несанкционированный доступ со стороны эвакуационных лестниц на этажи надземной и подземной частей при нормальном режиме эксплуатации (при отсутствии команды на эвакуацию).

Для исключения несанкционированного доступа на этажи подземной автостоянки из стилобатной и высотной частей на выходах из лифтовых холлов на этажи подземной автостоянки предусмотреть организацию точек доступа.

6.3 Требования к составу служебных помещений

В здании необходимо предусмотреть следующие служебные помещения:

- для размещения технологического оборудования ГУВД г. Москвы (оборудование системы оперативной радиосвязи – СОРС (прил.3.1 МГСН 4.19-2005) и ГПС (Государственная противопожарная служба) ГУ МЧС

РФ по г. Москве;

- для системы мониторинга несущих конструкций здания (можно совместить с диспетчерской), проектом определить места установки измерительных пунктов (прил. 3.2 МГСН 4.19-2005);

- для системы мониторинга инженерных систем (в соответствии с Постановлением Правительства г. Москвы от 06.05.2008 №375-ПП)

- центрального пункта управления (ЦПУ) системами комплексного обеспечения безопасности высотного объекта площадью не менее 30 м² (площадь уточняется при проектировании);

- локальных пунктов управления (ЛПУ) системами комплексного обеспечения безопасности высотного объекта (необходимость выделения служебных помещений для организации ЛПУ системами комплексного обеспечения безопасности определяется при проектировании);

- размещения личного состава службы безопасности (необходимость выделения помещений для размещения личного состава службы безопасности определяется при проектировании).

Необходимость организации и размещения других служебных помещений, используемых для решения задач комплексного обеспечения безопасности и антитеррористической защищенности, определяется в процессе проектирования.

Конкретное размещение ЦПУ определяют при проектировании с учетом принятых проектных решений по организации взаимодействия с инженерными системами и системами противопожарной защиты.

Центральный и резервный пункты управления системами обеспечения безопасности необходимо защищать от несанкционированного вторжения.

Центральный и резервный пункты управления системами обеспечения безопасности должны быть защищены от поражения находящегося в нем персонала стрелковым оружием.

Для центрального диспетчерского пункта управления инженерными системами необходимо предусмотреть служебное помещение площадью, определенной в задании на проектирование. Центральный диспетчерский пункт управления инженерными системами необходимо проектировать, предусматривая защитные мероприятия по предотвращению несанкционированного проникновения.

При проектировании определить необходимость выделения отдельного помещения для размещения резервного пункта управления системами комплексного обеспечения безопасности (центр управления в кризисных ситуациях). Рассмотреть возможность размещения резервирующего оборудования ЦПУ на одном из локальных пунктов управления (ЛПУ) системами комплексного обеспечения безопасности (определить проектом).

При проектировании входных групп в здание предусматривать размещение постов охраны и точек доступа, оснащенных необходимым досмотровым оборудованием. Количество точек доступа определить с учетом обеспечения санкционированного (контролируемого) прохода лиц в здание и в его зоны доступа, в том числе в периоды пиковых нагрузок (начало и конец рабочего дня для помещений офисного назначения).

Вестибюли проектируют с учетом как наибольшего скопления людей в часы пик, так и с учетом необходимости размещения постов охраны и точек доступа, оборудованных пропускными устройствами и досмотровым оборудованием.

Выбор мест размещения эвакуационных выходов из надземных частей секций и подземного объема здания необходимо проектировать с учетом возможности беспрепятственного и безопасного рассредоточения эвакуирующихся людей. При этом необходимо учитывать, что прибывающие подразделения сил реагирования будут размещаться со своей техникой на территории, прилегающей к высотному объекту.

6.4 Требования к защите конструктивных элементов

При проведении расчета несущей конструктивной системы здания необходимо определить критически важные точки.

К критически важным точкам здания необходимо отнести те строительные конструкции, одновременное несанкционированное воздействие на которые (сопровождающееся такими поражающими факторами, как диверсионные взрывы, таран транспортным средством, комбинация тарана транспортным средством с диверсионным взрывом и последующим пожаром, воздействие механическим инстру-

ментом и др.) может привести к прогрессирующему обрушению.

Перечень критически важных точек (узлов строительных конструкций) и меры по их защите определяют при проектировании.

Критически важные точки (узлы строительных конструкций, коммуникации, воздухозаборники, узлы и оборудование, помещения и ниши, в которых располагаются элементы инженерно-технических систем безопасности и жизнеобеспечения) должны оснащаться средствами охранной сигнализации, видеонаблюдения, контроля и управления доступом и, при необходимости, физическими барьерами во избежание несанкционированных воздействий на них.

Все выходы на кровлю здания в отсутствие команды на эвакуацию или при их посещении уполномоченными сотрудниками служб эксплуатации и безопасности должны быть заперты и оборудованы средствами обнаружения несанкционированного проникновения и тревожно-вызывной сигнализации.

Потенциально доступные для проникновения нарушителя окна должны быть оборудованы средствами обнаружения (сигнализацией на разбивание остекления и открывание).

Выходы вентиляционных коробов, воздухозаборы и др. должны быть оборудованы средствами обнаружения вскрытия.

Подземные и наземные коммуникации высотного объекта, имеющие входы или выходы в виде колодцев, люков, лазов, шахт, открытых трубопроводов, каналов и других подобных сооружений, через которые можно проникнуть на прилегающую территорию и в здания, должны быть оборудованы постоянными или съемными решетками, крышками, дверями с запорами и находиться под контролем системы охранной сигнализации. Постоянные решетки должны устанавливаться на все коммуникации, не подлежащие открыванию и также находиться под контролем средств охранной сигнализации. Оборудованию подлежат все проемы, имеющие диаметр более 250 мм (сечение 250 х 250 мм). Меры по защите проемов определяют при проектировании.

Конструкции окон, витражей и их крепление к несущим конструкциям должны обеспечивать безопасность людей, находящихся в здании и на прилегающей территории, от поражения фрагментами перечисленных элементов.

7 ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВХОДА/ВЫХОДА В ВЫДЕЛЕННЫЕ ЗОНЫ ДОСТУПА

На входе/выходе в зоны ограниченного доступа необходимо осуществлять контроль проходящих лиц (проезжающего транспорта) посредством организации точек доступа.

Все точки доступа должны быть оснащены средствами контроля и управления доступом, обеспечивающими санкционированное перемещение людей (транспорта) и создающими препятствие несанкционированному перемещению.

Точки доступа входов в функциональные блоки здания должны оснащаться пропускными устройствами. При проектировании определить перечень стационарных и мобильных средств, обеспечивающих обнаружение запрещенных для проноса вещей (оружия, взрывчатых и радиоактивных и других опасных веществ).

Алгоритмы прохода в контролируемые зоны различных категорий лиц должны быть определены проектом. Алгоритмы прохода в контролируемые зоны различных категорий лиц должны быть уточнены на этапе опытной эксплуатации.

Точки доступа, оснащенные постами с постоянным и временным пребыванием сотрудника сил безопасности, организуются на входах в вестибюльные группы, на въездах (выездах) в подземную автостоянку. На таких точках доступа должны быть предусмотрены средства осмотра личных вещей (или транспорта соответственно), средства связи.

Точки доступа, не оснащенные постами охраны с постоянным пребыванием сотрудника службы безопасности, должны обеспечивать задержку несанкционированного проникновения и оснащаться средствами охранной сигнализации, контроля и управления доступом и телевизионного наблюдения.

Точки доступа, не оснащенные постами с постоянным пребыванием сотрудника сил безопасности, такие как, эвакуационные выходы и т.п., должны быть оснащены аварийными дверями, обеспечивающими эвакуацию через них только в экстренных случаях. Должна обеспечиваться возможность ручной и автоматической разблокировки таких проходов по сигналам систем безопасности, предусмотренными алгоритмами прохода.

Точки доступа, не оснащенные постами с постоянным пребыванием сотрудника сил безопасности, такие как, входы на технические этажи, в технические, инженерно-

технологические и служебные помещения должны обеспечивать возможность прохода через них только допущенного персонала.

Выходы на кровлю в отсутствие команды на эвакуацию должны быть доступны только для сотрудников служб эксплуатации и безопасности. Они должны быть оснащены средствами охранной сигнализации, контроля и управления доступом и телевизионного наблюдения.

8 ТРЕБОВАНИЯ К СТРУКТУРНЫМ КОМПОНЕНТАМ И ЭЛЕМЕНТАМ ТЕХНИЧЕСКИХ СРЕДСТВ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Исходя из принятых угроз и моделей нарушителя, объект должен быть оборудован техническими системами комплексного обеспечения безопасности, в состав которых, в общем случае, должны входить:

- системы противопожарной защиты, в том числе: автоматическая пожарная сигнализация, автоматическое пожаротушение, противопожарный водопровод, автоматика дымоудаления;
- система охранной сигнализации, в том числе охраны квартир;
- система тревожно-вызывной сигнализации;
- система контроля и управления доступом;
- система видеодомофонной связи;
- система телевизионного (видео) наблюдения, в том числе система охранного телевидения;
- система оповещения и управления эвакуацией людей из здания при возникновении чрезвычайных ситуаций, в том числе при пожаре;
- система мониторинга несущих конструкций;
- система мониторинга инженерных систем;
- *система контроля воздушно-газовой* среды в системе вентиляции;
- обеспечивающие системы.

В состав обеспечивающих систем КОБ должны входить:

- система оперативной связи;
- система телекоммуникаций;
- система защиты информации;
- система электропитания;
- система охранного освещения;
- система эвакуационного освещения.

Все перечисленные системы и подсистемы должны быть объединены (интегрированы) в единый комплекс инженерно-технических средств обеспечения безопасности и антитеррористической защищенности объекта с целью:

- наиболее полного использования возможностей каждой из систем для обнаружения и раннего пресечения подготовки террористических актов, чрезвычайных ситуаций техногенного характера, а также противоправных действий людей;
- повышения надежности каждого элемента КСБ за счет использования ресурсов смежных систем;
- достижения максимальной надежности и живучести КСБ за счет интеграции и взаимного дублирования;
- создания единого адаптированного программного обеспечения, обеспечивающего глубокую интеграцию систем и создание единого информационного пространства, необходимого для эффективного управления СКОБ в штатных и чрезвычайных ситуациях;
- сокращение затрат на содержание КСБ за счет использования элементов каждой из систем в интересах других.

Выбор оборудования каждой из подсистем проводить с учетом возможности их интеграции в единый комплекс инженерно-технических средств обеспечения безопасности и антитеррористической защищенности высотного объекта.

Требования к системам противопожарной защиты устанавливаются техническими условиями, согласованными в установленном порядке.

При проектировании систем безопасности, помимо выполнения ими основных функций, должно обеспечиваться взаимодействие с инженерными системами жизнеобеспечения по алгоритмам эксплуатации зданий в нормальных условиях, в период проведения регламентных работ, при чрезвычайных ситуациях и ликвидации их последствий.

Обмен информацией между инженерными системами и системами безопасности предусмотреть в уровне оборудования центрального диспетчерского пункта управления инженерными системами (ЦДП) и центрального пункта управления системами комплексного *обеспечения безопасности (ЦПУ) объекта, а* также локальных коммутационных центров внутри пожарных отсеков, что необходимо для сохранения взаимодействия между системами и обеспечения их работы в режимах чрезвычайных ситуаций при разрыве сетей связи между локальными коммутационными центрами и аппаратурой ЦДП и ЦПУ.

Для организации взаимодействия ЦДП ЦПУ с городскими службами в составе технических средств комплексного обеспечения безопасности предусмотреть создание системы мониторинга инженерных систем (СМИС).

В состав технических средств комплексного обеспечения безопасности должны входить средства досмотровой техники.

Проектирование и размещение дополнительных средств комплексного обеспечения безопасности, устанавливаемых арендаторами, должны осуществляться по согласованию со службой безопасности объекта. Управление в данном случае средствами КОБ арендаторов осуществляется с локальных пунктов управления (ЛПУ), которые должны быть оснащены средствами оперативной связи с ЦПУ. Места размещения ЛПУ определяются в процессе проектирования и согласовываются с администрацией и со службой безопасности объекта.

При угрозе и возникновении ЧС, а также при возникновении расчетных кризисных ситуаций, информация от средств КОБ, установленных арендаторами в своих помещениях, должна быть доступна на ЦПУ. Перечень и характеристики передаваемых сигналов подлежат согласованию со службой безопасности высотного объекта. При проектировании следует предусмотреть не менее 25% резерва емкости всех систем КОБ для подключения аппаратуры арендаторов. Номенклатура аппаратуры и способы подключения подлежат согласованию со службой безопасности высотного объекта.

При изменении функционального назначения арендуемых помещений, смене арендатора и т.п. вопросы замены применяемых средств КОБ подлежат обязательному согласованию со службой безопасности высотного объекта.

Постоянно неиспользуемые, временно неиспользуемые или иные помещения, не находящиеся под постоянным контролем со стороны арендаторов, должны находиться под наблюдением со стороны системы КОБ высотного объекта и СБ. Данные помещения следует объединять в группы и предусматривать установку:

- средств контроля и управления доступом на входе/выходе в группу помещений;
- средств системы охранной сигнализации на возможных путях проникновения;
- средств телевизионного наблюдения за входами и коридорами указанных групп помещений.

Средства пожарной сигнализации и пожаротушения размещают в соответствии с требованиями действующих нормативных документов.

9 ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМАМ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

9.1 Общие положения

В данном разделе формулируются требования к составным частям системы комплексного обеспечения безопасности. Требования подразделов являются общими для различных категорий объектов и согласуются с требованиями стандартов и руководящих документов, выпущенных федеральными органами исполнительной власти.

9.2 Система охранной сигнализации

Система охранной сигнализации должна обеспечивать:

– обнаружение несанкционированного доступа в охраняемые зоны, помещения;

– выдачу сигнала о срабатывании средств обнаружения персоналу охраны и/или службы безопасности и протоколирование этих *событий;*

– ведение архива всех событий, происходящих в системе, включая действия операторов, с фиксацией всех необходимых сведений для их последующей однозначной идентифика-

ции (тип и номер устройства, тип и причина события, дата и время его наступления и т.п.), исключая возможность внесения изменений в эту информацию;

– исключение возможности бесконтрольного снятия с охраны/постановки под охрану;

– выполнение процедур снятия с охраны всех входов и выходов на пути эвакуации при возникновении чрезвычайной ситуации в соответствии с алгоритмами функционирования;

– задание временных интервалов на выполнение процедур взятия под охрану/снятия с охраны;

– управление внешними устройствами (телевизионными камерами, дополнительным освещением, звуковыми и световыми оповещателями и др.) в автоматическом режиме по сигналам от охранных извещателей.

Перечень помещений, которые должны быть оснащены средствами охранной сигнализации, количество и тип рубежей охранной сигнализации определяют при проектировании в зависимости от функционального назначения, местоположения помещений, с учетом результатов анализа уязвимости проектных решений высотного объекта и требований МГСН 4.19-2005. Сведения уточняются на стадии опытной эксплуатации.

9.3 Средства тревожно-вызывной сигнализации

Средства тревожно-вызывной сигнализации предназначены для экстренного вызова групп оперативного реагирования подразделений охраны и/или службы безопасности, информирования персонала охраны о фактах совершения противоправных действий (разбойных нападений, хулиганских действий и т.д.).

Тревожно-вызывная сигнализация должна обеспечивать:

- информирование персонала службы безопасности о срабатывании устройств тревожно-вызывной сигнализации;
- определение места вызова;
- возможность скрытной и открытой установки и удобство пользования вызывным устройством;
- невозможность отключения устройств тревожно-вызывной сигнализации;
- отличительность сигналов срабатывания устройств тревожно-вызывной сигнализации от сигналов срабатывания системы охранной сигнализации и от других средств и систем;
- приоритет информации, поступающей в центральный пункт управления системами комплексного обеспечения безопасности от средств тревожно-вызывной сигнализации, по сравнению с сигналами, поступающими от других технических средств.

Средствами тревожно-вызывной сигнализации должны оснащаться точки доступа, оборудованные постами с постоянным или временным пребыванием сотрудника службы безопасности.

Перечень мест, которые необходимо оборудовать устройствами тревожно-вызывной сигнализации должен определяться при проектировании.

9.4 Система контроля и управления доступом

Система контроля и управления доступом должна обеспечивать санкционированный доступ людей и транспорта.

Система контроля и управления доступом должна обеспечивать исключение (или существенное затруднение) несанкционированного доступа нарушителей в охраняемые зоны и помещения. В случае обнаружения попыток несанкционированного доступа, а также при выявлении фактов силового воздействия на элементы конструкций пропускных устройств и терминалов системы контроля и управления доступом, соответствующая информация должна в реальном масштабе времени предоставляться дежурному(ым) оператору(ам).

В том случае, если не предусмотрены специальные аварийные проходы, пропускные устройства системы контроля и управления доступом должны отвечать требованиям, предъявляемым к аварийным проходам.

По классификации ГОСТ Р51241-98 СКУД должна соответствовать:

- по способу управления системы контроля и управления доступом - централизованным (сетевым) или универсальным системам;
- по функциональным характеристикам системы контроля и управления доступом - системам с расширенными функциями или многофункциональным;

5-ому классу устойчивости от разрушающих несанкционированных воздействий на автоматические тамбуры и двери точек доступа по следующим показателям:

- защищенность от взлома одиночными ударами;
- защищенность от взлома набором инструмента;
- пулестойкость;
- устойчивость к взрыву.

Примечание: Список точек доступа, отвечающих данным требованиям, определяется при проектировании.

В комплекс средств и систем контроля и управления доступом (систем КУД) должны входить:

- средства и системы, обеспечивающие реализацию пропуска непосредственно на территорию лиц, имеющих право на посещение высотного объекта или пребывания на его территории;
- средства и системы, обеспечивающие реализацию пропуска в помещения;
- средства и системы, обеспечивающие пропуск лиц в подземную автостоянку;
- средства и системы, обеспечивающие санкционированный пропуск транспортных средств;
- средства и системы, обеспечивающие реализацию санкционированного пропуска обслуживающего персонала в служебные и технические помещения (технические этажи).

Система контроля и управления доступом должна обеспечивать:

- организацию доступа людей и транспортных средств в соответствии с требованиями документов объектового уровня;
- реализацию режима шлюзования проезжающего транспорта при въезде/выезде на подземную автостоянку;
- протоколирование всех действий, совершаемых операторами, администраторами, персоналом системы, а также фактов изменения состояния средств КУД;
- автоматический контроль работоспособности средств системы и линий передачи информации, в том числе с использованием встроенных средств самодиагностики и тестирования;
- автономную работу контрольно-пропускных пунктов и точек доступа при нарушении связи с управляемыми устройствами с регистрацией и хранением информации обо всех событиях (с фиксацией даты и времени);
- сохранение работоспособности системы при отключении электропитания продолжительностью не менее 2 ч;
- ведение шифров допусков;
- использование идентификаторов, не содержащих информацию, знание и применение которой может привести к несанкционированному доступу;
- защиту от несанкционированного доступа при записи кодов идентификационных признаков в память системы;
- ручное, полуавтоматическое или автоматическое открывание преграждающих управляемых (УПУ) устройств для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с правилами установленного режима и правилами противопожарной безопасности;
- передачу сигнала тревоги на ЦПУ (ЛПУ) при использовании системы аварийного открывания УПУ;
- защиту технических и программных средств от несанкционированного доступа к элементам управления, установке режимов и информации;
- возможность подключения к системе дополнительных средств специального контроля и средств досмотра;
- возможность изготовления пропусков как для жильцов, постоянных сотрудников арендуемых помещений и их транспортных средств, так и для посетителей, при этом должен вестись полный архив изготавливаемых и выдаваемых пропусков.

9.4.1 Требования к пропускам

Пропуска, используемые в системе контроля и управления доступом, не должны содержать информацию, знание и применение которой может привести к несанкционированному доступу (ПИН-коды и другие эталонные данные).

Пропуска должны выдаваться каждому лицу, имеющему право прохода в контролируемые зоны, а водителям дополнительно пропуска на транспортные средства для автоматизированного учета проездов на автотранспортных КПП.

Пропуска для лиц, имеющих постоянное право прохода на высотный объект, должны обеспечивать возможность хранения видимой визуальной информации (фамилия, имя, отчество; фото и другие атрибуты, определяемые службой безопасности высотного объекта).

Лицам, получившим право временного или разового прохода должны выдаваться пропуска в соответствии с требованиями пропускного режима.

Структура СКУД должна быть построена таким образом, чтобы неисправное состояние одного блока электропитания или контроллера не приводило к одновременной неуправляемости замковыми устройствами дверных проемов в выделенную зону доступа.

В замковых устройствах должна быть обеспечена возможность механического разблокирования ригелей с внутренней и наружной сторон.

Средства контроля и управления доступом для прохода в помещения должны обеспечивать возможность принудительного отпирания двери ключом в аварийных ситуациях.

Средства контроля и управления доступом должны быть устойчивы к вскрытию. При каждой попытке вскрытия должен выдаваться соответствующий сигнал и блокировать обслуживаемую точку доступа.

9.5 Средства локализации взрывных устройств

На постоянно эксплуатируемых входах и выходах в здания и на входах в зоны контролируемого доступа должны быть установлены средства локализации взрывных устройств.

Средства локализации взрывных устройств предназначены для обеспечения безопасности людей и конструкций здания от взрывных устройств фугасного и осколочного действия с массой взрывчатого вещества до 1000 г тринитротолуола.

Места установки средств локализации взрывных устройств и их характеристики уточняются при проектировании.

9.6 Досмотровые средства

На контрольно-пропускных пунктах должны быть установлены стационарные или ручные средства, обеспечивающие досмотр проходящих лиц и проезжающего транспорта на предмет проноса (провоза) запрещенных предметов (оружия и других изделий из металла, взрывчатых веществ и т.п.). Конкретный перечень технических средств досмотровой техники и оснащение ими постов контроля определяется проектом.

Устанавливаемые металлообнаружители (МО) должны обеспечивать выдачу звукового и светового сигналов тревоги при проносе через зону контроля предметов из черных и цветных металлов массой 150 г и более и/или с габаритами 20x20x20 мм и более при скорости проноса через зону контроля от 0,3 до 2,5 м/сек.

Примечание: допускается использование принципов обнаружения:

- по массе;
- по объему;
- по массе и объему.

МО должен быть работоспособен при размещении на расстоянии не более 1 м от массивных движущихся и стационарных металлических предметов.

Для определения наличия запрещенных предметов могут использоваться рентгенотелевизионные установки (интраскопы). Характеристики интраскопов и размер досмотрового коридора выбираются при проектировании.

Для обнаружения наличия взрывчатых веществ необходимо использовать стационарные и ручные средства досмотра. Перечень используемых средств и их характеристики выбираются при проектировании.

9.7 Система телевизионного (видео) наблюдения (охранного телевидения)

Система телевизионного наблюдения должна обеспечивать дистанционное наблюдение за подступами к охраняемым зонам, участками периметров зон доступа (как внешних, так и внутренних) и другими областями пространства, а также охраняемыми помещениями и критически важными точками высотного объекта с целью оценки текущей обстановки, на-

блюдения за действиями и продвижением нарушителей, координации действий персонала службы безопасности.

По классификации ГОСТ Р51558-2000 система телевизионного наблюдения (охранного телевидения) должна соответствовать:

– группе систем с расширенными функциями или многофункциональных;

– классу «повышенная устойчивость» или классу «высокая устойчивость» по степени устойчивости от несанкционированных действий.

Система телевизионного наблюдения должна обеспечивать интеграцию с другими подсистемами комплексного обеспечения безопасности на аппаратном и программном уровне (включая, системы охранной и пожарной сигнализации, КУД, управления эвакуацией).

Система телевизионного наблюдения должна обеспечивать защиту от несанкционированного доступа к видеоинформации.

Центральное оборудование системы телевизионного наблюдения должно обеспечивать:

- возможность наращивания и замены блоков (модулей) без остановки работы системы;
- видеозапись информации в реальном времени из зон наблюдения по сигналам срабатывания средств обнаружения с включением информации, предшествовавшей срабатыванию с заданной продолжительностью;
- аварийное сохранение цифровых видеоархивов;
- оперативное отображение видеоинформации из зон наблюдения по сигналам от систем охранной, пожарной сигнализации, контроля и управления доступом;
- получение видеоинформации в объеме и с качеством, обеспечивающем определение характера и места нарушения, направление движения нарушителя;
- контроль над действиями персонала охраны с возможностью последующего анализа;
- представление оператору необходимой и достаточной информации об обстановке на высотном объекте и в его отдельных контролируемых зонах, сооружениях и помещениях (число камер, их направление, углы обзора и другие параметры определить проектом);
- отображение, регистрацию и архивирование всей поступающей информации, включая изображение (звук), номер камеры место установки, дату и время съемки (длительность хранения архивированной информации и ее объем, необходимый для последующего анализа возникающих нештатных ситуаций определяют проектом);
- работоспособность во всех условиях ее эксплуатации, определенных в нормативно-технической документации;
- контроль наличия неисправностей (пропадание видеосигнала, вскрытие оборудования, попытки доступа к линиям связи и т.п.), информирование об этом оператора и архивирование данной информации.

9.7.1 Требования к размещению телекамер

При организации телевизионного контроля на границах контролируемых зон телекамеры необходимо устанавливать в пределах прямой видимости, как минимум, одной из телекамер соседних участков.

При размещении телекамер необходимо обеспечивать возможность сопровождения цели (нарушителя) на наиболее вероятном пути движения к контролируемым зонам (последовательным переключением телекамер).

Должна быть предусмотрена возможность визуального определения номеров автотранспортных средств, подъезжающих к местам въезда (выезда) на территорию и на парковки.

Установку телекамер и необходимого осветительного оборудования следует производить с учетом оптимальной реализации рабочих характеристик телевизионной и осветительной аппаратуры и максимального затруднения несанкционированного доступа к ней.

Время перехода аппаратуры системы охранного телевидения от дежурного режима к рабочему должно быть сведено к оправданному минимуму.

Выбор мест размещения телекамер, необходимого осветительного оборудования определить проектом.

9.7.2 Требования к постам наблюдения

Рабочее место оператора системы видеонаблюдения - разместить на центральном пункте управления системами комплексного обеспечения безопасности. Количество мониторов, технические характеристики аппаратуры, угловые размеры зоны наблюдения, качество изображения необходимо выбрать при проектировании.

Компьютер рабочего места анализа видеоархива - разместить отдельно.

Предусмотреть возможность организации дополнительных постов наблюдения:

- на рабочем месте администратора безопасности;
- на рабочем месте ответственного дежурного службы безопасности;
- на постах охраны.

9.8 Система управления эвакуацией людей при возникновении чрезвычайных ситуаций (СУЭВ)

СУЭВ должна обеспечивать организацию оповещения и управление системами комплексного обеспечения безопасности и инженерными системами жизнеобеспечения с целью беспрепятственного и своевременного движения людских потоков из здания в следующих случаях:

– ***вынужденной эвакуации*** при возникновении чрезвычайной или критической ситуации, когда жизнь и здоровье людей, находящихся в здании, подвергаются реальной опасности;

– ***превентивной эвакуации,*** когда существует обоснованная возможность реализации конкретной угрозы;

– ***тренировочной эвакуации*** при отработке действий при возможных чрезвычайных ситуациях.

Для каждого из перечисленных случаев эвакуации должны быть разработаны алгоритмы функционирования СУЭВ при полной или частичной, одновременной или поэтапной, в отдельных случаях с использованием лифтов, эвакуации людей из здания в зоны безопасности, расположенные на прилегающей к зданию территории. При разработке алгоритмов функционирования СУЭВ необходимо учитывать возрастной состав, физическое состояние эвакуирующихся людей и возможное поведение людей, обусловленное различными уровнями психофизиологической напряженности при различных случаях эвакуации.

Система управления эвакуацией людей при чрезвычайных ситуациях должна интегрироваться с системами:

- звукового, речевого и светового оповещения о пожаре;
- контроля и управления доступом;
- охранной сигнализации;
- пожарной сигнализации;
- охранного телевидения;
- аварийного освещения эвакуационных путей;
- управления инженерным оборудованием высотного объекта.

При проектировании СУЭВ необходимо разрабатывать расчетные варианты эвакуации в зависимости от места возникновения и характера ЧС, в том числе поэтапную или частичную эвакуацию из высотных секций здания.

При разработке СУЭВ необходимо учитывать:

- функциональную структуру здания;
- разделение на пожарные отсеки;
- реализуемые СУЭВ функции;
- максимальное количество людей, которое может одновременно находиться в здании;
- характеристики технических средств, входящих в состав интегрированной системы управления эвакуацией людей при чрезвычайных ситуациях.

Комплекс технических средств (КТС) СУЭВ должен обеспечивать оператору следующие возможности:

- представление на экране монитора информации о пожаре или ЧС;
- передачу по громкоговорящей связи сообщения лицу, принимающему решение (ЛПР) об эвакуации, информации о месте возникновения пожара или другой ЧС и количестве людей, подвергающихся опасности, сообщение автоматически должно транслироваться в пожарные подразделения и в

Единую систему оперативно-диспетчерского управления в чрезвычайных ситуациях г. Москвы.

Комплекс технических средств СУЭВ должен обеспечивать запись информации:

- о времени поступления сигнала о пожаре (ЧС) и месте его возникновения;
- о времени начала и окончания эвакуации;
- все речевые сообщения, включая сообщения ЛПР, и все команды управления оборудованием, с привязкой к времени и дате.
- Оператор, получив разрешение на эвакуацию, должен иметь возможность сформировать команды:
- включения технических средств светового, звукового, речевого оповещения, относящихся к той схеме эвакуации, которая соответствует возникшей расчетной ситуации;
- поиска (осуществляется автоматически) речевых инструкций, соответствующих конкретной схеме эвакуации;
- отключения запирающих устройств и других элементов СКУД по алгоритму, соответствующему данному варианту эвакуации;
- отключения и/или перевода в другой режим работы средств охраны, при этом персонал службы безопасности должен выполнять предписанные функции, соответствующие данному варианту эвакуации.

Оператор, управляя процессом эвакуации (до прибытия подразделений МЧС), должен иметь возможность поддерживать постоянную связь с задействованными экстренными службами (МЧС России, МВД России, службой скорой помощи).

При проведении эвакуации должна в автоматическом режиме осуществляться запись всех переговоров, которые ведутся по средствам связи, а также речевых инструкций, транслируемых по громкоговорящей связи.

Разработка проекта СУЭВ должна осуществляться на основании расчетов эвакуации при различных вариантах пожара или ЧС.

Результаты расчетов вариантов эвакуации, варианты управления эвакуацией должны использоваться при проектировании систем контроля и управления доступом, охранной и пожарной сигнализации, охранного телевидения и, при необходимости, других систем комплексного обеспечения безопасности, при обосновании требований к времени живучести этих систем при различных чрезвычайных ситуациях.

Взаимосвязь задач, решаемых СУЭВ при чрезвычайных ситуациях, определяется общим алгоритмом функционирования, который отражает принятую стратегию управления в соответствии с разработанными схемами эвакуации.

Алгоритмы управления периферийными устройствами при управлении эвакуацией должны предусматривать:

- включение в определенном порядке световых указателей и знаков;
- речевое оповещение об эвакуации;
- управление устройствами контроля доступа на путях эвакуации.

9.9 Система мониторинга несущих конструкций

Система мониторинга несущих конструкций должна быть разработана на этапе проектирования объекта, установлена во время его строительства, и использоваться в период эксплуатации.

В рамках проектирования системы мониторинга несущих конструкций должны быть определены:

- ответственные узлы и конструкции;
- вероятные сценарии отказа работы строительных конструкций объекта;
- перечень контролируемых параметров напряженно-деформированного состояния несущих конструкций;
- расчетные значения параметров контроля напряженно-деформированного состояния объекта, полученные в результате математического моделирования работы строительных конструкций объекта;
- состав и технические характеристики аппаратного и программного обеспечения;
- архитектура построения системы, программного обеспечения и способы интеграции с другими автоматизированными системами объекта;

– алгоритм и критерии принятия управленческих решений по оценке технического состояния объекта;

– форма заключения по результатам мониторинга;

– сценарии реагирования, в том числе регламент взаимодействия со специализированными организациями, выполняющими инструментальное обследование отдельных элементов конструкций.

Система мониторинга несущих конструкций должна иметь следующую структуру:

– первичные датчики и оборудование;

– система сбора, управления и первичной обработки данных;

– математическая (компьютерная) модель объекта для комплексных инженерных расчетов определения вероятных сценариев отказов и параметров контроля напряженно-деформированного состояния строительных конструкций объекта;

– комплекс специального программного обеспечения по обработке данных и отображению результатов мониторинга, оценке технического состояния (устойчивости, сейсмостойкости, остаточного ресурса и долговечности) и определению управляющих решений и рекомендаций по эффективной эксплуатации.

Первичные датчики и оборудование в зависимости от конкретной схемы системы мониторинга должны фиксировать следующие показатели:

– колебания строительных конструкций;

– измерения наклонов, прогибов и кренов строительных конструкций;

– измерения неравномерной и абсолютной осадки оснований зданий и сооружений;

– геометрические параметры здания с использованием автоматизированной высокоточной геодезической аппаратуры;

– деформации строительных конструкций (фундаментная плита, колонны, перекрытия, несущие стены, ответственные узлы);

– температурно-влажностный режим.

Система сбора, управления и первичной обработки данных должна обеспечивать централизованное управление, получение и обработку данных измерений по каналам проводной или беспроводной связи, хранение результатов измерений, проверку работоспособности и калибровку первичных датчиков и оборудования.

Математическая (компьютерная) модель объекта разрабатывается для объективного анализа результатов мониторинга деформационного состояния несущих конструкций, для проведения инженерных расчетов по оценке возникновения и развития дефектов в строительных конструкциях, в том числе и в различных кризисных ситуациях.

Математическая модель объекта мониторинга должна быть разработана независимо от разрабатываемой конструкторами расчетной модели объекта с использованием другого расчетного программного комплекса.

Математическая модель объекта должна уточняться при получении показаний датчиков системы мониторинга в рамках работ по научно-техническому сопровождению строительства, осуществляемого в соответствии с ТР 182-08 «Технические рекомендации по научно-техническому сопровождению и мониторингу строительства большепролетных, высотных и других уникальных зданий и сооружений».

Математическая модель объекта мониторинга (после всех уточнений) должна максимально соответствовать построенному объекту и используется на этапе строительства и эксплуатации для анализа результатов мониторинга, оценки и прогноза развития дефектов.

Комплекс специального программного обеспечения по обработке данных и отображению результатов мониторинга, оценке технического состояния (устойчивости, сейсмостойкости, остаточного ресурса и долговечности) и определению управляющих решений и рекомендаций по эффективной эксплуатации должен состоять из двух модулей:

– программный модуль (спецпроцессор) по интегрированной обработке разнородных измерений для определения технического состояния несущих конструкций, алгоритм работы которого должен быть основан на критериях сравнения измеренных значений с допустимыми, установленными специалистами применительно к зданию на начальной стадии эксплуатации системы мониторинга (после ввода объекта в эксплуатацию). В спецпроцессор должны быть заложены критерии для определения технического состояния несущих конструкций;

– программный модуль на базе современных геоинформационных систем для управления системой мониторинга, регулярной проверки работоспособности элементов системы мониторин-

га, прогноза и формирования перечня факторов, угрожающих безопасности объекта, анализа результатов мониторинга и формирования отчетных материалов для эксплуатационной службы объекта. Программный комплекс должен обеспечивать возможность отображения на трехмерной модели объекта мест и динамики развития дефектов (в том числе и скрытых) и внешних факторов (например, зон образования карстовых явлений под фундаментом здания). Программный комплекс должен быть открыт для интеграции с системами диспетчеризации и управления инженерным оборудованием для передачи в систему диспетчеризации информации об ухудшении технического состояния объекта.

В системе мониторинга несущих конструкций должны применяться апробированные и сертифицированные в установленном порядке способы, технические и программные средства для определения технического состояния несущих конструкций.

9.10 Система мониторинга инженерных систем (СМИС)

Система мониторинга инженерных систем предназначена для автоматизированного сбора информации от инженерных систем объекта, контроля возникновения дестабилизирующих факторов и передачи оперативной информации по предупреждению и ликвидации последствий чрезвычайных ситуаций в Единую систему оперативно-диспетчерского управления города.

Система мониторинга инженерных систем должна обеспечивать контроль работоспособности инженерных систем и возникновения угроз нарушения нормальной эксплуатации объекта:

В рамках проектирования системы мониторинга инженерных систем должны быть определены:

- перечень контролируемых инженерных систем объекта;
- перечень контролируемых параметров работы инженерных систем;
- расчетные (проектные) значения контролируемых параметров работы инженерных систем;
- структурная схема автоматизации СМИС и способы интеграции со смежными системами объекта;
- состав и технические характеристики аппаратного и программного обеспечения;
- месторасположение программно-аппаратного обеспечения СМИС;
- алгоритм и критерии принятия управленческих решений по оценке работоспособности инженерных систем, оценке угрозы нарушения нормальной эксплуатации и передаче сообщений в Единую систему оперативно-диспетчерского управления города;
- технические решения по взаимодействию СМИС с инженерными системами объекта;

СМИС должна быть реализована в виде программно-аппаратного комплекса с возможностью репликации данных.

СМИС должна обеспечивать возможность ведения архива данных не менее чем за 12 месяцев.

В СМИС не должны включаться оконечные устройства (исполнительные устройства), контроллеры и другое оборудование, используемое для сбора информации и контроля работоспособности инженерных систем объекта. Данные устройства должны реализоваться в рамках инженерных систем объекта.

Взаимодействие СМИС с инженерными системами объекта должно осуществлять на программном уровне.

Аппаратно-программный комплекс СМИС должен обеспечивать возможность резервирования информации.

Аппаратное обеспечение СМИС должно включать:

- Основной сервер;
- Резервный сервер;
- Рабочую станцию автоматизированного рабочего места СМИС.

Программное обеспечение (ПО) СМИС должно включать системное и прикладное ПО.

Системное ПО СМИС состоит из операционных систем, антивирусов, драйверов оборудования, обеспечивающих функционирование аппаратного обеспечения СМИС.

Прикладное ПО СМИС обеспечивает реализацию функционального назначения СМИС и должно включать:

- программный модуль взаимодействия с инженерными системами (специализированные драйверы);
- программный модуль сбора данных для организации приема и хранения данных от инженерных систем;
- программный модуль ввода и отображения информации на базе геоинформацион-

ной системы;

– программный модуль обработки, анализа и фильтрации сигналов (Спецпроцессор для настройки правил обработки сигналов, их обработки и фильтрации);

– программный модуль передачи информации для осуществления передачи информации городским службам;

– программный модуль для настройки и администрирования СМИС.

9.11 Системы контроля воздушно-газовой среды в системах вентиляции и кондиционирования

Системы контроля воздушно-газовой среды в системах вентиляции и кондиционирования должны обеспечивать обнаружение отравляющих и других опасных веществ, горючих и токсичных газов, перечень которых должен уточняться при проектировании.

В случае выявления веществ, подлежащих обнаружению, должны определяться их концентрация и выдаваться соответствующие сообщения дежурным операторам в ЦПУ системами комплексного обеспечения безопасности и Центрального 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.

9.12 Требования к обеспечивающим системам

9.12.1 Требования к оперативной связи

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

Система оперативной связи должна обеспечивать:

– надежную и непрерывную работу на всей территории высотного 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 МВД и МЧС.

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

Прямая телефонная связь должна обеспечивать:

– телефонную связь оператора центрального пункта управления системами комплексного обеспечения безопасности высотного объекта с ответственным дежурным службы безопасности, с пунктами управления системами обеспечения безопасности функциональных блоков здания, где располагаются арендуемые помещения, с пропускными пунктами, с постами охраны, а также со службами (подразделениями) высотного 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

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 центральном пункте управления системами комплексного обеспечения безопасности необходимо предусматривать резерв средств радиосвязи (не менее 10%) для организации взаимодействия сотрудников службы безопасности с пожарными и спасателями при возникновении чрезвычайных ситуаций на высотном объекте.

9.12.2 Требования к системе телекоммуникаций

Системы КОБ должны объединяться в комплексы и строиться на базе единого информационного пространства, с использованием самостоятельных кабельных сетей, пространственно отделенных от других слаботочных систем высотного объекта.

Информационное взаимодействие с системами обеспечения безопасности арендуемых помещений следует осуществлять на уровне пультов управления.

Оборудование системы телекоммуникаций должно применяться в том случае, если штатное оборудование, входящее в состав функциональных систем комплексного обеспечения безопасности, не отвечает предъявляемым требованиям в части передачи циркулирующей в системах КОБ информации, а также для стыковки и согласования различных систем, участвующих в работе.

Система телекоммуникаций должна обеспечивать:

- передачу достоверной информации;
- непрерывность функционирования;
- тактически приемлемое время доставки сообщений;
- систематизацию, архивирование и документирование необходимой информации о функционировании системы телекоммуникаций;
- обмен информацией с другими элементами системы комплексного обеспечения безопасности высотного объекта.

В системе телекоммуникаций должны быть предусмотрены резервные каналы передачи функционально значимой для работоспособности системы комплексного обеспечения безопасности информации. Резервные каналы должны прокладываться по физически разнесенным с основными каналами маршрутам. Резервный канал должен обеспечивать передачу функционально значимой информации, собираемой на локальные пункты управления в пределах пожарного отсека (зоны доступа, блоков помещений определенного функционального назначения) до центрального пункта управления.

Система телекоммуникаций должна обеспечивать формирование замкнутой системы передачи информации, обеспечивая работоспособность отдельных(ой) охраняемых(ой) зон(ы). Для взаимодействия с остальными элементами системы комплексного обеспечения безопасности должны применяться один или несколько защищенных и недоступных для нарушителя каналов связи.

Для повышения живучести систем комплексного обеспечения безопасности в условиях чрезвычайных ситуаций, система телекоммуникаций должна проектироваться с учетом деления высотного объекта на функциональные и пожарные отсеки. В случае наступления чрезвычайной ситуации или выхода из строя телекоммуникационной системы какого-либо отсека, функционально-значимая информация от аппаратуры систем комплексного обеспечения безопасности других отсеков должна передаваться по резервному каналу в центральный пункт комплексного обеспечения безопасности.

К функционально-значимой информации следует относить информацию об изменении критически важных параметров, определяющих безопасность высотного объекта (определяется при проектировании).

Линейно-кабельные сооружения системы комплексного обеспечения безопасности высотного объекта (кабельные колодцы, участковые и распределительные шкафы) должны выполняться в защищенном исполнении и находиться под контролем системы охранной сигнализации.

Информационные кабели системы комплексного обеспечения безопасности высотного объекта должны прокладываться в соответствии с положениями и требованиями нормативных документов, инструкций по установке и эксплуатации технических средств КОБ высотного объекта и ПУЭ, а также с учетом требований по защите информации.

9.12.3 Система защиты информации

Необходимость защиты информации обусловлена наличием в системах комплексного обеспечения безопасности информации, определяющей режим их функционирования и/или раскрывающей систему защиты высотного объекта. Несанкционированное воздействие на такую информацию может привести к снижению эффективности функционирования системы комплексного обеспечения безопасности в целом или ее отдельных элементов.

Проектирование структурных компонентов (функциональных систем и подсистем) систем комплексного обеспечения безопасности высотного объекта, а также помещений, в которых размещаются центральный и локальные пульты управления с устанавливаемым в них оборудованием, должно проводиться с учетом реализации технических мероприятий по защите информации.

Сети обмена информацией между комплексами безопасности и управления инженерными системами должны относиться к классу не менее 1Г в соответствии с требованиями РД Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

Примечание: Класс защищенности определяется, исходя из категории высотного объекта, комбинации функциональных блоков, наличия в системе максимального уровня чувствительности информации.

9.12.4 Система электропитания

Все электроприемники технических средств КОБ по степени надежности электроснабжения должны быть отнесены к особой группе первой категории в соответствии с классификацией ПУЭ.

Электропитание основных элементов системы комплексного обеспечения безопасности в нормальных режимах должно осуществляться от двух независимых источников переменного тока с взаимным резервированием, а при нарушении электроснабжения, должно предусматриваться дополнительное питание от третьего независимого взаимно резервирующего источника питания.

В качестве третьего независимого источника питания могут быть использованы местные электростанции, автономные генераторные установки, агрегаты бесперебойного питания, аккумуляторные батареи и т.п.

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 системы комплексного обеспечения безопасности должны быть защищены от несанкционированных действий.

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

Для кабельных линий электропитания должны быть использованы выпускаемые силовые кабели и установочные провода, выбор которых при проектировании должен быть произведен с учетом условий их прокладки.

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

9.12.5 Система охранного освещения

Охранное освещение должно являться вспомогательным средством, обеспечивающим функционирование технических средств и охраны высотного объекта в темное время суток.

Охранное освещение должно обеспечивать реализацию следующих функций:

– создание необходимой по интенсивности, равномерной освещенности досмотровых площадок, а также контрольно-пропускных пунктов;

– ручное дистанционное включение освещения участков периметра, других охраняемых объектов из помещения ответственного дежурного службы безопасности при отказе автоматического управления;

– освещение входов в здание и в охраняемые помещения.

В качестве приборов охранного освещения могут быть использованы светильники с люминесцентными лампами и лампами накаливания, другие источники света при условии сопряжения цветовых температур источников света и телевизионных камер.

Проектирование охранного освещения должно осуществляться в соответствии с положениями СНиП 23.05-95 «Естественное и искусственное освещение».

Охранное освещение проектируют с учетом общей концепции подсветки территории высотного объекта и находящихся на его территории зданий.

Помещения службы безопасности, контрольно-пропускные пункты, входы в здания, коридоры, прилегающие к охраняемым помещениям, в соответствии с ПУЭ должны быть дополнительно оборудованы аварийным охранным освещением. Переход с охранного освещения на аварийное и обратно должен осуществляться автоматически без перерыва.

Освещение транспортных контрольно-пропускных пунктов, досмотровых площадок на этих пунктах должно обеспечивать проведение досмотра транспорта и провозимых грузов. Осветительные приборы должны быть расположены таким образом, чтобы досматриваемый транспорт равномерно освещался со всех сторон, в том числе и снизу. В необходимых слу-

чаях следует предусмотреть возможность использования переносного освещения.

9.12.6 Подсистема эвакуационного освещения

В здании должно быть предусмотрено рабочее и аварийное эвакуационное освещение. Применение аварийного освещения определяется для различных помещений требованиями СП 31-110-2003.

Периферийные устройства аварийного эвакуационного освещения (предупреждающие надписи, указатели направления движения) следует размещать с учетом разработанных вариантов эвакуации. При этом кроме основных устройств, необходимо дополнительно предусмотреть установку в качестве периферийных устройств систем аварийного эвакуационного освещения - светильники с автономным электропитанием.

Кроме того, высотные секции здания должны оснащаться фотолюминесцентными эвакуационными системами (ФЭС).

Фотолюминесцентные эвакуационные системы

Фотолюминесцентные эвакуационные системы предназначены:

– для обеспечения эвакуации людей в отсутствие электрического освещения или ограниченной видимости;

– для обозначения мест размещения спасательных средств, средств противопожарной и противоаварийной защиты, средств оказания первой помощи;

– для предотвращения возникновения паники в условиях чрезвычайной ситуации;

– для предоставления необходимой информации о правилах поведения в условиях ограниченной видимости или полной темноты.

В условиях выхода из строя систем энергоснабжения высотного объекта возможность ориентации в здании должна обеспечиваться свойством длительного послесвечения знаков безопасности, ориентирующих линий, разметки для визуализации коридоров, ступеней лестниц, дверей эвакуационных и аварийных выходов, планов эвакуации.

10 ОБОРУДОВАНИЕ ЦЕНТРАЛЬНОГО ПУНКТА УПРАВЛЕНИЯ СИСТЕМОЙ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Оборудование центрального пункта управления системами комплексного обеспечения безопасности должно обеспечивать:

– представление оператору поступающей информации о несанкционированном проникновении нарушителей в охраняемые зоны (помещения) в реальных буквенно-цифровых координатах высотного объекта;

– контроль состояния средств обнаружения;

– формирование звукового сигнала при изменении состояния контролируемых средств и устройств;

– сигнализацию об отказах и неисправностях аппаратуры системы;

– автоматический и ручной дистанционный контроль работоспособности подключенных средств обнаружения;

– регистрацию действий оператора по обработке сигналов и управлению системами;

– возможность тестирования аппаратуры в автоматическом режиме и по запросам оператора;

– предотвращение несанкционированного доступа к программным средствам и базам данных;

– сохранение вводимых данных параметрирования центральной аппаратуры при отключении напряжения электропитания;

– регистрацию времени поступления сигналов при срабатывании средств обнаружения и обработки их оператором;

– реализацию различных тактик постановки (снятия) под охрану (с охраны) средств обнаружения (группы средств обнаружения), выбираемых при проектировании из следующих вариантов:

– постоянно под охраной (без права снятия);

– централизованная (оператор с рабочего места);

– децентрализованная (пользователь по пропуску);

– комбинированная (пользователь и оператор).

Помещение центрального пункта управления системами комплексного обеспечения безопасности должно быть оборудовано:

– техническими средствами управления СУЭВ при чрезвычайных ситуациях;

– аппаратурой управления и видеоконтрольными устройствами (мониторами) системы охранного телевидения и контроля доступа;

– коммутатором прямой телефонной связи;

– средствами телефонной связи с ответственным дежурным службы безопасности, МЧС и с территориальными органами МВД.

На ЦПУ должен осуществляться контроль устойчивого функционирования технических систем жизнеобеспечения:

– инженерно-технического комплекса пожарной безопасности высотного объекта;

– теплоснабжения (центрального отопления, вентиляции и кондиционирования);

– водоснабжения и канализации;

– электроснабжения;

– лифтового оборудования;

– системы управления эвакуацией при чрезвычайных ситуациях.

Для этого на ЦПУ необходимо контролировать следующие основные дестабилизирующие факторы:

– возникновения пожара;

– нарушения в системе отопления, подачи горячей и холодной воды, вызванные выходом из строя инженерного оборудования на центральных тепловых пунктах, котельных, а также авариями на трубопроводах и приборах отопления;

– нарушения в подаче электроэнергии;

– отказ в работе лифтового оборудования;

– несанкционированное проникновение в служебные помещения;

– повышенный уровень взрывоопасных концентраций газо-воздушных смесей;

– затопление помещений, дренажных систем и технологических приямков;

– изменения состояния инженерно-технических конструкций (конструктивных элементов) высотного объекта.

Типы и количество информационных сигналов должны быть уточнены как по отдельным системам, так и в целом по высотному объекту на этапе рабочего проектирования.

Для управления СКОБ в условиях воздействия проектной угрозы должны быть организованы основной и резервный ЦПУ (при проектировании определить возможность использования одного из ЛПУ в качестве резервного ЦПУ).

Для управления отдельными подсистемами комплексного обеспечения безопасности могут организовываться ЛПУ Необходимость их организации и конкретные места размещения определяются в процессе проектирования.

ЛПУ организуются также для групп помещений, выделяемых под аренду. Необходимость их организации и порядок функционирования согласовывается со службой безопасности высотного объекта. В кризисных ситуациях (расчетных ситуациях) персонал ЦПУ должен иметь доступ к информации, поступающей на ЛПУ арендатора. Перечень видов такой информации и ее объем определяется при проектировании.

Управление оборудованием, размещенным в точках доступа, оснащенных постами с постоянным пребыванием сотрудника сил безопасности, осуществляется с ЛПУ. Техническое оснащение определяется при проектировании.

Управление дополнительными элементами СКОБ в помещениях, устанавливаемыми арендаторами (собственниками), обеспечивается с ЛПУ, которые должны работать совместно с центральным и резервным пунктом управления СКОБ высотного объекта. Порядок взаимодействия и протоколы обмена информацией, а также требования по защите информации определяются отдельными индивидуальными требованиями.

Приложение А

СПИСОК НОРМАТИВНО-ТЕХНИЧЕСКИХ ДОКУМЕНТОВ, ИСПОЛЬЗОВАННЫХ ПРИ РАЗРАБОТКЕ ТР, И РЕКОМЕНДУЕМЫХ ДЛЯ ИСПОЛЬЗОВАНИЯ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ И КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ВЫСОТНЫХ ОБЪЕКТОВ

Номер документа	Наименование документа
№ 35-ФЗ от 06.03.2006	Федеральный закон «О противодействии терроризму»
№ 184-ФЗ от 27.12.2002	Федеральный закон «О техническом регулировании»
2683-РП от 29.12.2005	Распоряжение Правительства Москвы «Об организации работы по обеспечению антитеррористической защищенности и комплексной безопасности высотных зданий и сооружений города Москвы»
№1305–РП от 27.06.2007	Распоряжение Правительства Москвы «Об утверждении Концепции комплексного обеспечения безопасности уникальных и высотных объектов города Москвы»
МГСН 4.19-2005	Временные нормы и правила проектирования многофункциональных высотных зданий и зданий-комплексов в городе Москве
ГОСТ 21.101-97	Система проектной документации для строительства. Основные требования к проектной и рабочей документации.
ГОСТ 21.110-95	СПДС. Правила выполнения спецификации оборудования, изделий и материалов.
ГОСТ 21.406-88	СПДС. Проводные средства связи. Обозначения условные графические на схемах и планах.
ГОСТ 21.501-93	СПДС. Правила выполнения архитектурно-строительных рабочих чертежей
ГОСТ 21.508-93	СПДС. Правила выполнения рабочей документации генеральных планов предприятий, сооружений и жилищно-гражданских объектов
ГОСТ Р 21.1703-2000	СПДС. Правила выполнения рабочей документации проводных средств связи
ГОСТ 21.607-82	СПДС. Электрическое освещение территории промышленных предприятий. Рабочие чертежи
ГОСТ 21.608-84	СПДС. Внутреннее электрическое освещение. Рабочие чертежи
ГОСТ 21.614-88	СПДС. Изображения условные графические электрооборудования и проводок на планах.
ГОСТ Р 50775-95*	Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения
ГОСТ Р 50776-95	Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию

ГОСТ 27990-88	Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования
ГОСТ 26342-84	Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры
ГОСТ 4.188-85	Средства охранной, пожарной и охранно-пожарной сигнализации. Номенклатура показателей
ГОСТ 28130-89	Пожарная техника. Огнетушители, установки пожаротушения и пожарной сигнализации. Обозначения условные графические
ГОСТ 12.1.004-91	ССБТ. Пожарная безопасность. Общие требования
ГОСТ 12997-84	Изделия ГСП. Общие технические условия
ГОСТ Р 50658-94	Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений
ГОСТ Р 50659-94	Системы тревожной сигнализации, Часть 2. Требования к системам охранной сигнализации. Раздел 5. Радиоволновые доплеровские извещатели для закрытых помещений
ГОСТ Р 51186-97	Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и, методы испытаний
ГОСТ Р 51179-98 (МЭК 870-2-1-95)	Устройства и системы телемеханики. Часть 2. Условия эксплуатации. Раздел 1. Источники питания и электромагнитная совместимость
ГОСТ Р 51089-97	Приборы приемно-контрольные и управления пожарные. Общие технические требования и методы испытаний
ГОСТ Р 51241-98	Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний
ГОСТ Р 51558-2000	Системы охранные телевизионные. Общие технические требования и методы испытаний
ГОСТ 22006-76*	Установки телевизионные прикладного назначения. Основные параметры и общие технические условия
ГОСТ 23456-79	Установки телевизионные прикладного назначения. Методы измерений и испытаний
ГОСТ Р 50725-94	Соединительные линии в каналах изображения. Основные параметры. Методы измерений
ГОСТ Р 50571.24-2000	Электроустановки зданий, Часть 5. Выбор и монтаж электрооборудования. Глава 51. Общие требования
ГОСТ Р 50571.10-96 (МЭК 364-5-54-80)	Электроустановки зданий. Часть 5. Выбор и монтаж электрооборудования. Глава 54. Заземляющие устройства и защитные проводники
ГОСТ Р 50571.18—2000 (МЭК 60364-4-442-93)	Электроустановки зданий. Часть 4 Требования по обеспечению безопасности. Глава 44. Защита от перенапряжений. Раздел 442. Защита электроустановок до 1 кВ от перенапряжений, вызванных замыканиями на землю в электроустановках выше 1кВ

ГОСТ Р 50571.19-2000 (МЭК 60364-4-443-95)	Электроустановки зданий. Часть 4. Требования по обеспечению безопасности. Глава 44. Защита от перенапряжений. Раздел 443. Защита электроустановок от грозовых и коммутационных перенапряжений
ГОСТ Р 50571.20-2000 (МЭК 60364-4-444-96)	Электроустановки зданий. Часть 4. Требования по обеспечению безопасности. Глава 44. Защита от перенапряжений. Раздел 444. Защита электроустановок от перенапряжений, вызванных электромагнитными воздействиями
ГОСТ Р 50571.21-2000 (МЭК 60364-5-548-96)	Электроустановки зданий. Часть 5. Выбор и монтаж электрооборудования. Раздел 548. Заземляющие устройства и системы уравнивания электрических потенциалов в электроустановках, содержащих оборудование обработки информации
ГОСТ Р 50571.22—2000 (МЭК 60364-7-707-84)	Электроустановки зданий. Часть7. Требования к специальным электроустановкам. Раздел 707. Заземление оборудования обработки информации
ГОСТ Р 12.2.143-2002	Системы фотолюминесцентные эвакуационные. Элементы систем. Классификация. Общие технические требования. Методы контроля
ГОСТ Р 12.4.026-2001	Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний
РД Гостехкомиссии России	Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации
СНиП 23.05-95*	Естественное и искусственное освещение
СНиП 21-02-99*	Стоянки автомобилей
ГОСТ 29073-01	Совместимость технических средств измерения, контроля и управления промышленными процессами электромагнитная. Устойчивость к электромагнитным помехам. Общие положения
ГОСТ Р 50009-2000	Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
ГОСТ Р 50752-95	Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники
Р 78.36.005-99	Выбор и применение систем контроля и управления доступом
РД 78.36.003-2002	Руководящий документ МВД России. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств

Р 78.36.002-99	Выбор и применение телевизионных систем видео контроля. Рекомендации
Р 78.36.008-99	Проектирование и монтаж систем охранного телевидения и домофонов. Рекомендации
РД 78.145-93	Системы и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приемки работ
РД 78.36.006-2005	Выбор и применение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрепленности для оборудования объектов
ТР 182-08	Технические рекомендации по научно-техническому сопровождению и мониторингу строительства большепролетных, высотных и других объектов уникальных зданий и сооружений